42

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

RED DE MULTISERVICIOS CORPORATIVOS PARA UNA EMPRESA DE TELECOMUNICACIONES

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICISTA

AREA ELECTRICA ELECTRONICA

P R E S E N T A N:

GERARDO NAUHYOTZIN GUADARRAMA ROBLES

ISRAEL PEREZ GARCIA

JAVIER DIAZ GAYTAN

JOSE GERARDO MARQUEZ GARCIA

RODOLFO RAMIREZ ALONSO

DIRECTOR: M. I. LAURO SANTIAGO CRUZ

MEXICO, D. F. 2001

De Israel Pérez G.

Al Señor Jesús mi Dios y Salvador que me capacitó en el conocimiento necesario para terminar esta licenciatura, por su ayuda en los momentos difíciles de mi vida y en aquellas horas en que tuve miles de cosas que hacer, y porque me sustentó y orientó para resolver cada una de ellas y siempre ha estado junto a mí.

Doy gracias a Dios por mis padres que me apoyaron en mis estudios desde que inicié mi carrera en la escuela, y por todo el tiempo en que me esforzaron por las noches y los días en que estudiaba. Porque costearon todos mis gastos, aún cuando no había y supieron darme lo necesario para culminar este trabajo. Dedico esta tesis a ambos en reconocimiento a su labor que hoy ha culminado otra de sus etapas en mi vida como estudiante.

A Nacho y a Miguel mis hermanos, porque me impulsaron en mis estudios y me hicieron esforzarme más cuando decían –"Échale ganas, ya falta poco" y por sus oraciones.

A Bárbara, Jóshua y Jonané que día a día han ido formando parte mas importante de mi vida, por su amor y sus oraciones que me fueron tan necesarios en los momentos difíciles, por su cariño incondicional que me hizo esforzarme más y más para conseguir algo mejor para ellos, para mí y toda mi familia.

A Canon, a Takeshi Ota mi jefe en Canon y a Enrique Ureña porque creyeron en mi y por su apoyo y cooperación en este proyecto.

A mis compañeros de Tesis, Gerardo M., Gerardo G., Javier y Rodolfo por su esfuerzo y dedicación en este trabajo, por los desvelos y el tiempo que quitaron a sus novias, hijos y familiares para invertirlo en este documento.

A nuestro asesor el M. Ing. Lauro Santiago por sus consejos y apoyo a nuestro grupo de tesis y por su tiempo.

Al PAT y a la Gente del Palacio de Minería por darnos la oportunidad de entrar al programa, cuyo esfuerzo culmina con nuestra titulación como Ingenieros dentro de la Facultad de Ingeniería de nuestra Alma Mater, la UNAM.

De Javier Díaz Gaytán

A mis Padres

Por otorgarme la vida y darme los cuidados necesarios. Por protegerme de todos los peligros y ofrecerme el apoyo siempre que lo necesito. Por darme la oportunidad de ser alguien en la vida al darme el estudio. Gracias por quererme tanto y darme la oportunidad de emprender el vuelo en el ámbito profesional, ya que sin duda hubiera sido bastante difícil lograrlo si ustedes no me hubieran apoyado. Por todo eso y más los amo papas.

A mis hermanos

Por compartir conmigo momentos buenos y malos, y sobre todo por quererme y por estar siempre juntos representando la hermandad sobre todo, sin importar las pequeñas rencillas de hermanos durante nuestra niñez, adolescencia y juventud. Quiero que sepan que siempre estaré con ustedes en todo momento.

A Ericka

Por ser una compañera excepcional, que me ha brindado su ayuda y amor con todo su corazón, por escucharme y compartir mis tristezas así como mis logros sin ningún interés de por medio. Y por su valiosa ayuda para la realización de este documento. Gracias linda y sobretodo gracias por ser mi novia..... te amo.

A mi familia

Por ser parte de mi, por estar siempre al pendiente de lo que pasa a mi alrededor desde mi nacimiento hasta el dia de hoy. Gracias abuelos, gracias tios por ser parte de mi.

A mis compañeros

Por haber realizado un excelente trabajo de equipo, por apoyarnos en todo momento durante la realización de nuestra tesis y sobre todo por mantener una amistad entrañable. Gracias por haberme hecho participe de este gran equipo.

A Jorge Luis

Por mantener esta amistad, la cual a durado a pesar del paso del tiempo. Por compartir momentos inolvidables de ambos y sobre todo por dar el apoyo sin recibir nada a cambio. Gracias amigo.

Con el más profundo agradecimiento y cariño, dedico las siguientes líneas a mis padres:

Cristina Alonso Alvarez y Juan A. Ramírez Cedillo.
Porque siguiendo su ejemplo de superación, firmeza y empeño,
Hoy he logrado el anhelo de ser profesionista, un gusto que comparto con ustedes.

Agradezco a mis queridos hermanos: Elizabeth, Laura y Oscar,
Por su apoyo a lo largo de estos años, teniendo un verdadero orgullo de tenerlos como mi familia.

A mis apreciables amigos, con los cuales compartí estos años de gratos momentos; esperando
Que perdure por siempre nuestra amistad.

A mis compañeros tesis, por el gusto de contar con su apoyo y entusiasmo, logrando formar un
Excelente equipo de trabajo y un magnifico grupo de amigos, esperando perdure por siempre.

A mis amigos de trabajo, por su apoyo y consejos, y sobre todo por su amistad.

Agradezco a todas aquellas personas, que con su ayuda he logrado llegar a obtener el título profesional.

Agradezco principalmente a Dios que me permitió llegar a este momento, que Dios bendiga a todos por estar siempre conmigo.

Gracias

Rodolfo

De José Gerardo Márquez García

A Dios

Por otorgarme tantas bendiciones.

A mis padres

Por enseñarme a ser una persona honesta, por guiar mis pasos en los caminos difíciles, por compartir mis tristezas y alegrías, por apoyarme incondicionalmente y ayudarme a lograr una de las metas primordiales en mi vida.

A Lili

Por ser el motor de mi vida, por sus sonrisas y ternura, por sus travesuras, por sus tristezas y alegrías, por iluminar mi camino.

A Maye

Por todo su apoyo, comprensión y cariño, por caminar junto a mi.

A mis hermanos

Por su apoyo en los momentos difíciles, por formar una gran familia.

A mis cuñadas y mi cuñado

Por su apoyo para mi y para mis hermanos

A mis amigos

Por apoyarme en mis locuras y en todos mis planes.

ÍNDICE

CAPÍTULO 5 Implantación de la red

CAPÍTULO 6 Análisis del desempeño de la red

CAPÍTULO 7 Resultados y Conclusiones

INDICE DE FIGURAS

INDICE DE TABLAS

PRÓLOGO

Hoy es importante el uso de redes con soporte para la Internet y no sólo la red de redes, ya que este fenómeno está cambiando el modelo de los negocios, cuyos asuntos tienen que ver con las comunicaciones.

En el presente trabajo haremos una revisión de las nuevas soluciones de negocios de la Internet, dado que existen diferentes productos y servicios para el segmento de las pequeñas y medianas empresas. Para ello será necesario identificar las tendencias de la tecnología que actualmente se vende para este mercado. Iniciamos con el mercado de las pequeñas y medianas empresas.

Existen mercados empresariales donde las necesidades de servicios de red son miles y esto dependerá del número de usuarios y giro de la empresa. Por otro lado, existen también pequeñas y medianas empresas formadas por profesionales dedicados a prestar servicios varios a clientes particulares, u otras empresas cuyo número de usuarios no excede los 500. Uno de los requerimientos principales de estos negocios medianos, es que ellos regularmente tienen la necesidad de ubicar sus oficinas en diferentes ciudades, por lo que sus profesionales o empleados tienen que desplazarse continuamente y junto con ellos su equipo con conexión a la red corporativa. Otra necesidad común es la comunicación entre plazas instaladas en diferentes ciudades, por ello mismo son necesarios los servicios de red y recursos compartidos que permitan una comunicación total de un punto a otro dentro y fuera de la red.

Actualmente existen muchos usuarios de red conectados remotamente que pueden resolver problemas a distancia, ejecutar diagnósticos, resolver problemas de configuración, atender llamadas telefónicas vía IP y mantener videoconferencias, entre otras actividades sin la necesidad de estar frente a su escritorio o en su oficina. Estos empleados son una fuerza muy importante para las empresas de hoy. Todas estas empresas tienden a crecer rápidamente y deben adaptarse constantemente a estos cambios con facilidad, y es nuestra tarea construir la solución más conveniente para WideCOMM.

Todos sabemos que muchas empresas medianas y pequeñas no tienen dedicado un gran capital para invertir en los departamentos y proyectos de IT (*Information Technology*, Tecnología para la Información). Esto es una oportunidad para nosotros como desarrolladores de soluciones para este mercado y por ello debemos estar muy consientes de ello.

Otro punto importante es que algunas empresas no contratan personal calificado para el soporte de sus sistemas de información, prefieren contratar los servicios de otras empresas.

Hoy en día los servicios de red como la Internet, video conferencias, voz por IP, servicios de mensajes y otros, son más comunes y necesarios que hace apenas algunos años, por lo que, aun las pequeñas y medianas empresas requieren de ellos para mantenerse a la vanguardia en tecnología de información, y para no perder la oportunidad de seguir creciendo y compitiendo con las empresas del mismo ramo en que se desenvuelven. Por ello, es necesario invertir e implementar un sistema que pueda de alguna manera ser modular, y que permita con el tiempo una actualización para hacerla crecer de forma continua y que a la vez sea completamente funcional y eficiente para la empresa y sus empleados o usuarios.

Las soluciones se conforman comúnmente por software, hardware y servicios de valor agregado, que se complementan para cubrir integralmente los requerimientos de las empresas y cada uno de sus usuarios.

Para definir de manera acertada las necesidades de una empresa debemos preguntarnos :¿Qué es lo que actualmente tienen conectado?, ¿Qué cantidad de información es la que envían y reciben?, ¿Qué tipo de información es ésta?, ¿Son simplemente correos o aplicaciones multimedia?, ¿Actualmente gastan en documentos?, ¿Qué es lo que pueden hacer actualmente con la conectividad?, Con esto podemos definir que clase de servicios podrían facilitar su trabajo para hacerlo más eficiente. También tendríamos que trabajar con cada departamento de la empresa. Por ejemplo, podríamos encontrar en el departamento de contabilidad un sistema clave específico que haga exactamente lo que ellos necesitan. Entonces, si nosotros vamos al departamento de Recursos Humanos, por ejemplo, probablemente encontraríamos un sistema dedicado a hacer esas tareas específicas para también usarlas, dado que ellos realmente tienen tareas especificas que cumplir y trabajar con sistemas centralizados.

Otro asunto importante es comenzar con la extensión del poder de cómputo de la empresa, ya que ahora se puede tener la habilidad de conversar casualmente en una comunicación persona a persona, probablemente por un medio como la Internet, mientras los usuarios hacen un documento en Word o una hoja de Excel, que posteriormente se envíen por el mismo medio. Lo que significaría el uso de procesos organizacionales automatizados con computadoras y tecnología de Red, donde la Internet juega un papel fundamental para promover un crecimiento continuo. Hoy en día muchas empresas están adoptando estas tecnologías que permiten el desarrollo de forma veloz y reduciendo costos en los negocios que realizan y con ello ser más competitivos.

Con todos estos cambios tecnológicos tenemos la habilidad de compartir información de manera más eficiente en un momento, para tomar decisiones y reducir costos y nuevamente sacar ventaja a la competencia al no estar detenidos en un proceso por falta de información o tiempos de retraso, evitando costos por información y esfuerzos duplicados.

Nosotros podemos entonces eliminar mucha información redundante y publicar en un Web Site la información importante para nuestros clientes, usando tecnologías de Internet e Intranet. De acuerdo a sus necesidades y en el horario que ellos prefieran. Lo anterior sobre la red corporativa. Un ejemplo de la tecnología a la que nos referimos en estos casos es con el uso del protocolo IP. Con este protocolo de red nosotros tenemos transporte de información y damos a las cosas independencia de plataformas. También los *Web browser(Buscadores de Internet)* que nosotros usamos como medio de interfaz para la red es otra herramienta de tecnología común que podemos usar en las Intranet de

las empresas. Estos *Web brousers* nos permiten interactuar en diferentes sistemas operativos como Windows o Apple MacIntosh.

El trabajo en diferentes plataformas de computadoras nos da la oportunidad de accesar a la información con sencillez, además de que son aplicaciones que se pueden implementar con rapidez y darnos una extensión global a la información que estamos tratando de alcanzar dentro de nuestra Intranet, que nuevamente se refleja en una reducción de costos e incremento en la productividad.

Los servicios mencionados anteriormente nos permiten desarrollar aplicaciones como aprendizaje a distancia, soporte técnico, videoconferencia y otros, además nos ayuda en tareas como calendarios centralizados y organización de agendas en las empresas, facilitan la comunicación interna y externa. Hoy en día, muchas empresas tienen una Intranet como medio para facilitar estos trabajos, reduciendo dramáticamente los recursos y las horas empleadas por diferentes departamentos. Lo mismo para las divisiones de ventas, recursos humanos, el área legal, compras e importaciones, servicio y otros. Todo lo anterior y mucho más manejando el protocolo IP en la Red.

También existen servicios de extranet útiles para mantener comunicación con distribuidores, clientes y proveedores, llevar a cabo programas de educación y entrenamiento en línea con sistemas de audio y voz simultáneos, brindar servicios a clientes como revisiones del estado de sus ordenes de compra o reportes de cuenta, stocks e inventarios, call centers entre otros, en cualquier hora del día. Estas aplicaciones hoy son comunes y se pueden implementar en una red con la misma infraestructura tecnológica.

Un ejemplo en particular son los servicios de telefonía para llamadas personales que nos dan la habilidad de combinar muchos formatos de mensajes como: correo de voz, faxes o correos electrónicos, que pueden proveerse a los usuarios para hacerlos más productivos y eficientes en sus labores cotidianas dentro de las empresas.

La implementación de estas tecnologías permite alcanzar la reducción de costos en redes amplias, con la eventual eliminación de los PBX y simplificando métodos de operación en la red y ahorrando los gastos de la red de voz, red de datos y videoconferencia.

En realidad se adquieren bastantes beneficios al poder tener infraestructura de red convergente con tecnología de datos, voz y videoconferencia convergentes, y es importante considerar que todavía existen empresas que creen no estar listas para este tipo de soluciones, pero generalmente es por el desconocimiento de las mismas, además de que consideran que salen de sus alcances.

De la tecnología de Redes de datos podemos decir que actualmente existen dispositivos verdaderamente eficientes como: switches para LANs, switches para Ethernet y muchos más, para migrar redes de área local a redes con mecanismos de acceso dedicado mediante switches en un campus. También conectar a usuarios dentro de la red y comunicarlos a través de routers y servidores de acceso, además de la conectividad por la Internet.

Existen tecnologías de multiservicios que proveen soluciones para voz, datos y video y todas ellas giran alrededor de la tecnología de Internet, que es el núcleo de toda esta tecnología. Así como servicios de banda ancha para consumidores particulares, Redes

Virtuales Privadas que permiten conectar organizaciones sobre redes públicas (la Internet), con sistemas de seguridad con las que pueden darse diferentes servicios a las empresas y su clientes.

Todo lo anterior funciona sobre una infraestructura tecnológica de redes interconectadas, con tecnología WAN que serán el tema principal de este documento incluyendo los servicios necesarios para proveer multiservicios de red y voz al corporativo WideCOMM.

CAPÍTULO 1

Introducción

En este capítulo describiremos la historia de las redes de cómputo, el gran apoyo que se ha tenido en todos los ambientes laborales al hacer las tareas más llevaderas se bosquejará la evolución de las mismas conforme han cambiado las necesidades de la economía mundial. También hablaremos de la problemática derivada de los requerimientos de intercambio de información y en general del manejo de recursos compartidos dentro de un corporativo de telecomunicaciones que llamaremos *WideCOMM*, así como la comunicación de voz entre las diferentes sucursales de la empresa.

1.1. Historia de las redes

Hasta hace muy poco la infraestructura de las comunicaciones de las *PyMEs* (*Pequeñas y Medianas Empresa*) era un rubro en el que no se podía elegir el invertir o no en grandes cantidades de dinero, tenía que hacerse. Tales comunicaciones implicaban fundamentalmente una red de voz; compuesta de un *PBX (Private Branch eXchange, Central de Conmutación Privada*), el cableado sin estructurar y los aparatos de extensiones para comunicar interna y externamente a los empleados, de forma que toda la administración de las comunicaciones estaba centralizada en emuladores de centrales telefónicas pequeñas, con la capacidad de interpretar los tipos de señalización de la *PSTN (Public Switched Telephone Network, Red Pública Telefónica Conmutada.)*

En un principio, la mayoría de los corporativos recibían enlaces de troncales analógicas, mejor conocidas como *COT's, (Central Office Trunks, Troncales de Oficina Central)* pero después se dio el salto hacia enlaces de más capacidad y se empezó a hablar de enlaces *E1's* y *T1's*, que provienen de los esquemas de enlaces de comunicaciones convencionales *PDH (Plesiochronous Digital Hierarchy, Jerarquía Digital Plesiócrona) y SDH (Synchronous Digital Hierarchy, Jerarquía Digital Síncrona)* que manejan la cantidad de información transmitida con base a múltiplos de canales compuestos por la cantidad mínima necesaria para soportar un enlace de voz digitalizado, es decir 64 kbps. Señalando que los enlaces *E1's* y *T1's* representan enlaces digitales en formato europeo y americano, respectivamente. Ya sea en su modalidad punto a punto o punto multipunto, estos enlaces transportaban más información y eran adecuados para corporativos más grandes que medianos. Conforme el mercado internacional fue apuntando hacia una globalización, tal y como la conocemos hoy en día, las comunicaciones fueron cambiando de igual forma para proveer de los servicios que demandaban las *PyMEs*.

En el ramo de las comunicaciones, la necesidad de compartir la información ha derivado en el desarrollo de varias tecnologías que apuntan hacia la eficiencia en los servicios que prestan, apoyándose en conceptos como administración de recursos, monitoreo y prevención de fallas, entre otras.

Existe toda un historia desarrollada alrededor de estos conceptos y que en particular refleja la forma en la que ha evolucionado el mundo de las redes de comunicaciones, en especial de datos, no obstante que la transmisión de voz, aunque ha seguido un camino diferente, tiende en estos tiempos a utilizar las técnicas de señalización y transporte que emplea el envío de datos, ya sea por conmutación de circuitos de celdas o de paquetes.

La historia de las redes está dividida en 4 etapas, las cuales están descritas por sus características más importantes. La primera etapa se refiere al procesamiento centralizado de los años 60s y 70s, la segunda fase se define por la aparición de las primeras redes locales, la tercera parte describe a las interredes (en los años 80s) y finalmente la etapa actual con las redes globalizadas. Cada una de estas fases se detallarán a continuación:

Procesamiento centralizado. Esta etapa se caracteriza por la concentración total de todos los procesos con la intención de compartir recursos en equipos conocidos como *main frames (sistema principal)*, y que permitían el acceso a la información en dicho

sistema central por medio de sesiones desde equipos terminales, cuya función específica consistía en obtener datos y desplegarlos en monitores por medio de mecanismos de peticiones/respuestas que el equipo central atendía de manera ordenada en un esquema de *Round Robin (toma circular secuencial)* en un multiplexado por eventos. Este tipo de red fue implementado con equipos *IBM (Industries for Business Machines, Equipos para Industrias de Negocios)*; y son típicos los controladores de terminales 3270 y 3276 operando con protocolos orientados al conteo de bytes como es el caso de *SDLC (Synchronous Data Link Control, Control de Enlace de Datos Síncrono)*, todo sobre una arquitectura de red llamada *SNA (System Network Architecture, Arquitectura de Sistema de Red)* creada también por IBM. Este tipo de red se ilustra en la Figura 1.1 en donde se indica el elemento distribuidor hacia los equipos terminales de datos.

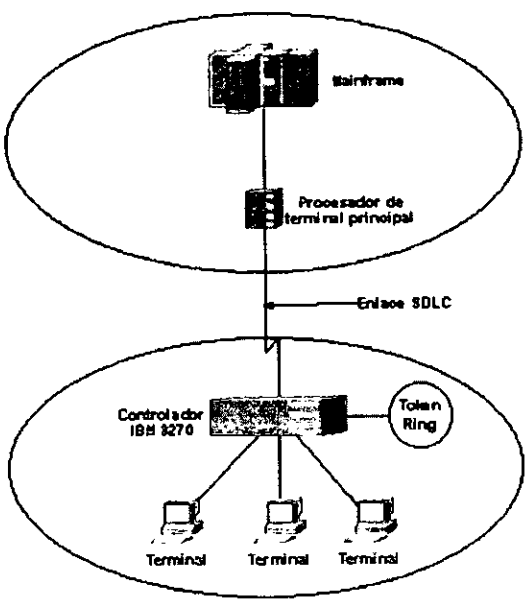


Figura 1.1. Red de procesamiento centralizado basado en controladores.

Redes. En esta etapa se desarrollaron las primeras redes verdaderas que permitían el acceso a los recursos de forma compartida y distribuida; también se distingue por el surgimiento de los primeros estándares de redes *LAN* (*Local Area Network, Red de Área Local*) tales como *Ethernet, Token Ring y ArcNET*, entre otros. Además, se desarrollan las interfaces de configuración y gestión de los recursos compartidos en ambientes gráficos (Windows 3.x, Chamaleon, Wollongong, etc.), lo que hace más amigable el contacto con las redes de datos. Este periodo es también testigo de la aparición de los protocolos de red que se convertirían en los más populares como lo son el *TCP/IP (Transmition Control Protocol / Internet Protocol, Protocolo de Control de Transmisión / Protocolo de Internet)* que acompañaba a ciertas versiones de *UNIX* y la totalmente propietaria *Netware* de *Novell*, sin dejar de mencionar a *X.25* que operaba sobre redes públicas. Es aquí donde se visualiza de forma clara la ventaja que ofrece la

conectividad de recursos dentro de una empresa y las aplicaciones, que ahora son comunes, representan una novedad en ese momento tales como: el correo electrónico, transferencia de archivos, aplicaciones cliente servidor, acceso remoto, etc. Esta etapa se muestra en la Figura 1.2 en forma de redes aisladas.

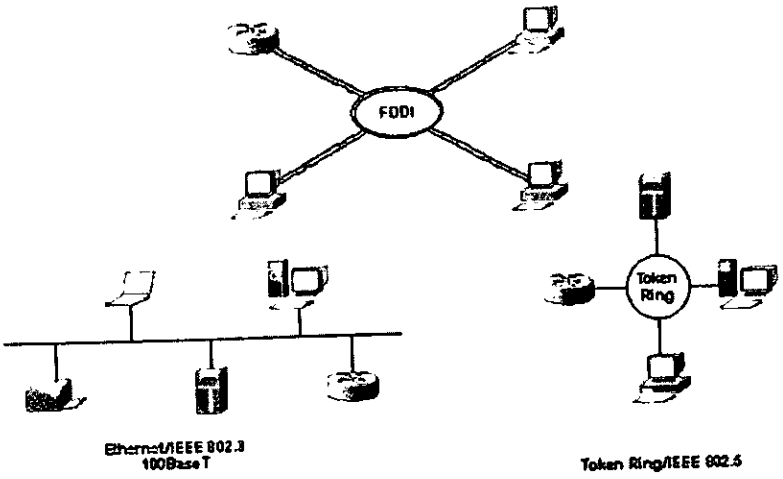


Figura 1.2. Diferentes topologías de redes locales (LANs).

Interredes. Para los 90's, la globalización que se mencionó antes y no la tecnología, obliga a que las aplicaciones tradicionales de redes se extiendan a más allá de las redes locales convencionales, apareciendo el concepto de redes *WAN* (*Wide Area Network, Redes de Área Amplia*) mucho más desarrollado que en la etapa anterior, en donde era raro que existiera la necesidad de comunicar maquiladores con proveedores, por ejemplo. La expansión de empresas y la creación de sucursales dentro de otra ciudad u otro país obliga a extender de igual forma la conectividad de las aplicaciones, dando lugar a enlaces dedicados o privados, justificando así un tráfico constante y que además ahorre los costos de larga distancia acumulados. Aparecen dispositivos de comunicaciones que antes no eran necesarios como los *routers* y *switches* de capa tres, entre otros. La figura 1.3 muestra la conexión de diferentes topologías de redes locales para formar una red de área amplia.

Así mismo, esta figura indica que la diferencia de tecnologías de las redes locales no impide su interconexión en una base más amplia, debido a que el protocolo IP permite esta interoperabilidad al ser un protocolo abierto. No obstante, esta etapa está marcada por otro fenómeno que acrecienta el desarrollo de las redes en general y es lo que se conoce como la Internet.

Definir todo lo que significa la Internet en un párrafo sería poco más que imposible; sin embargo se tratará de abarcar lo más posible, la Internet cambió y está cambiando la forma en que vivimos, trabajamos y aprendemos. Cabe comentar que existe alguna confusión entre los términos *WWW (World Wide Web, Red Amplia Mundial)* e Internet, y a veces se usan indistamente como sinónimos, lo cual no es necesariamente cierto, ya que mientras el WWW se refiere al conjunto de páginas programadas *en HTML*

(Hypertext Mark-Up Language, Lenguaje de Marcado de Hipertexto), ASP (Active Server Pages, Páginas de Servidor Activo), etc., que se encuentran ligadas entre sí e identificadas por contenido, la Internet es un conjunto de redes o como se le conoce en la jerga de comunicaciones "la red de redes", y en donde se mezclan todas las topologías existentes y que tienen en común el protocolo de comunicaciones TCP/IP o alguna emulación del mismo, implementado sobre un medio diferente al de las redes de difusión o redes punto a punto, con el simple propósito de conectarse a la inmensa nube de la Internet, como se ve en la figura 1.4.

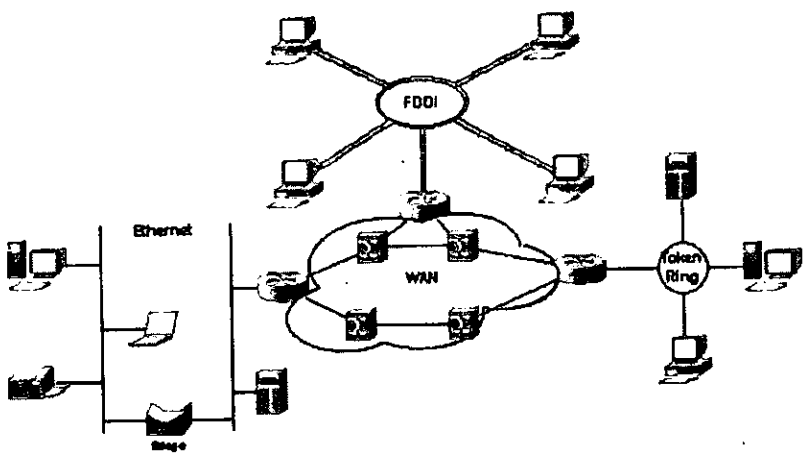


Figura 1.3. Interredes.

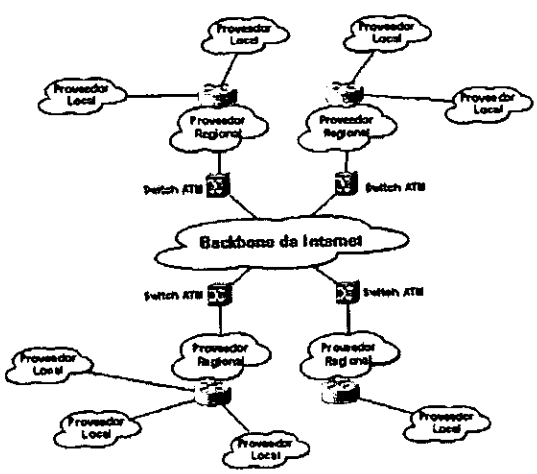


Fig.1.4. Arquitectura básica de Internet.

Interredes globalizadas. El concepto de cadena de valor agregado, hace que las redes corporativas crezcan dentro de la nueva economía internacional y se expandan a otros países, al igual que la saturación de los mercados locales obliga a las maquiladoras a desplazarse a otros países donde la mano de obra sea más barata. El correo electrónico como lo conocimos en su primera etapa de redes locales y redes *WAN*, así como la transferencia de archivos y aplicaciones de red cambian para convertirse en una pieza fundamental en la estrategia de crecimiento de las compañías. Aparecen el *EDI (Electronic Data Interchange, Intercambio Electrónico de Datos)*, los portales (horizontales y verticales), las transacciones entre provedores, así como el comercio electrónico.

Como resultado del crecimiento de las redes, surgen nuevos tipos de demanda en las *IT (Information Technologies, Tecnologías de Información)*,por ejemplo: video en demanda, videoconferencia, aprendizaje electrónico, etc.; y consecuentemente, la implementación de las mismas plantea desafíos que van desde proveer de una mayor cantidad de ancho de banda hasta garantizar el mecanismo de *QoS (Quality of Service, Calidad de Servicio)*, y sobre todo una adecuada administración de todos los recursos de la red. En principio, la idea de mayores velocidades en la red implica un cambio en el tipo de conmutación de paquetes de como se ha venido haciendo hasta ahora; proponiéndose conmutación de celdas como lo propone la tecnología *ATM (Asinchronous Transfer Mode,* que basa su funcionamiento en tasa de transmisión garantizadas y del mejor esfuerzo para proveer diferentes tipos de servicios que requieran ya sea una u otra, según se ilustra en la Figura 1.5

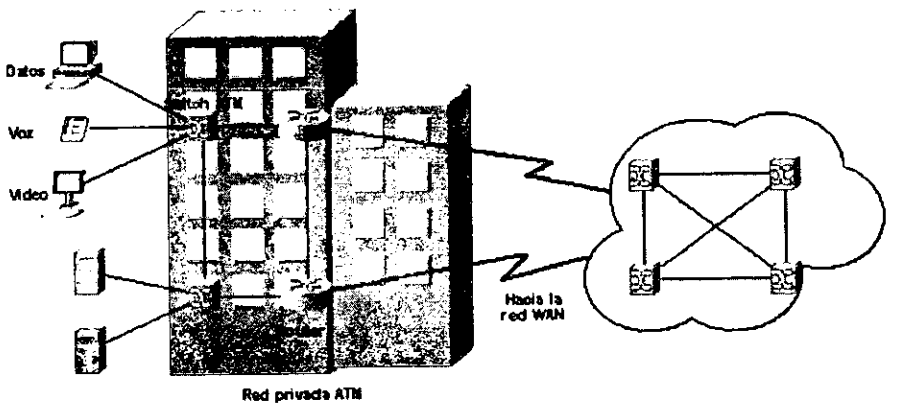


Figura 1.5. Red utilizando tecnología ATM.

No hay que olvidar que el protocolo base de la Internet es el *IP* y aunque esta tecnología ha sido probada por más de 30 años, surgió como el resultado de un experimento de redes militares que tenía como objetivo principal la conmutación de paquetes (o en este caso datagramas) que fuera robusto por la misma naturaleza militar en la que operaría. Nunca se pensó, por ejemplo, que el *IPv4* (la versión actual del protocolo de Internet) haría transferencias con calidad de servicio ni transacciones bancarias. Es por eso que se

está experimentando con una versión nueva, la *IPv6* que promete corregir la mayoría de las fallas de las que adolece su versión antecesora.

La evolución que han tenido las redes de datos ha sido resultado de satisfacer la necesidad de nuevos y diversos servicios, que han hecho que muchas empresas vayan modificando su red con tal de contar con las nuevas ventajas que se ofrecen en las modernas redes, este es el caso de *WideCOMM,* una empresa que ha tenido un crecimiento en su estructura y que ahora requiere de nuevos servicios para su red, lo que motiva a un planteamiento de reestructuración de su actual red, para ello, es necesario considerar la problemática que tiene en este momento, definiendo los requerimientos para su nueva red. Se debe señalar la importancia que tiene la descripción de la problemática que se desarrollará en el siguiente apartado, ya que dará pauta para determinar los lineamientos del plan de reestructuración de la red de *WideCOMM* y que a su es la base sustancial para el desarrollo del presente documento.

1.2. Problemática

La empresa de telecomunicaciones *WideCOMM* realiza la comercialización de equipos de comunicaciones, y efectúa labores de integración de redes para soluciones de pequeñas y medianas empresas, que les permitan elevar la productividad en sus negocios al mismo tiempo que presta servicios de consultoría y auditoría a redes, para determinar el desempeño de las redes de sus clientes y ubicar puntos de fallas y así establecer oportunidades de negocio.

El problema de la empresa *WideCOMM* es que no posee una infraestructura de red que permita el intercambio de datos entre sus diferentes sucursales a lo largo del territorio nacional. Esto incrementa los gastos de operación del corporativo, ya que los procesos administrativos se hacen más largos y el cliente necesita una respuesta eficaz y rápida. Aunado a esto, se mantiene una comunicación vía telefónica en forma constante con las sucursales para tener al día los inventarios, los estados contables, las nóminas, todo esto en lo que se refiere a la parte administrativa, y una situación similar se presenta al brindar soporte técnico a los diferentes equipos instalados, lo que implica el establecer llamadas telefónicas muy prolongadas en tiempo o en su defecto la contratación de personal eventual o de planta para realizar esta labor, lo cual depende de la cantidad de usuarios. Lo anterior implica que la organización requiera de una solución tecnológica que permita la optimización de los recursos de enlaces dedicados, el ahorro en la facturación de llamadas de larga distancia, el entrenamiento y soporte remotos y la transmisión segura de datos confidenciales haciendo uso de un esquema básico de seguridad. *WideCOMM* no cuenta con conexiones en red para compartir los recursos del equipo de cómputo entre la Ciudad de México y las sucursales en provincia; lo que sí posee es un acceso a Internet vía *modem (modulador-demodulador)* para sólo una de las computadoras de la oficina central en la Ciudad de México.

El envío de los datos administrativos se realiza mediante cintas magnéticas utilizando los servicios de empresas de mensajería, que además de los retrasos para la entrega de los paquetes, exponen al corporativo a la fuga de información o la pérdida de la misma. Para la comunicación de voz entre ellas se está utilizando la telefonía convencional con servicios de larga distancia, con el alto costo en rentas que esto implica. En la figura 1.6 se ilustra el estado de actual de redes locales aisladas en la empresa *WideCOMM.*

1.3. Soluciones Alternas

Algunas de las soluciones para la problemática presente son: Servicios Conmutados implementados con *modems*, *ASPs (Application Service Providers, Proveedores de Servicios de Aplicación)* y la implementación de una red de área amplia. Analizando las tres opciones encontramos que los Servicios Conmutados presentan retrasos considerables en la transmisión de voz y datos, así como la dependencia de un solo proveedor de servicios, que sumados a la implementación de un protocolo de autenticación, daría como resultado tiempos de espera muy prolongados.

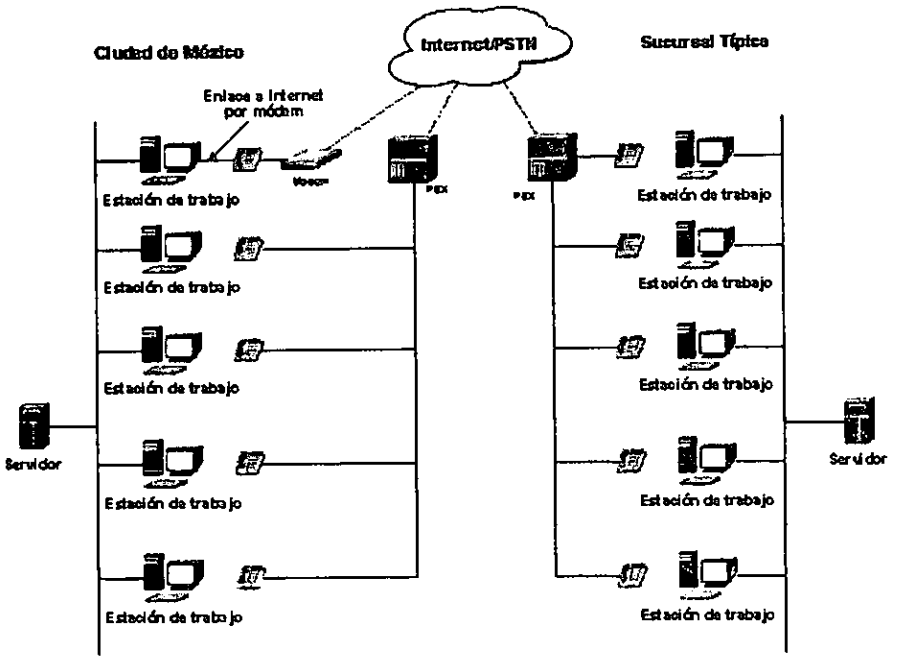


Figura 1.6. Estado actual del corporativo WideCOMM.

Los *ASPs* son compañías de software que montan aplicaciones específicas en la *WEB* para que sus clientes puedan correr programas de facturación, diseño, etc., sin tener que comprar una copia de la licencia del software e instalarlo en sus equipos. Una de las ventajas que ofrece este servicio radica en el ahorro de la compra de software al igual que en la capacitación del personal para administrarlo ya que la solución se implementa por completo del lado del proveedor. Sin embargo, una clara desventaja es la exposición de la información de alguna compañía en el tráfico de la Internet y falta confidencialidad en el intercambio de datos y exponen la información de *WideCOMM* en forma indirecta ya que en la Internet siempre existe el riesgo de ser observados y ser blanco de ataques por terceros.

Por lo tanto, nuestro enfoque se dirige a una red de área amplia. La propuesta considera el diseño e implementación de una red *WAN* con terminaciones *LAN* en todas las sucursales. En un modelo de red colapsada hacia el centro, donde los servicios de voz, video y datos estarán provistos de acuerdo a la prioridad en cada oficina y también dependiendo del ancho de banda de que se destine a cada uno. El protocolo de red propuesto es IP y en general, las aplicaciones pertenecen a la pila de protocolos *TCP/IP*, en un ambiente de Windows 9.X y Windows NT como sistema operativo dominante en las estaciones de trabajo y servidores.

El esquema de voz se compondrá de 2 a 4 enlaces analógicos por sucursal mediante interfaces a equipos multilíneas en las sucursales y mediante servicios digitales a la oficina central. La seguridad de la red estará compuesta por 2 aspectos: por un lado, en la transmisión de datos se implementarán túneles de redes virtuales con aperturas en cada una de las sucursales, ya sea como cliente *VPN (Virtual Private Network, Red Privada Virtual)* en PC's o mediante un *router* y terminaciones en el nodo central para su autenticación empleando *DES (Data Encrypted Standar, Estándar de Encripción de Datos)* como algoritmo de encriptación; por otro lado, se colocará una barrera de seguridad mediante un par de *Firewall's (Pared de Fuego)* en modo redundante para vigilar el tráfico saliente y entrante desde la Internet. El diseño de la solución para el corporativo *WideCOMM* consistirá de cuatro etapas que describimos a continuación:

Etapa1 Instalación y configuración de los equipos de comunicación al igual que la contratación de servicios digitales, por ejemplo enlaces dedicados. En esta primera etapa se montarán y configurarán todos y cada uno de los equipos de comunicaciones tales como: *routers, PBXs, switches, hubs*; además de los servidores en cada una de las sucursales, incluyendo las estaciones de trabajo, de tal manera que se puedan hacer pruebas con cada una de las ciudades antes de conectar las LANs a la red principal. El enlace entre ciudades deberá hacerse con canales dedicados (DS0s) que se contratarán con Telmex. Estos enlaces deben de cumplir con la *CIR (Comitted Information Rate, Tasa de Intercambio de información Comprometida.)*

Etapa2 Adecuación de los equipos de comunicación de datos para su conexión con los equipos telefónicos convencionales: Instalación de tarjetas de voz y la adquisición de líneas telefónicas domésticas.

Etapa3 Estructuración de esquemas de seguridad para la red, instalación de *firewalls*, creación de redes privadas virtuales, y configuración de políticas de seguridad.

Etapa4 Optimización y ajustes de la red. Se pondrá a punto la operación de la red y se medirán los parámetros de desempeño de la misma; al igual que se probará la seguridad mediante ataques controlados desde la Internet con software de hackers y barrido de puertos.

1.4. Objetivos

Al final del proyecto se espera obtener una red donde los gastos de operación serán mínimos y que además, incrementarán el nivel productividad del corporativo, donde

gracias al sistema, la comunicación entre nodos será más eficiente. La reducción de gastos podrá observarse en la facturación telefónica mensual, ya que el uso de la red interna, evitará los gastos de larga distancia; además de proveer servicios adicionales como *DISA (Direct Inward System Access, Sistema de Acceso Entrante Directo)*, los cuales permitirán ingresar al conmutador local con una clave, y obtener permisos de comunicación de llamadas locales y red interna, sin la necesidad de estar presente en la oficina central de México o en la oficina local en cada estado. En ese sentido, la generación de reportes de llamadas y el control de los recursos (tiempo de llamada, cuota límite, etc.) estará enlazada a un sistema que permitirá poner topes de tiempo y límites de gastos para obtener un control de llamadas más granular.

Otro aspecto importante que ahorrará recursos a la corporación es el hecho de enviar reportes de facturación en tiempo real, y que elimina el envío de cintas de respaldo por mensajería que implica gastos y tiempos de envío.

Por su parte, el incremento en la productividad del personal es un rubro más subjetivo de evaluar directamente, debido a que son factores personales que se verán reforzados por la alta disponibilidad de los recursos y la confianza con la que los datos viajen en la red. Al momento de tener presentes todos los recursos necesarios para el desempeño del personal (servicios de correo, transferencia de archivos, comprobación de gastos en línea, inventarios, etc.) en los horarios necesarios y con la velocidad de acceso requerida, los empleados se podrán concentrar únicamente en sus funciones específicas y esto aumentará su productividad.

En la parte de soporte técnico a las sucursales, el tiempo de respuesta a un soporte se verá directamente beneficiado dado que los accesos mediante la red serán inmediatos y no se luchará contra la saturación de las líneas.

Además que un diseño de esta envergadura pondrá a prueba los conocimientos de ingeniería de las diferentes partes involucradas en el proyecto, logrando con ello una excelencia en el desempeño de las labores cotidianas.

CAPÍTULO 2

Conceptos Básicos

En este capítulo describimos conceptos necesarios para la comprensión de las redes, dado que el conocimiento plasmado en este trabajo tiene su base teórica en sistemas implementados por computadoras.

Iniciamos con el concepto de red, ventajas y uso de ellas en grupos de trabajo dentro de oficinas y empresas. Seguimos con servicios de red, donde se tocan algunos de los servicios más importantes para el funcionamiento, administración de usuarios, aplicaciones y otros. También se contemplan los medios de transmisión alámbricos e inalámbricos y los medios más comunes para la comunicación entre equipos de cómputo. Posteriormente escribimos acerca de los dispositivos necesarios para formar redes en sus diferentes plataformas y arquitectura, puntualizando en conectores, tarjetas de red y dispositivos de enlace en general.

La comunicación entre computadoras se hace mediante protocolos de comunicación, en este capítulo se describen los más significativos y usados en el mundo de las redes de computadoras y se incluyen protocolos de transmisión de datos y voz.

Al final del capítulo escribimos sobre seguridad de datos y el mantenimiento integral de la información de las empresas de telecomunicaciones.

2.1. Introducción a las redes

La definición más clara de una red es la de un sistema de comunicaciones que permite comunicarse con otros usuarios y compartir archivos y periféricos, como lo muestra la figura 2.1. Esto a través de un conjunto interconectado de computadoras autónomas. Se dice que dos computadoras están interconectadas, si éstas son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, también puede hacerse mediante el uso de láser, microondas y satélites de comunicación.

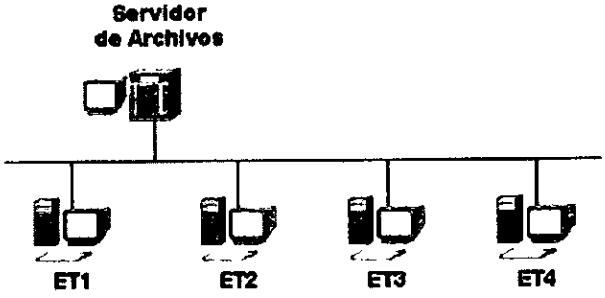


Figura 2.1. Red de Computadoras.

Son muchas las organizaciones que cuentan con un número considerable de computadoras en operación y con frecuencia alejadas unas de otras. Por ejemplo, una compañía con varias fábricas puede tener una computadora en cada una de ellas para mantener un seguimiento de inventarios, observar la productividad y llevar la nómina local.

Inicialmente cada una de estas computadoras puede haber estado trabajando en forma aislada de las demás, pero en algún momento, la administración puede decidir interconectarlas para tener así la capacidad de extraer y correlacionar información de toda la compañía; es decir, el objetivo básico es compartir recursos, hacer que todos los programas, datos y equipos estén disponibles para los clientes de la red que lo soliciten, sin importar la localización del recurso o del usuario.

Un segundo objetivo es proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una no se encuentra disponible, podría utilizarse alguna de las copias.

La presencia de múltiples computadoras significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico, y es obvio que las grandes máquinas tienen una rapidez mucho mayor.

Una red de computadoras puede proporcionar un poderoso medio de comunicación entre personas que se encuentran a largas distancias.

Con el empleo de una red es relativamente fácil para dos personas, que viven en lugares separados escribir un informe. En la figura 2.2 vemos un ejemplo de comunicación entre dos personas de distintas ciudades, una está en la CD. de México y la segunda en Monterrey. Su enlace es vía telefónica por medio de un MODEM (MOdulador-DEModulador).

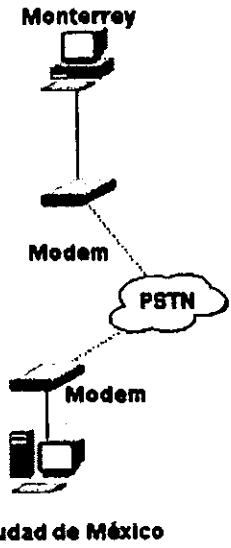


Figura 2.2. Comunicación entre personas a larga distancia.

2.1.1. El trabajo en red

Las redes en general, se utilizan para compartir recursos y uno de sus objetivos es el ahorro económico. Las computadoras pequeñas tienen una mejor relación costo / rendimiento, comparada con la ofrecida por las máquinas grandes. Éstas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas constituidos por poderosas computadoras personales, una por usuario, con los datos guardados.

Este objetivo conduce al concepto de redes con varias computadoras en el mismo edificio. A este tipo de red se le denomina LAN (*Local Area Network*, Red de Área local), en contraste con lo extenso de una WAN (*Wide Area Network*, Red de Área Amplia) que se caracteriza por sus largas distancias de cobertura.

Una LAN constituye una forma de interconectar una serie de equipos informáticos. A su nivel más elemental, una LAN no es más que un medio compartido, con una serie de reglas que rigen el acceso a dicho medio. La LAN más difundida, la Ethernet, utiliza un

mecanismo denominado CSMA/CD *(Carrier Sense Multiple Access with Collision Detection, Acceso Múltiple por Sensado de Portadora con Detección de Colisiones)*. Esto significa que cada equipo conectado sólo puede utilizar el medio de comunicación cuando ningún otro equipo lo está utilizando. Si hay algún conflicto, el equipo que está intentando establecer la conexión la anula y efectúa un nuevo intento más adelante. La Ethernet transfiere datos a 10 o 100 Mbits/seg., lo suficientemente rápido como para hacer inapreciable la distancia entre los diversos equipos y dar la impresión de que están conectados directamente a su destino.

Existen topologías muy diversas (· bus, estrella, anillo) y diferentes protocolos de acceso. A pesar de esta diversidad, todas las LAN comparten la característica de poseer un alcance limitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte transparente para los usuarios de los recursos.

Además de proporcionar un acceso compartido, las LAN modernas también proporcionan al usuario multitud de funciones avanzadas. Hay paquetes de *software* de gestión para controlar la configuración de los equipos que forman la LAN, la administración de los usuarios, y el control de los recursos de la red. Una estructura muy utilizada consiste en varios servidores a disposición de distintos usuarios. Los primeros, por lo general máquinas más potentes, proporcionan servicios como control de impresión, ficheros compartidos y correo a los últimos, por lo general computadoras personales. Los servicios en la mayoría de las LAN son muy potentes. La mayoría de las organizaciones no desean encontrarse con núcleos aislados de utilidades informáticas. Por lo general prefieren difundir dichos servicios por una zona más amplia, de manera que los grupos puedan trabajar independientemente de su ubicación. Los *routers (ruteador)* y los *bridges (puentes)* son equipos especiales que permiten conectar dos o más LAN. El *bridge* es el equipo más elemental y sólo permite conectar varias LAN de un mismo tipo. El *router* es un elemento más inteligente capaz de interconectar redes de área local así como redes de área extensa o bien una LAN con una WAN.

Las grandes empresas disponen de redes corporativas de datos basadas en una serie de redes LAN y *routers*. Desde el punto de vista del usuario, este enfoque proporciona una red físicamente heterogénea con aspecto de un recurso homogéneo.

Hay situaciones en las que deja de ser práctico seguir ampliando una LAN. A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras. Dos de los componentes importantes de cualquier red son la red de teléfono y la de datos. Son enlaces para grandes distancias que amplían la LAN hasta convertirla en una WAN. Casi todos los operadores de redes nacionales ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad, que funcionan basándose en la red pública de telefonía hasta los complejos servicios de alta velocidad (como *frame relay* y *SMDS-Synchronous Multimegabit Data Service*) adecuados para la interconexión de las LAN. Estos servicios de datos a alta velocidad suelen denominarse conexiones de banda ancha. Se prevé que proporcionen los enlaces necesarios entre LAN para hacer posible lo que han dado en llamarse autopistas de la información.

Normalmente en una LAN se reemplazan máquinas grandes por estaciones de trabajo, esto no ofrece la posibilidad de introducir muchas aplicaciones nuevas, aunque podrían mejorarse la fiabilidad y el rendimiento. Sin embargo, la disponibilidad de una WAN si genera nuevas aplicaciones viables, y algunas de ellas pueden ocasionar importantes efectos en la sociedad. Para dar una idea de los usos importantes de redes de computadoras, tenemos como ejemplos: el acceso a programas remotos, el acceso a bases de datos remotas y las facilidades de comunicación de valor añadido.

Una compañía que ha producido un modelo que simula la economía mundial, puede permitir que sus clientes se conecten usando la red y ejecuten un programa para ver como pueden afectar a sus negocios las diferentes proyecciones de inflación de tasas de interés y de fluctuaciones de tipos de cambio. Con frecuencia se prefiere este planteamiento que vender los derechos del programa, en especial si el modelo se está ajustando constantemente ó necesita de una máquina muy grande para correrlo.

Todas estas aplicaciones operan sobre redes por razones económicas, el llamar a un computadora remota mediante una red resulta más económico que hacerlo directamente. La posibilidad de tener un precio más bajo se debe a que el enlace de una llamada telefónica normal utiliza un circuito caro y en exclusiva durante todo el tiempo que dura la llamada, en tanto que el acceso a través de una red, hace que sólo se ocupen los enlaces de larga distancia cuando se están transmitiendo los datos.

Una tercera forma que muestra el amplio potencial del uso de redes, es su empleo como medio de comunicación (*Internet)*. Como ejemplo, el tan conocido por todos, e-mail (*Electronic Mail, Correo Electrónico*), que se envía desde una terminal a cualquier persona situada en cualquier parte del mundo que disfrute de este servicio. Además de texto, se pueden enviar fotografías, imágenes, videos, archivos y otros.

2.1.2. Modelos de Cómputo

En el siguiente punto se describirán los diferentes modelos de cómputo como son:

Cliente servidor

En los entornos con grandes computadoras y mini computadoras, el procesamiento y la memoria se encuentran centralizados. Hay varias razones para ello, incluyendo el costo, la seguridad y la gestión.

La computadora central se convierte en el núcleo de la organización de proceso de datos, habiendo un equipo de profesionales que tienen como única tarea el trabajar y administrar el sistema.

Los terminales conectadas al computadora central permiten que otros usuarios puedan compartir las posibilidades de cálculo y la memoria de las computadoras centrales.

Este tipo de proceso centralizado se diferencia del sistema de proceso distribuido utilizado por las LAN.

En un sistema de proceso distribuido, la mayor parte de las transacciones se lleva a cabo en la memoria individual de las computadoras personales, a las que denomina estaciones de trabajo. El servidor de archivos o sistema principal se convierte en un lugar para almacenar los archivos y para gestionar la red, además de ser el lugar al que se conectan las impresoras y otros recursos compartidos. A continuación detallamos el modelo cliente / servidor como parte fundamental para el logro de una mejor comunicación en la red.

Cliente / servidor

El proceso cliente / servidor no es en sí mismo un producto, sino más bien un estilo y un método de diseño y construcción de aplicaciones de proceso. Esta formado por:

- Plataformas de proceso programables
- Separación entre función / proceso de aplicación
- Comunicación entre procesos
- Enfoque "solicitante / proveedor de servicios"

Los clientes pueden ser cualquier tipo de sistemas inteligentes, desde PCs a sistemas propietarios, y lo mismo pueden ser los servidores.

Cliente es una entidad programable que maneja parte de una aplicación que no es compartida por otros usuarios y que debe solicitar servicio e interactuar con una parte de la aplicación que reside en una función "servidor programable". La relación del cliente con el servidor es necesaria para ejecutar esa aplicación en su totalidad. La función servidor es compartida por clientes y a ellos le ofrece servicios. Las aplicaciones cliente / servidor pueden tener diferentes controles: centrado en el *host* o centrado en el cliente.

Para el caso del control centrado en el *host*, éste conoce todas las opciones de que disponen todos los usuarios en todo momento, las actividades de visualización, ejecución de programas y gestión de recursos.

Para el caso del control del cliente, éste tiene el control absoluto de la ejecución de la aplicación y los recursos compartidos son controlados por el servidor.

La evolución de las arquitecturas cliente / servidor es el resultado de cambios que han tenido lugar entre los requerimientos de los clientes, en tecnología y en la competencia.

2.1.3. Elementos de una Red

Entre los componentes básicos de una red tenemos: el servidor, las estaciones de trabajo, las tarjetas de conexión de red, el cableado, etc. Las características principales de estos elementos se explican a continuación.

El servidor

El servidor es una computadora utilizada para gestionar el sistema de archivos de la red, da servicio a las impresoras, controla las comunicaciones y realiza otras funciones.

Puede ser dedicado o no dedicado. La tarea de un servidor dedicado es procesar las peticiones realizadas por la estación de trabajo. Estas peticiones pueden ser de acceso a disco, a colas de impresión o de comunicaciones con otros dispositivos. La recepción, gestión y realización de estas peticiones puede requerir un tiempo considerable, que se incrementa de forma paralela al número de estaciones de trabajo activas en la red. Como el servidor gestiona las peticiones de todas las estaciones de trabajo, su carga puede ser muy pesada.

Se puede entonces llegar a una congestión, el tráfico puede ser tan elevado que podría impedir la recepción de algunas peticiones enviadas.

Cuanto mayor es la red, resulta más importante tener un servidor con elevadas prestaciones. Se necesitan grandes cantidades de memoria RAM para optimizar los accesos a disco y mantener las colas de impresión. El rendimiento de un procesador es una combinación de varios factores, incluyendo el tipo de procesador, la velocidad, el factor de estados de espera, el tamaño del canal, el tamaño del bus, la memoria caché, así como de otros factores.

En lo que se refiere al servidor no dedicado, es aquel en que a comparación del dedicado, su carga de trabajo es menor en cuanto a comunicación, ya que en con éste se puede interactuar con distintas aplicaciones sin alterar su funcionamiento. Por lo general este tipo de servidor se utiliza en redes pequeñas. También puede funcionar como una estación de trabajo, compartiendo al mismo tiempo sus recursos con otras computadoras. El sistema operativo de red es el que determina si se puede o no tener servidores no dedicados, sus capacidades y cantidad de servidores.

Por ejemplo: En el caso de dos servidores no dedicados y una estación de trabajo, la estación tendrá acceso a los recursos compartidos en los otros dos servidores, pero no podrá compartir sus recursos con ellos. Mientras que los servidores pueden compartir entre ellos sus recursos .

Estaciones de Trabajo

Las estaciones de trabajo se pueden conectar a través de la tarjeta de red y el cableado correspondiente. Estas estaciones por lo general son sistemas inteligentes que se encargan de sus propias tareas de procesamiento, por ello en cuanto mayor y más rápidas sean serán mejores.

Por otro lado, encontramos las terminales conocidas como tontas que son utilizadas en las redes, y no poseen capacidad propia de procesamiento, utilizando el espacio de almacenamiento así como los recursos disponibles en el servidor.

Existen otros elementos que componen a una red típica, tales como las tarjetas de interconexión, todas las variedades de cableado, etc. Desde luego, los dispositivos de comunicaciones representan también elementos de la conectividad para datos y voz (*hubs, switches, routers, bridges, gateways*, etc.); sin embargo, estos últimos elementos se detallan más adelante con la profundidad suficiente para sentar las bases requeridas en el diseño de la solución.

La figura 2.3. representa una red Ethernet con el medio compartido para diferentes servidores y sus estaciones de trabajo.

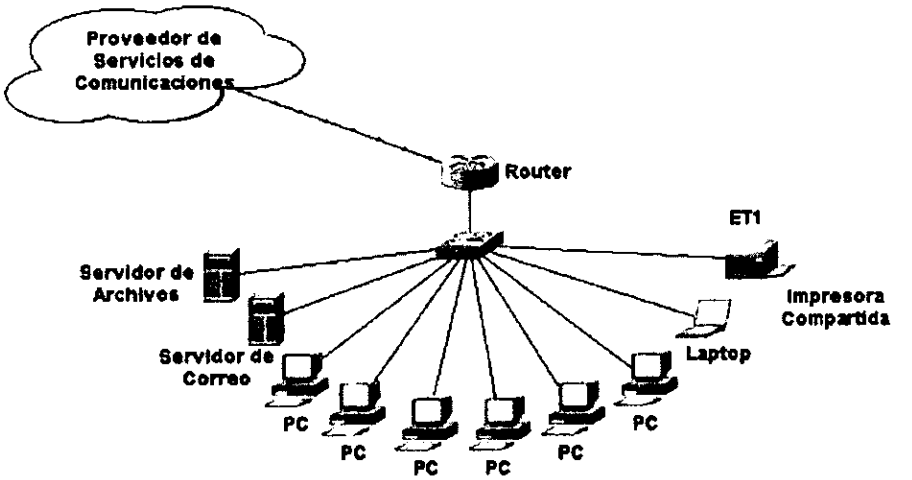


Figura 2.3. Arquitectura básica modelo cliente servidor.

2.1.4. Esquemas de red más usados

Los diferentes esquemas de red usados han ido evolucionando conforme las necesidades de las aplicaciones lo han demandado, al igual que la tecnología ha permitido desarrollar más velocidad de acceso. La mayoría de los mecanismos están basados en conexiones físicas que compiten por transmitir su información. Como se verá más adelante, los métodos de acceso pueden ser por contención del medio, o por reglas que controlan de forma determinística el turno que le corresponde a cada estación de trabajo para transmitir su información. Cabe mencionar que aunque existen tecnologías inalámbricas que operan bajo esquemas de saltos de frecuencias, éstas no serán cubiertas en el presente documento, ya que la implementación del proyecto en su totalidad estará constituida por redes alámbricas. Tomando como punto de partida el esquema de contención de redes, revisaremos las redes Ethernet como el antecedente por tradición con algunas de sus variantes, y terminaremos los esquemas con las redes de anillo tanto en cobre como en fibra óptica. Esto es, los esquemas de redes serán definidos desde un punto de vista del acceso al medio.

Contensión del medio (Ethernet)

La tecnología de acceso al medio por competencia es la forma más antigua en la que las redes de datos han intercambiado sus mensajes y su información. Al principio, la idea de interconectar recursos de cómputo tales como archivos y aplicaciones no representaba las demandas de nuestros días, por lo que la tecnología de los 60's usó cable coaxial grueso, cuya capacidad de velocidad estaba más que sobrada para compartir 100 equipos. Por lo mismo, el protocolo que ordenaba este intercambio se

basaba en el simple hecho de escuchar la transmisión presente en el medio y aguardar hasta que éste se desocupara. En ese sentido, las peticiones eran atendidas tan rápido que era raro que dos intentos de transmisión provenientes de estaciones distintas coincidieran; de forma tal que se aprovechaban esos eventos para controlar el acceso. La primera integración de este tipo de redes fue estandarizado por Digital, Intel y Xerox, en lo que se conoció como red Ethernet, y cuyo protocolo se nombró CSMA/CD. Este protocolo indicaba la autorización a transmitir desde una terminal siempre y cuando el medio (el "ether") estuviera libre de señales montadas en la portadora; esto es, el host o anfitrión detectaba ciertos niveles de voltaje y con base a umbrales predeterminados, transmitía, retransmitía o se inhibía hasta una nueva condición de medio libre. Velocidades típicas de este mecanismo eran 10 ó 1000 mbps.

Paso de testigo (Token Ring/FDDI)

En esta tecnología, las redes ofrecían una forma más eficiente de controlar el acceso al medio y formaron lo que se conoce como redes determinísticas, ya que permitían determinar de forma precisa el tiempo que le correspondía a una estación el enviar sus datos. Desde luego dentro del entramado de esta tecnología existían campos que permitían asignar prioridades, lo cual rompe con la rotación en *round-robin* de uno a la vez. El paso de testigo consiste básicamente en enviar un *token* (serie de bits) a lo largo de todo el anillo para asignar el turno de enviar información a quien lo requiera. Este mecanismo puede desarrollar velocidades de 8/16 Mbps y la versión de fibra óptica *FDDI (Fiber Data Distributed Interface, Interfaz de Datos Distribuidos por Fibra*) soporta hasta 100 mbps. Otra diferencia entre el modelo clásico de *Token Ring* y *FDDI* es la adecuación de dispositivos duales que permiten implementar redundancia, al igual que habilitan la circulación de diferentes *tokens* a lo largo del anillo para aprovechar los tiempos muertos entre la salida y la llegada de otros *tokens*.

Interconexión de Redes

Actualmente existe una gran variedad de redes no sólo por el número sino también por la diversidad de protocolos que ellas utilizan. Por tanto es necesario conocer la naturaleza de las distintas redes y los distintos protocolos cuando se desea establecer conexión entre ellas.

En general se pueden presentar los siguientes casos de conexión entre distintas redes.

- Red de área local con red de área local.
- Red de área local con red de área extensa
- Red de área extensa con red de área extensa
- Red de área local con red de área local a través de una red de área extensa.

La red puede aumentar sus capacidades, tanto de interoperatividad como de cobertura, o simplemente incrementar el número de estaciones conectadas mediante los siguientes dispositivos:

- Repetidores
- Puentes o Bridges
- Encaminadores o Ruteadores
- Pasarelas o Gateways

Tipos de Redes

Las redes según sea la utilización por parte de los usuarios pueden ser: compartida o exclusiva.

Redes dedicadas o exclusivas

Son aquellas que por motivo de seguridad, velocidad o ausencia de otro tipo de red, conectan dos o más puntos de forma exclusiva. Este tipo de red puede estructurarse en redes punto a punto o redes multipunto.

Redes punto a punto

Permiten la conexión en línea directa entre terminales y computadoras. La ventaja de este tipo de conexión se encuentra en la alta velocidad de transmisión y la seguridad que presenta al no existir conexión con otros usuarios. Su desventaja sería el precio muy elevado de este tipo de red.

Redes multipunto

Permite la unión de varios terminales a su correspondiente computadora compartiendo una única línea de transmisión. La ventaja consiste en el abaratamiento de su costo, aunque pierde velocidad y seguridad. Este tipo de redes requiere amplificadores y difusores de señal o de multiplexores que permiten compartir líneas dedicadas.

Redes compartidas

Son aquellas a las que se une un gran número de usuarios, compartiendo todas las necesidades de transmisión e incluso con transmisiones de otras naturalezas. Las redes más usuales son las de conmutación de paquetes y las de conmutación de circuitos.

Redes de conmutación de paquetes

Son redes en las que existen nodos de concentración con procesadores que regulan el tráfico de paquetes.

Paquete.- Es una pequeña parte de la información que cada usuario desea transmitir. Cada paquete se compone de la información, el identificador del destino y algunos caracteres de control.

Redes de conmutación de circuitos

Son redes en las que los centros de conmutación establecen un circuito dedicado entre dos estaciones que se comunican.

Redes digitales de servicios integrados(RDSI)

Se basan en desarrollos tecnológicos de conmutación y transmisión digital. La RDSI es una red totalmente digital de uso general capaz de integrar una gran gama de servicios

como son la voz, datos, imagen y texto. La RDSI requiere de la instalación de centrales digitales.

Las redes según los servicios que satisfacen a los usuarios se clasifican en:

Redes para servicios básicos de transmisión

Se caracterizan por dar servicio sin alterar la información que transmiten. De este tipo son las redes dedicadas, la red telefónica y las redes de conmutación de circuitos.

Redes para servicios de valor añadido

Son aquellas que además de realizar la transmisión de información, actúan sobre ella de algún modo. Pertenecen a este tipo de red las que gestionan mensajería, transferencia electrónica de fondos, acceso a grandes bases de datos, videotex, teletex, etc.

Las redes según el servicio que se realice en torno a la empresa puede subdividirse en:

Redes intra empresa

Son aquellas en las que el servicio de interconexión de equipos se realiza en el ámbito de la empresa.

Redes inter empresa

Son las que proporcionan un servicio de interconexión de equipos entre dos o más empresas.

Las redes según la propiedad a la que pertenezcan pueden ser:

Redes privadas

Son redes gestionada por personas particulares, empresas u organizaciones de índole privado. A ellas sólo tienen acceso los terminales de los propietarios.

Redes públicas

Son las que pertenecen a organismos estatales, y se encuentran abiertas a cualquier usuario que lo solicite mediante el correspondiente contrato.
Ejemplo: Redes telegráficas, redes telefónicas, redes especiales para transmisión de datos.

Las redes según la cobertura del servicio pueden ser:

Redes de área local (LAN)

Son redes que interconectan equipos dentro de un entorno físico reducido. En general no se extiende más allá de un edificio, recinto o campus.

Redes de área extensa (WAN)

Son las que unen equipos instalados en distintos edificios e inclusive en distintas ciudades. Utilizan normalmente enlaces de telecomunicación de la compañía telefónica.

Distribución y Topología de Redes

Topología de red es la forma en que se distribuyen los cables de la red para conectarse con el servidor y con cada una de las estaciones de trabajo.

La topología de una red es similar a un plano de la red dibujado en un papel, ya que se pueden tender cables a cada estación de trabajo y servidor de la red.

La topología determina donde pueden colocarse las estaciones de trabajo, la facilidad con que se tenderá el cable y el corte de todo el sistema de cableado.

La flexibilidad de una red en cuanto a sus necesidades futuras se refiere, depende en gran parte de la topología establecida. A continuación describiremos brevemente las diferentes topologías de red

Topología estrella

Se utiliza un dispositivo como punto de conexión de todos los cables que parten de las estaciones de trabajo. El dispositivo central puede ser el servidor de archivos en sí o un dispositivo especial de conexión. Ejemplo: Starlan de AT&T.

El diagnóstico de problemas es fácil, debido a que las estaciones de trabajo se comunican a través del equipo central. Los fallos en el nodo central son fáciles de detectar y es fácil cambiar los cables. La colisión entre datos es imposible, ya que cada estación tiene su propio cable, y resulta fácil ampliar el sistema.

En algunas empresas tienden a agruparse los cables en la unidad central lo cual puede ocasionar errores de gestión.

Topología Bus

El servidor y todas las estaciones están conectados a un cable general central. Todos los nodos comparten este cable y éste necesita acopladores en ambos extremos.

Las señales y los datos van y vienen por el cable, asociados a una dirección destino. Cada nodo verifica las direcciones de los paquetes que circulan por la red para ver si alguna coincide con la suya propia. El cable puede extenderse de cualquier forma por las paredes y techos de la instalación. Ejemplo: Ethernet y G-Net.

La topología bus usa una cantidad mínima de cable y el cable es muy fácil de instalar, ya que puede extenderse por un edificio en las mejores rutas posibles. Así el cable debe ir de equipo en equipo.

Las principales desventajas son: El cable central puede convertirse en un cuello de botella en entornos con un tráfico elevado, ya que todas las estaciones de trabajo comparten el mismo cable. Es difícil aislar los problemas de cableado en la red y determinar que estación o segmento de cable los origina, ya que todas las estaciones están en el mismo cable. Una rotura de cable hará caer el sistema.

Topología Anillo

Las señales viajan en una única dirección a lo largo del cable en forma de un bucle cerrado. En cada momento, cada nodo pasa las señales a otro nodo.
Con la topología en anillo, las redes pueden extenderse a menudo a largas distancias, y el coste total del cableado será menor que en una configuración en estrella y casi igual a la bus. Una rotura del cable hará caer el sistema. Actualmente existen sistemas alternativos que evitan que esto ocurra.

Topología Estrella / bus

Es una configuración híbrida. Aquí un multiplexor de señal ocupa la posición del dispositivo central. El sistema de cableado de la red puede tomar la topología bus o anillo. Esto ofrece ventajas en el cableado de edificios que tienen grupos de trabajo separados por distancias considerables.

Ejemplo: ARCNET. Ofrece gran flexibilidad para configurar la distribución de los cables y adaptarla a cualquier edifico.

2.2. Servicios de Red

En la labor cotidiana de una empresa generalmente se hace uso de los equipos de cómputo para realizar cálculos, manejar documentos, bases de datos, investigaciones por Internet, envío de correos y mucho más. El software que se ocupa para realizar todas esta clase de actividades se denomina "Software de Aplicaciones".

Normalmente necesitamos más de una aplicación para completar una tarea y tener poder de proceso, combinación de datos y controlar entradas y salidas de información. Los Servicios de Red permiten a los usuarios compartir estos recursos y aprovechar al máximo su utilidad en nuestro trabajo.

Muchas de las aplicaciones que proveen servicios de red son combinadas dentro de un Sistema Operativo de Red. Estos sistemas son creados para controlar, coordinar y proveer múltiples servicios de Red a otras computadoras de aplicaciones. Como tipos de servicio de red podemos mencionar los siguientes:

- Servicios de Archivos
- Servicios de Impresión
- Servicios de Mensajes
- Servicios de Aplicaciones

2.2.1. Servicios de Archivos

Los Servicios de Archivos son aplicaciones para almacenamiento, carga y movimiento de archivos. También sirven para: leer, escribir, controlar el acceso y la administración de datos, nos ayudan a mover rápidamente archivos de un lugar a otro, hacer respaldos de archivos importantes y usar eficientemente el hardware de almacenamiento, dicho de otra manera dentro de los servicios de archivos tenemos las siguientes facilidades:

- Transferencia de Archivos
- Almacenamiento y Migración de Datos
- Sincronización y Actualización de Datos

Transferencia de Archivos

La transferencia de archivos incluye: salvar, copiar y mover archivos de un cliente de la Red, para manejar eficientemente sus datos. Un usuario de la Red puede hacer copias o mover archivos en cuestión de segundos, evitando viajes o envíos postales que retrasan la información e incrementan los gastos por viáticos o valijas.

La transferencia de archivos puede hacerse con relativa facilidad a pesar de las largas distancias o el tamaño de los archivos.

Almacenamiento y Migración de Datos

El almacenamiento de datos en las computadoras puede ser de diferentes tipos: medios magnéticos u ópticos como disquetes, cintas magnéticas entre otros, como podemos ver en la figura 2.4

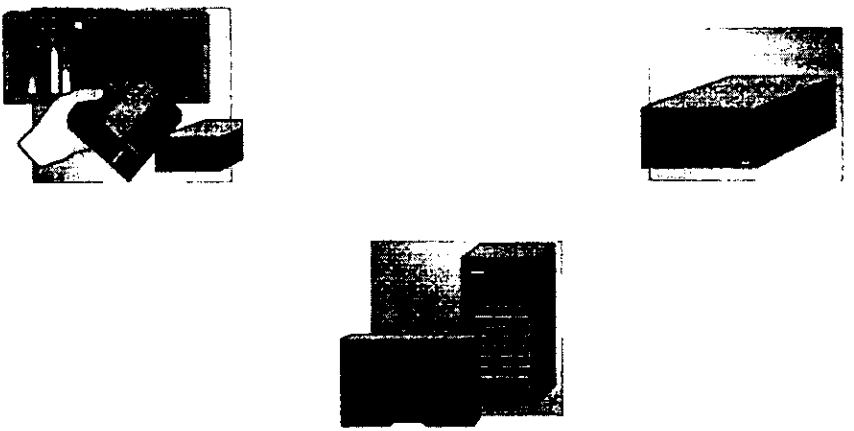


Figura 2.4. Dispositivos de almacenamiento comunes.

El uso eficiente de cada uno de los dispositivos de almacenamiento necesita administración continua. Las aplicaciones de Red son una excelente herramienta para controlar y gestionar las actividades de almacenamiento en diferentes sistemas de

respaldo. Para mejorar y reducir el tiempo de acceso, resguardo e integridad de los datos, almacenamos los archivos y usamos funciones de migración, con ellos todos los usuarios de la red pueden sacar provecho de los archivos con su computadora.

Sincronización y Actualización de Datos

Actualmente en los lugares de trabajo se ha incrementado el uso de computadoras móviles (*LapTops)* para aumentar la productividad de los empleados. Cuando el personal necesite trabajar con un archivo en particular, puede guardar una copia en el disco duro de su *LapTop* para cuando no esté conectado a la red. Por lo anterior, el mismo archivo ahora existe en dos lugares diferentes. El segundo al editarse, cambiará al original cuando sea salvado dentro del servidor. En este caso dicho archivo estará con fecha diferente.

El servicio encargado de identificar cambios en los archivos y administrar el proceso de actualización para mantener la integridad de los archivos, es conocido como servicio de actualización y sincronización de archivos. Lo anterior se puede ver en la figura 2.5.

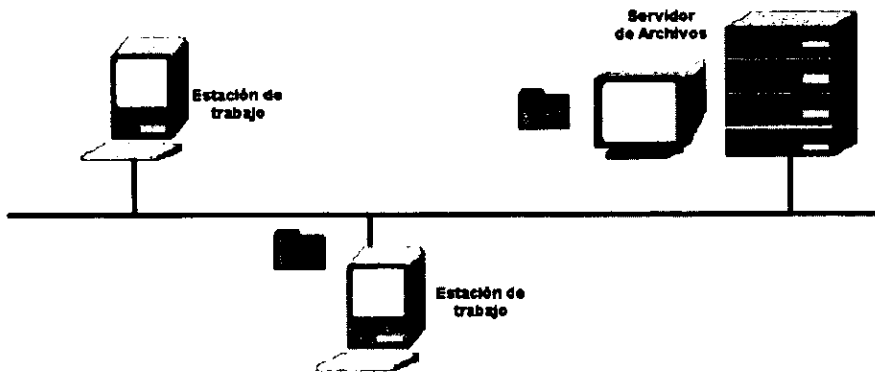


Figura 2.5. Sincronización de archivos.

2.2.2. Servicios de Impresión

Los servicios de impresión son aplicaciones de red que nos ayudan a controlar y administrar el acceso a impresoras de calidad, impresoras de color y faxes. Al usar un servicio de impresión podemos reducir el número de impresiones, administrar colas de impresión por prioridades, reducir los tiempos de espera de impresiones enviadas, compartir impresoras especializadas, etc.

Los funciones de estos servicios incluyen:

- Provisión de accesos múltiples desde interfaces limitadas.
- Manejo simultaneo de requisiciones y encolamiento de estas mismas.
- Servicios de impresión distribuida.

- Impresoras compartidas.

Provisión de accesos múltiples desde interfaces limitadas

Normalmente en las empresas, sólo dos o tres computadoras pueden conectarse a una impresora. Con los servicios de impresión en red, todo un grupo de usuarios puede enviar sus documentos a un mismo impresor, por medio de un servidor o un software que retenga los trabajos en una cola de impresión. Al disminuir el número de equipos de impresión, una empresa reduce considerablemente sus gastos por conceptos de equipos múltiples, pólizas de servicio, consumibles y la cantidad de proveedores, que facilita la administración del activo fijo de la compañía. Figura 2.26.

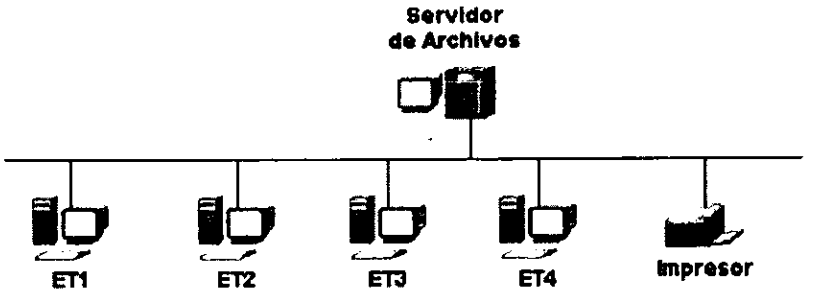


Figura 2.6. Impresión en Ambiente de Red.

Manejo simultáneo de requisiciones y encolamiento de estas mismas

En un grupo de trabajo mediano o grande dentro de una empresa, es normal que más de una persona envíe documentos a impresión. En este caso, los archivos compiten por las limitantes del impresor para aceptar y atender todos los requerimientos. El encolamiento de documentos resuelve este cuello de botella. Una cola de impresión captura y atiende todos los trabajos de impresión de un grupo de personas y puede retenerlos, darles prioridad y administrarlos. Es común que los proveedores de servicios de impresión ofrezcan encolamiento de documentos. Esto lo podemos ver en la figura 2.7. Cuando usamos servicios de impresión en red, los documentos enviados a impresión llegan a la cola de impresión y son retenidos en ella, hasta que la impresora está lista para atenderlos e imprimirlos.

Servicios de impresión Distribuida

Los servicios de impresión distribuida ofrecen grandes mejoras en los sistemas de impresión por colas de impresión. Algunos de estos son:

- Descarga e instalación automática de *drivers (manejadores)*
- Integración con servicios de directorios
- Administración centralizada y simplificada

Impresoras Compartidas

Existen impresoras para usos específicos con gran velocidad de salida, impresión de alta calidad, impresión a color. Equipo que normalmente es caro y por ello se requiere un control más estricto. La opción de conectividad en red a estos equipos reduce comúnmente los gastos por usuario y optimiza el uso del impresor.

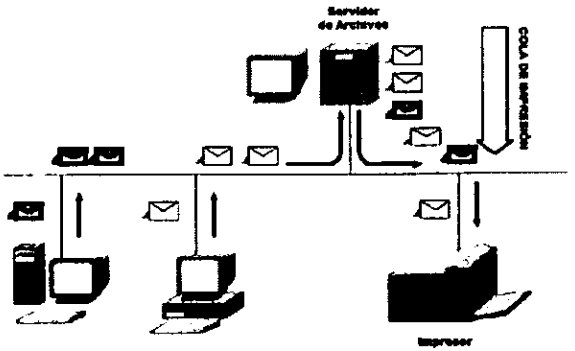


Figura 2.7. Encolamiento de archivos enviados a impresión.

2.2.3. Servicios de Mensajes

Actualmente en todas las empresas se requieren servicios tales como: almacenamiento y acceso de archivos, gráficos, video digitalizado y datos de voz en sus labores cotidianas. Son estos Servicios los que intentaremos describir en esta parte del documento. Los servicios de Mensajes nos ayudan a: intercambiar notas y archivos generados por computadoras, enviar correo electrónico integrado con sistemas de correo de voz, direccionar y compartir datos, organizar y mantener directorios de información de dispositivos y usuarios. Esto lo podemos observar en la figura 2.8.

A continuación trataremos las siguientes aplicaciones de mensajes:

- Correo electrónico.
- Correo electrónico integrado con sistemas de correo de voz.
- Aplicaciones para grupos de Trabajo

Correo electrónico

El servicio de correo electrónico o *E-mail* es el intercambio electrónico de mensajes de datos entre dos o más computadoras conectadas en red. Los mensajes de *E-mail* incluyen una variedad de texto digital, gráficos, datos de audio y video. Existe software que ofrece herramientas de transporte y presentación de documentos en una amplia gama de formatos.

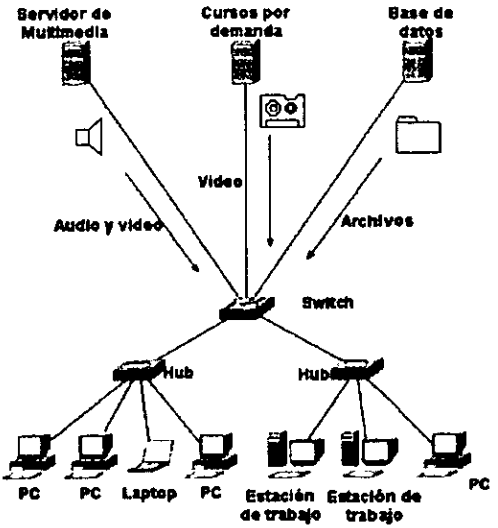


Figura 2.8. Servicios de video, voz y datos en red.

Correo electrónico integrado con sistemas de correo de voz

Los sistemas de administración de red pueden combinarse con algunos servicios de correo o localización, para alertar a los administradores de red cuando existen condiciones críticas en las redes o en los dispositivos que la componen. Los servicios de mensajes que integran correo electrónico y correo de voz pueden también agregarse, ya que existen equipos especializados de cómputo que son compatibles con los servidores y computadoras de la red. Estos dispositivos se tocarán con más detalle en la sección cuatro de este documento.

Aplicaciones para grupos de trabajo

Los servicios de mensajes incluyen también las aplicaciones de administración de grupos de trabajo, conocidas también como aplicaciones para la administración del flujo de trabajo. Estas aplicaciones pueden enrutar formas, noticias, y documentos a los clientes de la red. Proveen también manejo de procesos distribuidos y multiusuarios.

2.2.4. Servicios de Aplicaciones

Los servicios de aplicaciones son servicios de red que permiten a los usuarios de la red ejecutar software. Estos servicios difieren de los servicios de archivos porque permiten a las computadoras compartir su poder de procesamiento, no sólo compartir datos.

Coordinar *hardware* y *software* para ejecutar utilerías en plataformas mas apropiadas e incrementar la capacidad de *hardware* especializado sin la necesidad de actualizar cada computadora de la red, son tareas de los servicios de aplicaciones.

Las funciones de los servicios de aplicaciones de red incluyen:

- Especialización de servidores
- Escalabilidad y crecimiento

Especialización de servidores

Estas aplicaciones emplean equipos especializados y utilerías o software para incrementar velocidad, conservar la integridad de datos y mantener seguridad en los datos. Normalmente los servidores de aplicaciones tienen mejor desempeño de proceso que las estaciones de trabajo comunes, ya que cuentan con sistemas operativos más eficientes que mejoran y optimizan el rendimiento de operaciones especializadas o especificas.

Un ejemplo de servidor de aplicaciones es un *PBX (Private Branch eXchange, Conmutador)* que es una computadora que provee servicios de conmutación telefónica.

Escalabilidad y crecimiento

Los servicios de escalabilidad proporcionan a las empresas grandes ahorros, porque permiten la no sustitución de equipos especializados, donde comúnmente se requiere poder y velocidad de procesamiento.

Un claro ejemplo en las empresas es cuando se compra *software* para una aplicación especifica, pero al paso del tiempo, el proceso de la computadora donde inicialmente funcionaba correctamente se va haciendo lento y más lento. Podemos en este caso incrementar el tiempo de respuesta cambiando el dispositivo de cómputo por uno más poderoso o compartiendo el proceso con otro servidor, mientras la primer computadora funciona sin problemas. Los beneficios de la escalabilidad y crecimiento dependen de la habilidad para usar un mismo sistema operativo en una computadora nueva o de soportar la misma aplicación en otro sistema operativo.

2.3. Medios de Transmisión

El medio de transmisión es el ente que nos permite transportar o conducir la información de un punto a otro, como tal es uno de los elementos fundamentales para la implementación de una red.

Existeń varios tipos de medios de transmisión que poseen distintas características físicas, las cuales son aprovechadas en diversos tipos de redes y en diferentes espacios físicos. Cada tipo de medio de transmisión posee ventajas y desventajas sobre los demás medios, que con el tiempo se han acrecentado o disminuido ante el avance tecnológico e introducción de materiales mejorados y nuevos.

2.3.1. Medios de transmisión más comunes

Actualmente existe una variedad de medios de transmisión que son utilizados de acuerdo a las necesidades y los recursos disponibles de aquellos que requieren de una red, sin embargo dentro de esa variedad de medios de transmisión existen algunos que son frecuentemente utilizados y que consideramos adecuado mencionarlos de acuerdo a su clasificación en :

Alámbricos: par trenzado, cable coaxial, fibra óptica.
Inalámbricos: radio, microondas, infrarrojo.

A continuación describiremos cada uno de ellos.

2.3.2. Medios de Transmisión Alámbricos e Inalámbricos

Los medios de transmisión alámbricos también son llamados cables. Son los medios que físicamente tienen forma definida y visible.
Los medios de transmisión inalámbricos no son visibles y de forma física no definida, y no se observa una ruta física en la transmisión. A continuación se explicaran con más detalle cada uno de los dos tipo de medios de transmisión.

Medios Alámbricos

Dentro de los medios de transmisión alámbricos encontramos una gran variedad de medios, que van desde el uso del cobre sin *blindaje UTP (Unshielded Twisted Pair, Par Trenzado Sin Blindaje)* o con blindaje STP *(Shielded Twisted Pair, Par Trenzado Blindado)*, pasando por el cable coaxial y terminando con la fibra óptica, las cuales se detallan a continuación.

Par Trenzado

Se trata de dos hilos de cobre aislados y trenzados entre sí, y en la mayoría de los casos cubiertos por una malla protectora. Los hilos están trenzados para reducir las interferencias electromagnéticas con respecto a los pares cercanos que se encuentran a su alrededor (dos pares paralelos constituyen una antena simple, en tanto que un par trenzado no). Se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende de la sección de cobre utilizado y de la distancia que tenga que recorrer. Se trata del cableado más económico y la mayoría del cableado telefónico es de este tipo. Presenta una velocidad de transmisión que depende del tipo de cable de par trenzado que se esté utilizando. El cable de par trenzado está dividido en categorías:

- **Categoría 1**: Hilo telefónico trenzado de calidad de voz, no adecuado para las transmisiones de datos. Velocidad de transmisión inferior a 1 Mbits/seg
- **Categoría 2** : Cable de par trenzado sin apantallar. Su velocidad de transmisión es de hasta 4 Mbits/seg.
- **Categoría 3** : Velocidad de transmisión de 10 Mbits/seg, con este tipo de cables se implementa las redes Ethernet 10-Base-T
- **Categoría 4** : La velocidad de transmisión llega a 16 Mbits/seg.
- **Categoría 5** : Puede transmitir datos hasta 100 Mbits/seg.

Un par trenzado tiene una longitud máxima limitada y a pesar de los aspectos negativos es una opción a tener en cuenta debido a que ya se encuentra instalado en muchos edificios como cable telefónico lo cual permite utilizarlo sin necesidad de realizar alguna obra de adecuación en las instalaciones. Además resulta fácil de combinar con otros tipos de cables para la extensión de redes. La figura 2.9. muestra el aspecto del cable o par trenzado.

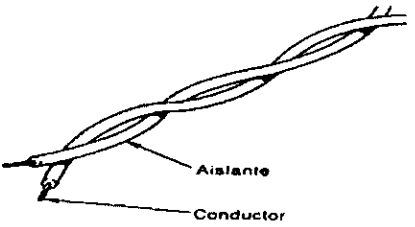


Figura 2.9. Cable de par trenzado.

Cable Coaxial

Consiste en un núcleo de cobre rodeado por una capa aislante. A su vez, esta capa está rodeada por una malla metálica que ayuda a bloquear las interferencias; este conjunto de cables está envuelto en una capa protectora. Cabe señalar que emite señales que pueden detectarse fuera de la red. Este tipo de cable es utilizado generalmente para señales de televisión y para transmisiones de datos a alta velocidad, a distancias de varios kilómetros. La velocidad de transmisión suele ser alta, de hasta 100 Mbits/seg; pero hay que tener en cuenta que a mayor velocidad de transmisión, menor distancia podemos cubrir, ya que el periodo de la señal es menor, y por tanto se atenúa antes.

La nomenclatura de los cables coaxiales Ethernet tiene 3 partes, que son ejemplificadas en la tabla 2.3.

- La primera indica la velocidad en Mbits/seg.
- La segunda indica si la transmisión es en Banda Base (BASE) o en Banda Ancha (BROAD).
- La tercera los metros del segmento multiplicados por 100.

CABLE	CARACTERÍSTICAS
10-BASE-5	Cable coaxial grueso (Ethernet grueso). Velocidad de transmisión : 10 Mb/seg. Segmentos: máximo de 500 metros.
10-BASE-2	Cable coaxial fino (Ethernet fino). Velocidad de transmisión : 10 Mb/seg. Segmentos: máximo de 185 metros.
10-BROAD-36	Cable coaxial Segmentos: máximo de 3600 metros. Velocidad de transmisión: 10 Mb/seg. Segmentos: máximo 195 metros
100-BASE-X	Fast Ethernet. Velocidad de transmisión: 100 Mb/seg. Segmentos: máximo de 5000 metros Máximo: 50 metros

Tabla 2.1. Nomenclatura Cable Coaxial.

A continuación se ilustra como está constituido un cable coaxial , podemos notar la capa protectora que rodea al conductor como tal, existen gran variedad de cables en el mercado , de diferentes calibre y calidades. La señal viaja por el medio de cobre mientras que la tierra en conducida por la malla externa, estos se encuentran aislados entre si.

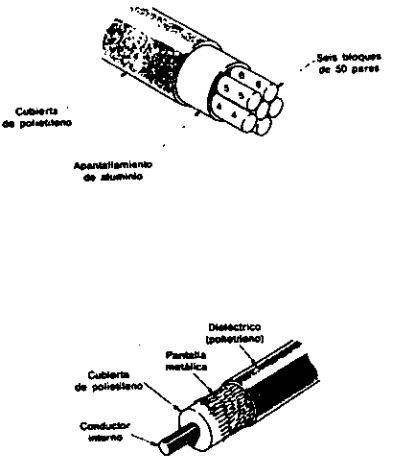


Figura 2.10. Estructura típica de un cable coaxial.

Fibra óptica

Una fibra óptica es un medio de transmisión de la luz que consta básicamente de dos cilindros coaxiales de vidrio transparentes y de diámetro muy pequeño. El cilindro interior se denomina núcleo y el exterior se denomina envoltura, siendo el índice de refracción del núcleo algo mayor que el de la envoltura.

En la superficie de separación entre el núcleo y la envoltura se produce el fenómeno de reflexión total de la luz, al pasar éste de un medio a otro que tiene un índice de refracción más pequeño. Como consecuencia de esta estructura óptica todos los rayos de luz que se reflejan totalmente en dicha superficie se transmiten guiados a lo largo del núcleo de la fibra.

El conjunto mencionado está envuelto por una capa protectora. La velocidad de transmisión es de 10 Mb/seg, siendo en algunas instalaciones especiales de hasta 500 Mb/seg, y no resulta afectado por interferencias.

Los cables de fibra óptica tienen muchas aplicaciones en el campo de las comunicaciones de datos:

- Conexiones locales entre computadoras y periféricos o equipos de control y medición.
- Interconexión de computadoras y terminales mediante enlaces dedicados de fibra óptica.
- Enlaces de fibra óptica de larga distancia y gran capacidad.

Los cables de fibra óptica ofrecen muchas ventajas respecto de los cables eléctricos para transmitir datos:

- Mayor velocidad.
- Mayor capacidad.
- Inmunidad ante interferencias electromagnéticas.
- No existen problemas de retorno de tierra.
- La atenuación se incrementa lentamente conforme a la distancia.
- Tasas de error del orden de 1 en 10^9.
- No hay riesgo de cortocircuito.
- Son de menor diámetro, flexibles y de fácil instalación.
- Resistencia al medio ambiente.
- Es difícil realizar drenados de datos sin que se tenga conocimiento de la acción.

La mayor desventaja es que no se puede "pinchar" fácilmente este cable para conectar un nuevo nodo a la red..

Las transmisiones de la señal a grandes distancias se encuentran sujetas a atenuación, que consiste en una pérdida de amplitud o intensidad de la señal, lo que limita la longitud del cable. Los segmentos pueden ser de hasta 2000 metros, la figura 2.11. muestra como viaja el haz a través de la fibra.

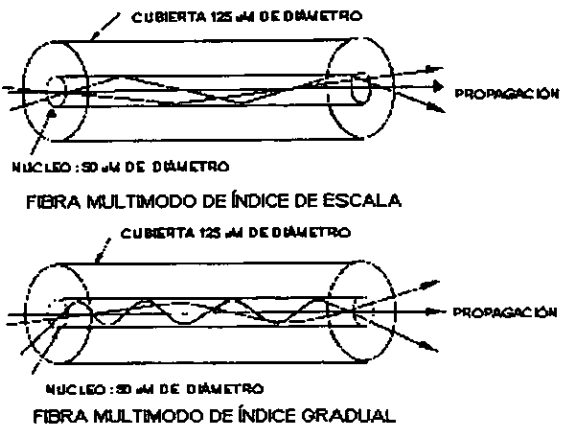


Figura 2.11. Propagación multimodo en una fibra óptica.

Medios inalámbricos

Enlaces ópticos al aire libre

El principio de funcionamiento de un enlace óptico al aire libre es similar al de un enlace de fibra óptica, sin embargo el medio de transmisión no es un polímero o fibra de vidrio sino el aire, un ejemplo se muestra en la figura 2.12.

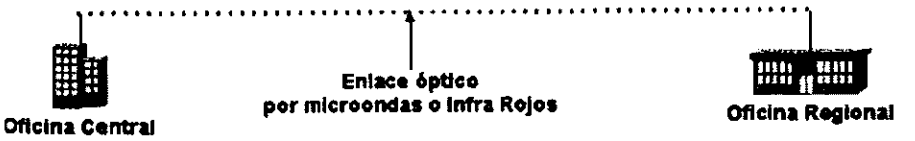


Figura 2.12. Enlace óptico al aire libre.

El emisor óptico produce un haz estrecho que se detecta en un sensor que puede estar situado a varios kilómetros en la línea de visión. Las comunicaciones ópticas al aire libre son una alternativa de gran ancho de banda a los enlaces de fibra óptica o a los cables eléctricos. Las prestaciones de este tipo de enlace pueden verse empobrecidas por la lluvia fuerte o niebla intensa, pero son inmunes a las interferencias eléctricas y no necesitan permiso de las autoridades responsables de las telecomunicaciones.

Las mejoras en los emisores y detectores ópticos han incrementado el rango y el ancho de banda de los enlaces ópticos al aire libre, al tiempo que reducen los costos. Se puede permitir voz o datos sobre estos enlaces a velocidades de hasta 45 Mbits/s. El límite para comunicaciones fiables se encuentra sobre los dos kilómetros. Para distancias de más de dos kilómetros son preferibles los enlaces de microondas.

Microondas

Los enlaces de microondas se utilizan mucho como enlaces donde los cables coaxiales o de fibra óptica no son prácticos. Se necesita una línea de visión directa para transmitir en la banda de *SHF (Super High Frecuency, Super Alta Frecuencia)*, de modo que es necesario disponer de antenas de microondas en torres elevadas en las cimas de las colinas o accidentes del terreno, para asegurar un camino directo con la intervención de pocos repetidores.

Las bandas de frecuencias más comunes para comunicaciones mediante microondas son las de 2, 4, 6 y 6.8 GHz. Un enlace de microondas a 140 Mbits/s puede proporcionará hasta 1920 canales de voz o bien varias comunicaciones de canales de 2 Mbits/s multiplexados en el tiempo.

Los enlaces de microondas presentan unas tasas de error en el rango de 1 en 10^5 a 1 en 10^{11}, dependiendo de la relación señal/ruido en los receptores. También pueden presentarse problemas de propagación en los enlaces de microondas, incluyendo los debidos a lluvias intensas que provocan atenuaciones que incrementan la tasa de errores. Pueden producirse pequeños cortes en la señal recibida cuando una bandada de pájaros atraviesa el haz de microondas, pero es poco frecuente que ocurra.

Luz Infrarroja

Permite la transmisión de información a velocidades muy altas: 10 Mbits/seg. Consiste en la emisión/recepción de un haz de luz, por esto, el emisor y receptor deben tener

contacto visual (la luz viaja en línea recta). Debido a esta limitación pueden usarse espejos para modificar la dirección de la luz transmitida.

Señales de Radio

Consisten en la emisión/recepción de una señal de radio, por lo tanto el emisor y el receptor deben sintonizar la misma frecuencia. La emisión puede traspasar muros y no es necesaria la visión directa entre emisor y receptor.

La velocidad de transmisión suele ser baja: 4800 kbits/seg. Se debe tener cuidado con las interferencias de otras señales.

Comunicación vía satélite

Un satélite de comunicaciones hace la labor de repetidor electrónico. Una estación terrena A transmite al satélite señales de una frecuencia determinada (canal de subida). Por su parte, el satélite recibe estas señales y las retransmite a otra estación terrena B mediante una frecuencia distinta (canal de bajada). La señal de bajada puede ser recibida por cualquier estación situada dentro del cono de radiación del satélite, y puede transportar voz, datos o imágenes de televisión. De esta manera se impide que los canales de subida y de bajada se interfieran, ya que trabajan en bandas de frecuencia diferentes.

La capacidad que posee un satélite para recibir y retransmitir se debe a un dispositivo conocido como transpondedor. Los transpondedores de satélite trabajan a frecuencias muy elevadas, generalmente en la banda de los gigahertz. La mayoría de los satélites de comunicaciones están situados en una órbita denominada geoestacionaria, que se encuentra a 36,000 km sobre el ecuador. Esto permite que el satélite gire alrededor de la tierra a la misma velocidad que ésta, de modo que parece casi estacionario. Así, las antenas terrestres pueden permanecer orientadas hacia una posición relativamente estable (lo que se conoce como "sector orbital") ya que el satélite mantiene la misma posición relativa con respecto a la superficie de la tierra.

2.4. Dispositivos de comunicaciones

La necesidad de lo que se conoce como conectividad inició con la simple idea de compartir recursos, desde archivos hasta impresoras o periféricos de los más diversos tipos y para la mayoría de las aplicaciones. Un ejemplo que hace patente esta idea es el *switch* AB, que permitía compartir impresoras en una especie de multiplexión por eventos, y en la que el uso de un impresor era asignado por turnos y el equipo no podía liberarse para otro usuario hasta que no terminara de procesarse un trabajo en el *buffer*.

Para poder desarrollar un tema que describiera los elementos de comunicaciones en redes de computadoras necesitamos las bases teóricas de los medios de transmisión, para después eslabonar las interfaces de cada medio con cada equipo. En el apartado 2.3, se describieron los medios de transmisión más comunes para hacer posible la comunicación entre computadoras. En esta sección tocaremos el tema de los elementos que conectan estos medios con las computadoras o en general, con otros equipos de comunicaciones. Además, daremos una visión global de los dispositivos que hacen posible las comunicaciones en una base local, pero también en una base

geográficamente más amplia, poniendo un particular interés en los enrutadores (o ruteadores) porque será a través de ellos por donde se llevarán los multiservicios de esta red.

2.4.1. Conectores

Podemos definir a los conectores como los elementos mecánicos, que bajo ciertas normas reciben y preparan las señales (principalmente eléctricas, aunque también pueden ser ópticas), pero que en ningún momento interpretan a las mismas. Este punto es muy importante y tiene que ver con conceptos de señal, mensaje, codificación y transmisión. Por el momento, basta con señalar que los conectores están basados en estándares o normas simplemente para asegurar la interoperabilidad entre todos los fabricantes en aspectos mecánicos y opto-eléctricos, no así en procedimientos o funcionalidad que dependen de las reglas o protocolos que se implementen en capas superiores (referenciadas al modelo *OSI, Open System Interconection*). La mayoría de los estándares pueden dividirse en dos grandes ramas: de jure y de facto, la primera se refiere a aquellos estándares que se desarrollaron como resultado de una teoría de común acuerdo entre varios fabricantes de tecnologías. Por su parte, los estándares de facto, son consecuencia del uso difundido (y a la vez probado) de un solo fabricante, pero que por su alta funcionalidad ha sido adoptado por los demás fabricantes sin que haya existido un foro de diseño que lo antecediera. Un ejemplo de este tipo de estándares sería el de los modems que aceptan comandos AT, los cuales son propietarios de los modems Hayes. En la tabla 2.4. se resumen algunas de las características principales que poseen los conectores usados para enlaces WAN.

Estándar	***Asociación que avala la norma***	***# terminales del conector***
EIA/TIA 232	Asociación de Industrias de Telecomunicaciones	25
EIA/TIA 449	Asociación de Industrias de Telecomunicaciones	37
EIA/TIA 530	Asociación de Industrias de Telecomunicaciones	25
V.35	Unión Internacional de Telecomunicaciones	34
X.21	Unión Internacional de Telecomunicaciones	15

Tabla 2.2. Estándares de interfaces WAN.

2.4.2. Tarjetas de red

No obstante que las normas mencionadas competen solo a interfaces *WAN*, no podemos dejar de mencionar a las tarjetas de red o *NICs (Network Interface Cards, Tarjetas de Interfaz de Red)* que conforman quizás el componente más conocido de las redes en forma general. En el contexto de redes de computadoras, las tarjetas de red deben integrarse a los equipos de cómputo como un periférico mas que obedece a la

arquitectura propia de cada sistema que soporta a dicha tarjeta. Siguiendo los lineamientos de la tecnología clásica en la manufactura de equipos de cómputo, las tarjetas de red deben formar parte del *bus* principal de datos y un área de memoria reservada para las interrupciones que use el procesador central y bajo las cuales haga las llamadas correspondientes a las *NICs*. De esto último se deriva la necesidad de la interacción entre el *hardware (NICs)* y el *software* (*Drivers* o *controladores*) de forma tal que las peticiones de transmisión y recepción de datos en los puertos de comunicaciones se lleven a cabo de la forma más óptima posible.

El estudio de las tarjetas de red lo podemos dividir en pequeñas secciones que identifican las funciones que realizan estas tarjetas, cubren los aspectos más importantes de su configuración, detallan los tipos de transceptores existentes, explican la compatibilidad con los canales de datos en cada sistema y mencionan NICs especializados.

Funciones básicas: Prácticamente, las tarjetas de red como cualquier otro periférico tienen una función específica, que se relaciona con el sistema central y que se encarga de transmitir y recibir información binaria, ya sea por medios eléctricos o medios ópticos. En particular, las *NICs* recogen la información del sistema central en forma paralela, proveniente del *bus* de datos y la lanzan en forma serial a semejanza de un dispositivo *UART (Universal Asynchronous Receiver Transmitter, Transmisor Receptor Universal Asíncrono)*, valiéndose de pequeños depósitos de memoria con los cuales serializan la información. La figura 2.13. muestra este proceso de forma esquemática.

Desde luego que antes de que la información salga en forma de bits por algún tipo de serializador, las tramas (*frames*) que se enviarán deben poseer un formato en especial y el cual está determinado por el protocolo de capa 2 que se esté implementando. Dicho protocolo está relacionado estrechamente con el medio al que se conecta la tarjeta y opera bajo un direccionamiento físico que se conoce como dirección *MAC (Media Access Control)*. Los detalles de este direccionamiento están cubiertos en la descripción del modelo *OSI* de comunicaciones, pero con relación al uso de *NICs*, estas direcciones están contenidas de forma intrínseca en dichas tarjetas en forma de EEPROMs (*Electrically Ereasable Programable Memory, Memoria Programable y Borrable Eléctricamente*) y es por eso que a veces se les conoce como *BIA (Burn In Address, Quemado en Dirección)*. Dentro del mecanismo con el cual las tarjetas intercambian mensajes, éstas deben ser capaces de interpretar tanto mensajes individuales como mensajes de grupo.

Otro tipo de tarjetas que se manejan como dispositivos de conectividad son las tipo tranceptores que se describen a continuación:

Los transceptores son la interfaz física a la cual se conecta el medio de transmisión y pueden ser construidos en la misma tarjeta principal del sistema principal o bien de forma externa. Los primeros son una versión moderna de los equipos de cómputo actuales en donde la integración de comunicaciones es una necesidad y por la cual las tarjetas ya vienen integradas, presentando un puerto *RJ-45* o un puerto *BNC* en la parte posterior de los equipos. La fabricación tradicional de los transceptores hacía uso de las interfaces *AUI (Attachment Unit Interface, Unidad Interface de Adjuntado)*, tanto en los equipos de comunicaciones como en los equipos terminales; y éste consta de un puerto *DB-15* en forma de "D" del tipo hembra, parecido a un puerto de juegos para

computadora. A este puerto se conecta el transceptor que convierte la interfaz para conectar un medio de coaxial, fibra o UTP.

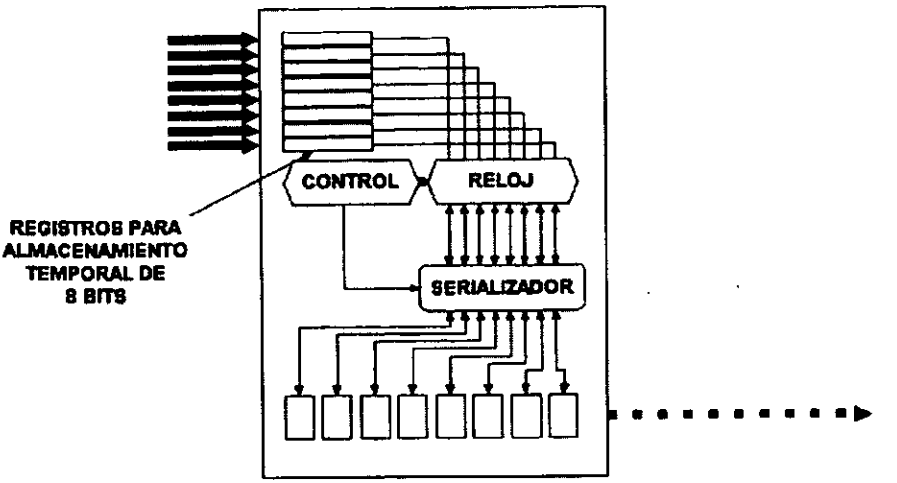


Figura 2.13. Proceso de conversión de datos de paralelo a serial.

2.4.3. Modems

Los modems son los equipos de comunicaciones usados para modular señales digitales en señales analógicas y poder transportar la información en líneas telefónicas convencionales. De hecho, la palabra modem es la unión de las palabras modular y demodular; ya que los modems efectivamente realizan ambas operaciones dependiendo del flujo de la información. La figura 2.14. muestra un esquema básico del uso de los modems en ambos extremos de la comunicación.

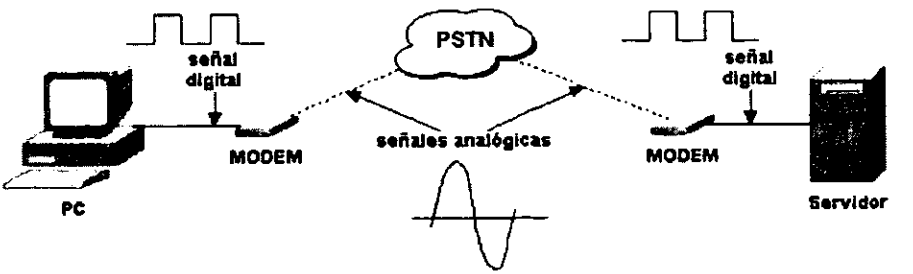


Figura 2.14. Los modems modulan información digital en líneas analógicas.

Así mismo, los modems pueden ser tanto internos como externos; siendo los primeros implementados en tarjetas parecidas a las tarjetas de red antes mencionadas y que se conectan mediante interfaces *ISA* o *PCI* al *bus* central. Por su parte, los modems externos se conectan a la *PC* mediante un cable serial *RS-232C* en *DB-9* hembra. La

conexión a la red pública conmutada se hace por medio de un conector *RJ-11* o telefónico que no es mas que una línea convencional que puede alcanzar velocidades de hasta 33,600 kbps con la norma v.36bis y de hasta 56 kbps con la norma v.90. Los datos completos de las normas más usadas se muestran en la tabla 2.3.

Estandar V	Tasa de transmisión
v.22	1200 bps
v.22 bis	2400 bps
v.32	4800 – 9600 bps
v.32 bis	4800 – 14400 bps
v.34	2400 – 28800 bps
*v.fc	2400 – 28800 bps
*v.fast	2400 – 28800 bps

**No son normas avaladas por la ITU-T, son propietarias.*

Tabla 2.3. Estándares V con tasa de transmisión

Otro punto a tratar en el estudio de los modems es el tipo de transmisión bajo el cual operan los mismos. Los modems pueden trabajar mediante transmisión síncrona o asíncrona. La transferencia síncrona se basa en la coordinación de los relojes de los dispositivos de comunicación y en donde se designa a un reloj maestro y a un reloj esclavo para poder alcanzar velocidades de transmisión muy altas. La comunicación asíncrona alcanza velocidades relativamente bajas debido al esquema de envío de caracteres con el cual trabaja. La comunicación asíncrona debe reconocer patrones en los bytes o caracteres de información para determinar si se trata de un carácter de inicio, de paro, de paridad, etc.; esto es lo que consume más tiempo y por lo mismo incrementa los tiempos de retardo.

El resto de los equipos de comunicaciones que quedan por analizar, a excepción de los conmutadores telefónicos, se revisarán de forma tal que se puedan mapear a una de las capas del modelo OSI, sin adentrarse en los aspectos específicos de la capa que se trate. En la mayoría de los casos, es fácil recordar las funciones que realiza cada uno de los equipos por las propiedades más notorias de cada capa del modelo *OSI*. De esta forma, podemos empezar a describir los equipos empezando por la capa más baja y subiendo hasta la capa de red, lo cual analizaremos con más detalle en el siguiente capítulo.

2.4.4. Repetidores

Los repetidores son dispositivos que reproducen la señal que los alimenta y la mandan hacia los demás puertos que posea, excepto el puerto por el que entró la señal. Es importante hacer notar que hay una diferencia entre repetidores y amplificadores, ya que estos también reproducen la señal que los alimenta con elementos activos (amplificadores operacionales, transistores, etc.), pero en todo momento se tratan de señales analógicas; mientras que los repetidores reproducen señales digitales. La figura 2.15. muestra este hecho haciendo la comparación entre amplificadores y repetidores.

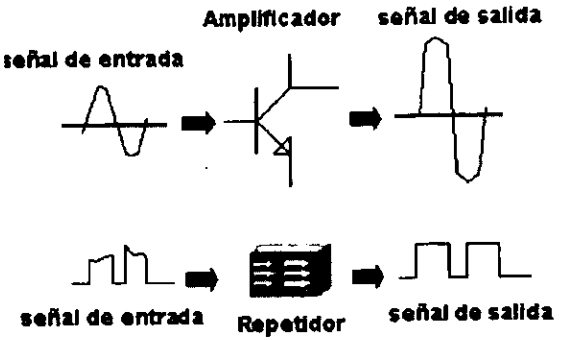


Figura 2.15. Diferencias entre amplificadores y repetidores.

La intención de los repetidores es tomar una señal digital débil y restaurarla para el próximo dispositivo. La funcionalidad del repetidor es la expansión de distancia que representa este dispositivo.

2.4.5. Concentradores (Hubs)

Los concentradores son elementos de comunicación que juegan un papel importante en las topologías de las redes locales, ya que se ubican en el punto central de las acometidas de los puertos de comunicaciones, y reparten los servicios comúnmente hacia los equipos terminales de usuarios. Existen dos tipos de concentradores: los pasivos y los activos. Los pasivos son equipos que sólo pueden retransmitir la información recibida en un puerto a los puertos restantes, y la mejor simbología está dada por un segmento de red Ethernet; aunque también existen concentradores para redes de anillo *(Token Ring)*, conocidos como *MSAU(Multiple Stations Access Unit, Unidades de Acceso a Múltiples Estaciones)*. La figura 2.16. muestra una conexión típica de equipos a un concentrador en red Ethernet.

Los concentradores activos presentan una variación importante en la expansión de las redes, sobre todo cuando se trata de cobre. Esta norma establece el alcance de 100m, en conexiones punta a punta; sin embargo, con los concentradores activos, los 100m de norma pueden extenderse a 100m de cada lado del concentrador en conexiones punta a punta. En general, los concentradores modernos pueden venir en presentaciones que interconecten puertos *RJ-45*, (lo más común) pero con puertos *BNC* para cable coaxial delgado.

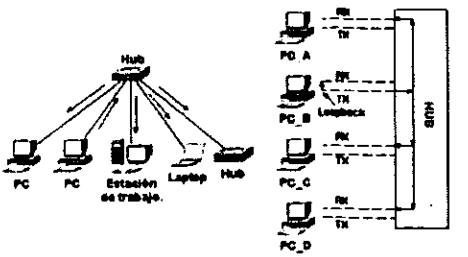


Figura 2.16. Conexión típica de concentradores.

2.4.6. Bridges

Los puentes son dispositivos de comunicación que permiten segmentar las redes con base a la cantidad de puertos de que dispongan. Estos equipos tienen la capacidad de almacenar tablas de direcciones físicas, asociando cada una de estas direcciones aprendidas en el tráfico con el puerto físico de donde provino el anuncio del *ARP(Access Request Point, Punto de Petición de Acceso)*. De esta forma, el puente "sabe" a donde dirigir el tráfico entrante conociendo las direcciones de destino y origen, en un esquema de protocolos basados en normas de la *IEEE 802* con respecto a redes locales. Las tablas de direcciones físicas mencionadas son recolectadas valiéndose de los mecanismos de requisición/respuesta del que hace uso el protocolo *ARP* (miembro de la familia *TCP/IP*) y en donde la necesidad de asociar las direcciones lógicas con las físicas permite armar las tablas de las que hacen uso los puentes. La figura 2.17 muestra el símbolo del puente en los diagramas de redes, al igual que muestra fragmentos de las tablas aprendidas en la generación de tráfico en la red.

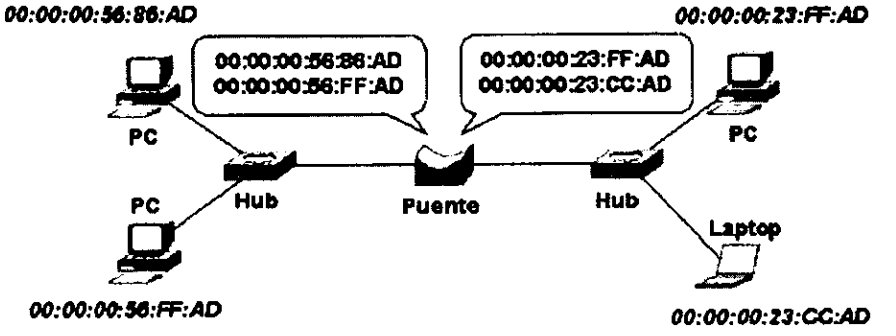


Figura 2.17. Trabajo de un Bridge.

Por la naturaleza del funcionamiento de los puentes, estos equipos se colocan en la capa 2 de operación del modelo *OSI*, y aunque son capaces de filtrar el tráfico según las direcciones de origen y destino que estén contenidas en los encabezados, no pueden filtrar los paquetes llamados de difusión completa o *broadcast*. Los detalles de cómo se compone esta dirección y otras similares se detallan en la sección de análisis del modelo *OSI* de comunicaciones.

2.4.7. Switches

Los *switches* representan una mejora sustancial a los puentes en tránsito de paquetes en las redes de datos. El término switch, aunque debería reemplazarse por el de conmutador no se hace por el significado que llevan los conmutadores de voz y que también se tratarán en esta sección.

Los conmutadores de voz también son switches, pero en el contexto de redes de datos, se prefiere nombrar a los avanzadores de tramas como switches (hay de capa 2 y de capa 3) y manejarlos así en la mayoría de la literatura técnica de redes.

El avance mencionado con respecto a los switches consiste en una técnica de servicio dedicado que permite asignar el ancho de banda completo a cada servicio o puerto cuando dos equipos intentan comunicarse. Este hecho hace que los switches sean equipos mucho más rápidos y eficientes que los puentes y desde luego que los concentradores; tomando el papel principal de conexión en las redes locales y que a últimas fechas poseen funciones de filtrado de contenidos y ruteo de paquetes (switches de capa 3). La figura 2.18 muestra la representación gráfica de los switches en una red local; al igual que la asignación de puertos en una comunicación de puerto a puerto, además se puede observar que al conectar dos computadoras (PC A y PC B) en un switch, el ancho de banda que manejan las *PCs* se ocupa por completo. En ese sentido, las colisiones como tal ya no se presentan puesto que los switches no contemplan el hecho que existan más de dos equipos en el mismo medio dedicado.

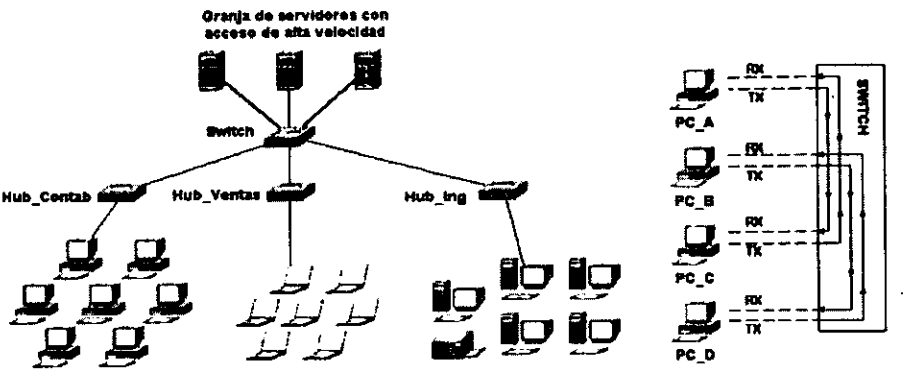


Figura 2.18. Switches en una red.

Por último, es bueno mencionar que las técnicas más comunes de switcheo para la transmisión de tramas son: Guarda y Envía (*store and forward*), Recorte breve (*cut through*) y Fragmento libre (*fragment free*).

2.4.8. Routers

Los routers o ruteadores, son el elemento clave en el diseño de la propuesta para la red de multi servicios corporativos, que unen las sucursales de todo el corporativo y se montan sobre ellos los servicios de voz y datos para toda la red. Los ruteadores son equipos que definen el direccionamiento lógico y permiten agrupar a todos y cada uno de los miembros de la red en subconjuntos, que hacen más eficiente la transmisión de paquetes de una localidad a otra. El ruteador se compone básicamente de dos partes; la primera que se encarga de la transmisión física de los paquetes está provista de circuitos *ASIC*, diseñados para que la retransmisión de las tramas sea lo más rápido posible, y la lógica empleada para ello interactúa con las interfaces *WAN* antes mencionadas. La segunda parte define el direccionamiento de paquetes y se encarga de encontrar la mejor ruta para el envío de paquetes, basándose en protocolos de ruteo que toman en cuenta variables (métricas) como retrasos y anchos de banda para tomar la mejor decisión al

respecto. La figura 2.19 señala estas dos partes y ejemplifica la inclusión de los ruteadores en una topología general de redes *WAN*.

2.4.9 Conmutadores

Los conmutadores telefónicos son los elementos clásicos en las redes antiguas de voz, que se encargaban de proveer las comunicaciones entre las empresas u organismos privados y la red pública de conmutación telefónica (*PSTN*). Al principio estas comunicaciones eran grupos de troncales analógicas, mejor conocidas como *COTs (Central Office Trunks)*, pero conforme fueron avanzando las comunicaciones, los servicios se digitalizaron y las troncales crecieron de tamaño para conectarse a los proveedores (carriers) por enlaces de mayor tamaño, tales como E1s, E3s, etc. La figura 2.20 muestra el esquema de los conmutadores y su conexión típica a la red PSTN y a otros conmutadores.

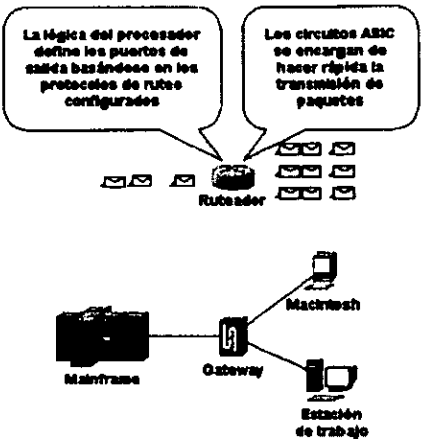


Figura 2.19. Función de los routers.

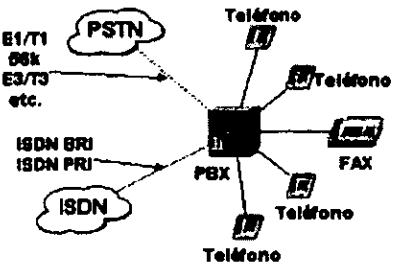


Figura 2.20. Representación de un conmutador.

2.5. Protocolos de Comunicaciones

En el 1973, la *DARPA (Defense Advanced Research Projects Agency, Agencia de Desarrollo Avanzado de Proyectos de la Defensa)* inició un programa de investigación de tecnologías de comunicación entre redes de diferentes características. El proyecto se basaba en la transmisión de paquetes de información, y tenia por objetivo la interconexión de redes.

Del proyecto DARPA surgieron dos redes: una de investigación, *ARPANET (Advanced Research Projects Administration Network, Red Avanzada de Administración de Proyectos*) y una de uso exclusivamente militar, *MILNET (Military Net, Red Militar)* Para comunicar las redes se desarrollaron varios protocolos: El protocolo de Internet y los protocolos de control de transmisión. Posteriormente estos protocolos se englobaron en el conjunto de protocolos *TCP/IP.*

Siguiendo con las investigaciones en 1980, este conjunto de protocolos se incluyeron en el *UNIX 4.2* de *BERKELEY,* y fué el protocolo militar standard en 1983. Con el nacimiento en 1983 de *INTERNET,* se popularizo bastante, y su destino va unido al de Internet. *ARPANET* dejo de funcionar oficialmente en 1990.

Protocolos estandarizados

A continuación enunciaremos brevemente los diversos protocolos que se encuentran en las diferentes capas, cabe comentar que el modelo de capas de TCP/IP es algo diferente al propuesto por ISO para la interconexión de sistemas abiertos.

En la capa de aplicación podemos considerar los siguientes protocolos:

- *BOOTP (Bootstrap Protocol)*
- *DNS (Domain Name Server)*
- *Echo Protocol*
- *NTP (Network Time Protocol)*
- *SNMP (Simple Network Management Protocol)*
- *ICMP (Internet Control Message Protocol)*
- *IGMP (Internet Group Management Protocol)*

En la capa de transporte tenemos los siguientes protocolos:

- *UDP (User Datagram Protocol)*
- *TCP (Transmision Control Protocol)*

Ahora hablando de la capa de Red encontramos :

- *IP (Internet Protocol)*
- *Direcciones IP*

Y finalmente en la capa física encontramos:

- *ARP (Address Resolution Protocol)*

- *RARP (Reverse Address Resolution Protocol)*

2.5.1. Modelo OSI

El modelo *OSI* fue desarrollado a finales de los años 70s por la Organización Internacional para la Estandarización (*ISO*), la cual es una organización internacional de representantes de la industria y organizaciones gubernamentales.

El *ISO* organizó un comité de profesionales en cómputo para ayudar a establecer los estándares que sirvieran para promover la interoperabilidad entre fabricantes de computadoras y comunicadores de datos en la industria. Al principio algunos fabricantes dudaron en cumplir con estos estándares, ya que suponían que deberían de mantener los canales de ventas logrados con el equipo que tenían establecido, pero gradualmente reconocieron la necesidad de apoyar la conectividad entre todos los tipos de equipo para mantener su base de clientes, y por que existen más variables al proveer componentes que al establecer interoperabilidad.

El Modelo de Referencia *OSI* organiza la comunicación entre redes en las siguientes 7 capas, como lo muestra la figura 2.21

El propósito de establecer el Modelo de Referencia *OSI* no es el de crear comunicaciones físicas, sino proveer un plan de funcionalidad entre las capas. Esta funcionalidad está especificada por los planos de los protocolos desarrollados por fabricantes y organizaciones de estándares. Cada capa tiene una tarea a realizar, y teóricamente los productos que cumplen con el modelo *OSI* pueden ser sustituidos por otros productos que también lo cumplan.

En las 7 capas del modelo *OSI*, cada capa transfiere datos entre las capas arriba y debajo de ella. Cuando dos dispositivos se comunican, cada nivel se comunica con un nivel comparable en el otro. Estos niveles comparables se denominan *peers (compañeros o amigos)*.

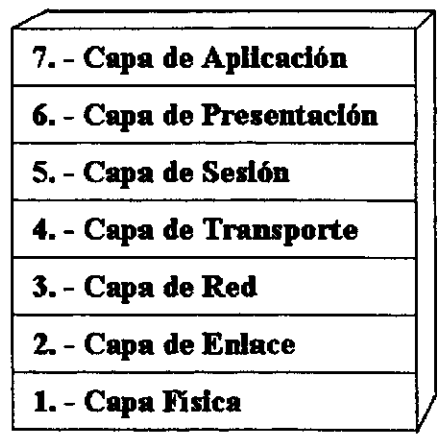


Figura 2.21. Capas en el modelo OSI.

Los *peers* pueden comunicarse uno con otro agregando un *header (encabezado* o *identificador*) a cada paquete de comunicación. Cada capa puede agregar su propio header al mensaje antes de pasarlo a la capa inferior. Los *headers* se quitan en orden inverso cuando la computadora de destino recibe la unidad de información, que consiste en *headers* y datos.

En la figura 2.21. se puede apreciar que a excepción de la capa más baja del modelo *OSI,* ninguna capa puede pasar información directamente a su contraparte en la otra computadora. La información que envía una computadora debe pasar por todas las capas inferiores, La información entonces se mueve a través del cable de red hacia la computadora que recibe y hacia arriba a través de las capas de esta misma computadora hasta que llega al mismo nivel de la capa que envió la información. Por ejemplo, si la capa de red envía información desde la computadora A, esta información se mueve hacia abajo a través de las capas de enlace y física del lado que envía, pasa por el cable de red, y sube por las capas física y enlace del lado del receptor hasta llegar a la capa de red de la computadora B, tal como lo muestra la figura 2.22 La interacción entre las diferentes capas adyacentes se llama interfase. La interfase define que servicios de capa inferior se ofrece en su capa superior y como estos servicios son accesados. Además, cada capa en una computadora actúa como si estuviera comunicandose directamente con la misma capa de otra computadora. La serie de reglas que se usan para la comunicación entre las capas se llama protocolo. A continuación se detallan las capas del modelo *OSI:*

Capa 1: Física

La capa física transmite y recibe bits con el medio de comunicación. Su unidad de información es el bit. A esta capa no le interesa si los bits están agrupados en patrones con cierto significado. Esta capa describe las características mecánicas de la red así como las reglas con las cuales se transmiten los bits. Debido a esto, le interesan los conectores empleados, la configuración de las terminales de conexción, las señales que aparecen en las terminales del conector, las características eléctricas de las señales, etc.

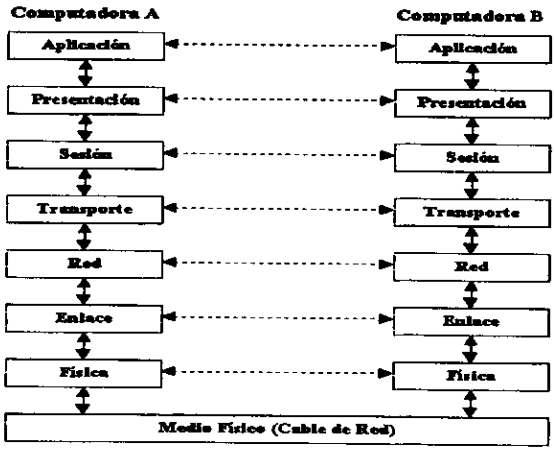


Figura 2.22. Intercambio de información.

Un protocolo conocido de la capa física es el *RS-232C*, el cual describe los conectores utilizados para interconectar dispositivos, así como los protocolos de las señales empleadas.

Capa 2: Enlace de datos

Esta capa recibe los unos y ceros (*bits*) de la capa física y los organiza en grupos lógicos llamados *frames (tramas)*. La capa de enlace de datos incluye las reglas que controlan los protocolos de acceso a redes, es decir, cuándo una estación puede transmitir, qué hacer cuando un nodo falla, y cómo verificar errores.

Esta capa le agrega un *header* a su componente de datos, el cual frecuentemente contiene información sobre las direcciones del que manda y del que se requiere que reciba. Esta información se usa para dirigir (*route*) la trama hacia el destino apropiado y asegurar que la computadora de destino conozca el origen de la trama.

En este nivel, la dirección se interpreta como dirección física por que usualmente se deriva de la configuración del hardware. Una organización de estándares le asigna a cada fabricante un rango de direcciones, y el fabricante le asigna una dirección específica de ese rango a su hardware. Dependiendo del estándar, se puede tener hardware con dirección física permanente (como *Ethernet y Token Ring*), lo cual obliga a que no haya dos tarjetas de red con direcciones físicas iguales; o dirección física configurable (como *ARCnet*), lo que causa problemas en *LANs*.

Capa 3: Red

La capa de red dirige mensajes a través de redes complejas. Su unidad de información es el paquete (*packet*). En redes sencillas, las direcciones físicas de fuente y destino son suficientes para mover mensajes eficientemente entre computadoras. Cuando las redes abarcan grandes áreas y tienen muchos segmentos de redes, es útil tener más información. Estas redes complejas se llaman *internetworks* o *internets*, y son simplemente redes entre redes.
En una *internet*, a cada segmento de red, es decir, cada red "local" dentro de la *internet*, se le asigna una identificación lógica de red, y esta asignación se maneja en la capa de red. Por ejemplo, *Netware* identifica segmentos de red individuales con números hexadecimales de 8 dígitos. La información de la red en un paquete es usada en la capa de red para dirigir el paquete eficientemente a través de la *internet* en una forma transparente a los protocolos de las capas superiores. La capa de transporte y las otras capas superiores no están conscientes de la configuración de la red ni de la forma en que se mandan mensajes entre sus fuentes y sus destinos. Un ejemplo de protocolo de esta capa es *X.25*.

Capa 4: Transporte

Esta capa asegura una entrega "confiable" de datos entre procesos que corren en las computadoras fuente y destino. Debe notarse que la comunicación es entre procesos, no entre dispositivos con direcciones de red. La unidad de información de esta capa se denomina segmento (*segment*).

La capa de transporte es responsable de asegurar que las unidades de datos se transmitan sin error, en sequencia, y sin pérdida o duplicación. "Confiable" no significa que los datos no puedan ser dañados o perdidos, sino que todas esas pérdidas o daños puedan ser detectados. El error debe ser corregido por la capa de Transporte o deben ser informados del error los protocolos de capas más altas.
Esta capa es responsable de tomar cadenas de mensajes y romperlas en unidades más pequeñas que puedan ser manejadas por la capa de red. La capa de transporte controla el flujo de los datos, provee información para recuperación de errores, reordena las unidades de mensaje y provee *acknowledgement* entre dispositivos que se están comunicando.

Capa 5: Sesión

Esta capa administra el diálogo entre dos computadoras al establecer, sincronizar y terminar comunicaciones.

Por ejemplo si dos personas quieren comunicarse, establecerán reglas de conversación, con respecto al lenguaje, por ejemplo, y usarán reglas de cortesía para asegurar que los mensajes se comuniquen en forma ordenada. Al final de la conversación, hay un intercambio amistoso para indicar que no se esperan más mensajes.

La comunicación entre dos computadoras es similar. Al establecer una comunicación, las computadoras negocian los protocolos que se usarán, los modos de comunicación, el chequeo y recuperación de errores, y otros aspectos de la comunicación. Cuando las computadoras ya no necesitan comunicarse, se utiliza un procedimiento para discontinuar la sesión en una forma ordenada.

Capa 6- Nivel de Presentación

En este los protocolos son parte del sistema operativo y de la aplicacion que el usuario acciona en la red. Traduce el formato y asigna una sintaxis a los datos que produce para su transmisión en la red . Determina la forma de presentación de los datos, sin preocuparse de su significado o semántica. Proporciona independencia a los procesos de aplicación de las diferencias en la representación de datos. Proporciona servicios para la capa de aplicaciones al interpretar el significado de los datos del intercambio. Manejo de Intercambio, M. de visualización.

Capa 7 - Nivel de Aplicación

En éste el sistema operativo de red y sus aplicaciones se hacen disponibles a los usuarios. Los usuarios emiten órdenes para requerir los servicios de la red. Entre los servicios que se proporcionan a los usuarios tenemos.

2.5.2. Otros modelos y su mapeo al modelo OSI

No se debe confundir la capa de Aplicación con los programas de aplicación que ejecuta en una computadora. Recuerde que la capa de Aplicación forma parte del modelo *OSI y* que no especifica la forma en que se realiza la interfaz entre el usuario y la ruta de comunicaciones, que es más un programa de aplicación que una implantación específica

de esa interfaz. Una aplicación real presta normalmente servicios de capa de Aplicación, Sesión y Presentación y deja los servicios de capa de Transporte, Red, Enlace de datos y Física a la red.

Cada capa se comunica con su igual en otras computadoras. Por ejemplo, la capa 3 en un sistema se comunica con la capa 3 de otro sistema informático. Cuando se pasa la información desde una capa superior a otra inferior, se añade una cabecera a los datos para indicar de dónde procede la información y a dónde se dirige. La cabecera, más el bloque de información de datos de una capa, se convierten en los datos de la siguiente capa. Por ejemplo, la capa 4 añade su propia cabecera cuando traspasa información a la capa 3. Cuando la capa 3 traspasa la información a la capa 2, ésta interpreta la cabecera y los datos de la capa 4 como datos y añade su propia cabecera a los mismos, antes de pasar esa combinación al nivel inferior. Las unidades de información reciben nombres distintos en cada capa. Por lo tanto, si conoce los términos utilizados para designar los datos, siempre sabrá de qué capa del modelo se está hablando.

Los términos utilizados por las capas *OSI* para hacer referencia a unidades de información pueden ser observados en la tabla 2.6.

Antes de adoptar el modelo *OSI*, el departamento de defensa de Estados Unidos definió su propio modelo de red, conocido como el modelo *DOD (Department Of Defense, Departamento de la Defensa)*. El modelo *DOD* está estrechamente relacionado con el conjunto de protocolos *TCP/IP*. Estos protocolos establecen una descripción formal de los formatos que deberán presentar los mensajes para poder ser intercambiados por equipos de cómputo; además definen las reglas que ellos deben seguir para lograrlo.

Capa OSI	Nombre de la unidad de información
Aplicación	Mensaje
Transporte	Segmento
Red	Datagrama
Enlace de Datos	Trama o paquete
Física	Bit

Tabla 2.4. Términos en capa OSI.

Los protocolos están presentes en todas las etapas necesarias para establecer una comunicación entre equipos de cómputo, desde aquellas de más bajo nivel (e.g. la transmisión de flujos de bits a un medio físico) hasta aquellas de más alto nivel (e.g. el compartir o transferir información desde una computadora a otra en la red).

Tomando al modelo *OSI* como referencia podemos afirmar que para cada capa o nivel que él define, existen uno o más protocolos interactuando. Los protocolos son entre pares (*peer-to-peer*); es decir, un protocolo de algún nivel dialoga con el protocolo del mismo nivel en la computadora remota.

Los protocolos desarrollados en las investigaciones de DARPA se denominaron el Conjunto de Protocolos *TCP/IP*, y surgieron de dos conjuntos previamente desarrollados; los Protocolos de Control de Transmisión *(Transmition Control Protocol)* e Internet (*Internet Protocol*). Como se muestra en la figura 2.23.

En la actualidad, las funciones propias de una red de computadoras pueden ser divididas en las siete capas propuestas por *ISO* para su modelo de sistemas abiertos *(OSI)*, sin embargo la implantación real de una arquitectura puede diferir de este modelo. Las arquitecturas basadas en *TCP/IP* proponen cuatro capas en las que las funciones de las capas de sesión y presentación son responsabilidad de la capa de aplicación. Las capas de enlace de datos y física son vistas como la capa de interface a la red. Por tal motivo para *TCP/IP* sólo existen las capas interface de red, la de intercomunicación en red, la de transporte y la de aplicación. Como puede verse *TCP/IP* presupone independencia del medio físico de comunicación, sin embargo existen estándares bien definidos a los nivel de enlace de datos y físico que proveen mecanismos de acceso a los diferentes medios y que en el modelo *TCP/IP* deben considerarse la capa de Interface de Red; siendo los más usuales el proyecto *IEEE802, Ethernet, Token Ring y FDDI.*

<table>
<tr><td>Aplicación
Presentación
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="5">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>

Figura 2.23. Relación de TCP/IP con OSI.

- *TCP = TRANSFER CONTROL PROTOCOL*
- *IP = INTERNET PROTOCOL*

2.6. Protocolos de voz

Una de las partes esenciales del proyecto de multiservicios consiste en proveer canales de voz por medio de la red de datos que se implementará en el corporativo WideCOMM. La intención es hacer una mezcla de redes convergentes con redes telefónicas convencionales, en el sentido de que una red completamente convergente aprovecha en su totalidad la existencia de un solo cableado (por lo general, alguna categoría de par trenzado) y monta los servicios telefónicos con base a un servidor especializado (gateway) que se encarga de proveer la mayoría de los servicios que un conmutador pequeño o un equipo multilíneas provee de forma normal (transferencias, conferencia tripartita, desviación, rellamada, etc.).

Puesto que la red de voz estará conectada con equipos convencionales, es necesario sentar las bases de los protocolos de voz de forma general, con los antecedentes necesarios para entender las técnicas de compresión que se usarán en la red; al igual que es necesario definir los conceptos de medición de la voz, para proseguir con las técnicas de señalización existentes y justificar más adelante la elección hecha.

El modelo clásico del tráfico de voz en la red pública conmutada es el antecedente directo de las redes WAN, de hecho la PSTN es una red de área amplia que se encarga de enlazar los circuitos de voz y hacer pasar por todo el mundo los mensajes y las señales de voz en tiempo real. Existen tres tipos de redes WAN para las comunicaciones que usan los *Carriers (Proveedores de Servicios)*. Estas redes se ilustran en la figura 2.24 y muestran la flexibilidad de lo que representamos con una simple nube de comunicaciones de cualquier proveedor, las redes disponibles son de tres tipos: Redes de datos por conmutación de circuitos, Redes de datos por conmutación de paquetes y Redes telefónicas basadas en el sistema de señalización.

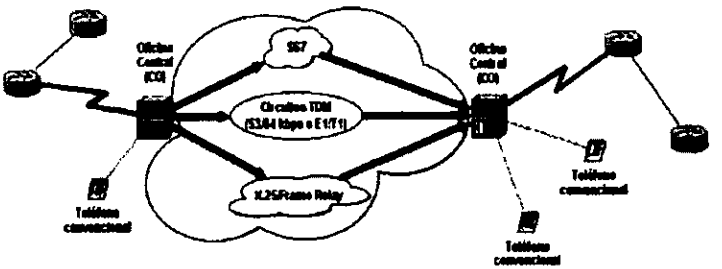


Figura 2.24. Tipos de redes WAN ofrecidas por los diferentes Carriers.

En el caso de redes telefónicas, por la naturaleza de los circuitos de voz, existe la necesidad de preestablecer la ruta de la llamada antes de hacer la conexión. Este sistema consta de tres partes básicamente: conexión de llamada, transferencia de datos y desconexión. Ahora, dentro de la estructura de redes WAN existen diferentes partes que componen a los enlaces de comunicaciones; estas partes reparten los servicios con base a una jerarquía, la cual se muestra en la figura 2.25

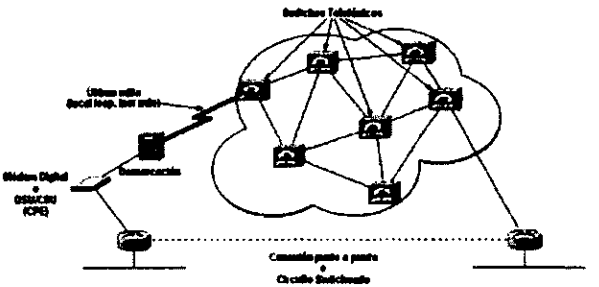


Figura 2.25. Elementos de los enlaces de comunicaciones.

De esta figura podemos resumir los elementos de la estructura de forma breve:

- *CPE (Customer Premises Equipment, Equipo en las Instalaciones del Cliente).* Estos dispositivos son variados y abarcan desde los modems digitales, pasando por los descanalizadores y llegando hasta acometidas de fibra óptica que se conocen como RDI. Aunque la descripción del nombre sugiere que los equipos pudiesen pertenecer al abonado o cliente, lo cierto es que lo único que indica es que se encuentra físicamente en las instalaciones del cliente, pero en todo momento el equipo es propiedad del *carrier*, lo que está incluido como equipo en renta mientras dure el contrato de servicios digitales o dedicados, según se trate (enlaces, servicio y DCE). La literatura técnica estándar hace uso frecuente de los términos DTE y DCE para referirse, de forma genérica, a los dispositivos que intervienen directamente en la fase de comunicación que enlaza, por un lado, a los equipos de datos y por otro, al medio de comunicación. Un *DTE (Data Terminal Equipment, Equipo Terminal de Datos)* se conectará siempre con un *DCE (Data Communications Equipment, Equipo de Comunicación de Datos)* y este último aportará la señal de reloj para la sincronización entre ambos. Este tipo de relación define una interfaz, la cual, a su vez indica parámetros, conectores y señalización en general. Realmente, la variedad de estos equipos depende de la cantidad de ancho de banda que se esté contratando y de la forma en la que el cliente recibe este medio (DTEs). Lo importante es entender de que forman se comunican estas dos clases de dispositivos, pues en ella se define la velocidad máxima de transmisión y la cantidad de ancho de banda que se puede manejar. En los equipos más modernos, algunas de las funciones realizadas por los DCEs empiezan a ser llevadas a cabo por los DTEs; como la descanalización de enlaces ISDN o E1s.

- Demarcación. Estos equipos tienen la función de concentrar los servicios de los clientes provenientes de los CPEs de una zona de servicio, y conectarla a un enlace de mayor capacidad hacia la central telefónica que corresponda por el área. Este tipo de equipos consiste en paneles de conexión en forma de tablillas de tornillos, que cruzan los pares de cobre de los abonados con el enlace de última milla del proveedor.

- Última milla. Término que describe a un enlace de cierta capacidad que une la demarcación con la *CO* que le corresponde a un área de servicio en particular.

Una vez definidos los términos de las redes WAN enfocados a enlaces telefónicos, hace falta una descripción general del modelo de comunicaciones telefónico. Este modelo se compone de tramos de conmutación, que se ramifica de un canal primario donde adquieren dos clasificaciones generales: conmutación local y conmutación troncal. La figura 2.26 esquematiza este modelo de forma básica, podemos observar los diferentes segmentos de comunicación y conmutación desde la central telefónica que corre por los enlaces físicos hasta los PBX de los diferentes usuarios . Así pues un determinado usuario puede lograr la comunicación con otro en otra oficina o ciudad utilizando la conmutación troncal.

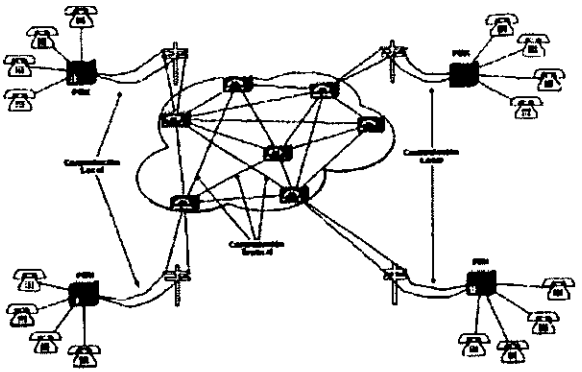


Figura 2.26. Los enlaces telefónicos convencionales se realizan mediante conmutaciones locales y troncales.

Revisados los antecedentes básicos de las redes que soportan la telefonía, podemos adentrarnos en los detalles que dan el soporte teórico del transporte de la voz.

2.6.1. Definición de la voz (señales analógicas)

La mayoría de nosotros está de alguna forma familiarizado con la transmisión de voz y con los mecanismos, para que una simple llamada se lleve a cabo por la red pública conmutada. Incluso, casi todos nosotros hemos hecho alguna valoración de calidad del servicio en dicha red cuando escuchamos entrecortado, muy débil o si se pierde la comunicación, todo esto de una forma subjetiva. No obstante, existen métodos para determinar de manera más objetiva los parámetros que componen la transmisión de voz. Para ello necesitamos establecer los parámetros de medición junto con sus unidades y los puntos de referencia usados.

Características de la señal analógica

Las señales analógicas son aquellas que siempre están definidas en un intervalo de tiempo continuo. Los parámetros básicos que componen una señal analógica son: frecuencia, amplitud y desplazamiento en el tiempo. La figura 2.27 muestra las características de las señales analógicas de forma general. Vemos también el canal de voz como tal puede extenderse desde frecuencias inferiores a los 200 Hz y hasta arriba de los 4000 Hz, para contener las señales con la energía necesaria para hacer inteligible la voz.

Como se ve la representación típica de las señales analógicas está dada por ondas senoidales suaves, pero las señales que representan la voz son mucho más complejas que eso, ya que contienen muchas componentes en frecuencia. La figura 2.28 muestra la distribución típica de la energía en las señales de voz. El eje vertical es la energía relativa y el eje horizontal es la frecuencia.

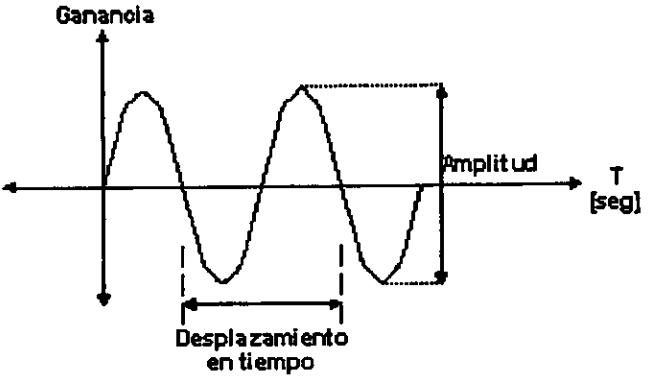


Figura 2.27. Características de una señal analógica.

Para eliminar las señales no deseadas (ruido) que podrían interferir con la voz o con las señales de control, los circuitos que procesan las señales telefónicas están diseñados para dejar pasar (filtrar) ciertas frecuencias. En el caso de la voz, estos circuitos filtran el rango de 0 – 4000 Hz, lo que se conoce como canal de voz o *VF* (*Voice Frequencies, Frecuencias de Voz*); sin embargo, la señal de la voz no requiere todo este ancho de banda, la voz ocupa realmente de 300 a 3300 hertz y a todas las señales que entra en ese rango se les llaman *señales-en-banda*. Como se verá más adelante, dentro de este rango de frecuencias, también pueden viajar otras señales que se encargan de controlar la forma en que se intercambian los mensajes (señales de control y señalización), dependiendo del valor de la frecuencia de estas señales, se dice que pueden pertenecer al rango que ocupa la voz (330-3300 Hz) o bien al rango del canal de voz (0-4000 Hz) arriba definido, lo que las define como señales en banda y fuera de banda.
A las señales dentro del rango de VF pero fuera del rango de la voz se les conoce como *señales-fuera-de-banda*.

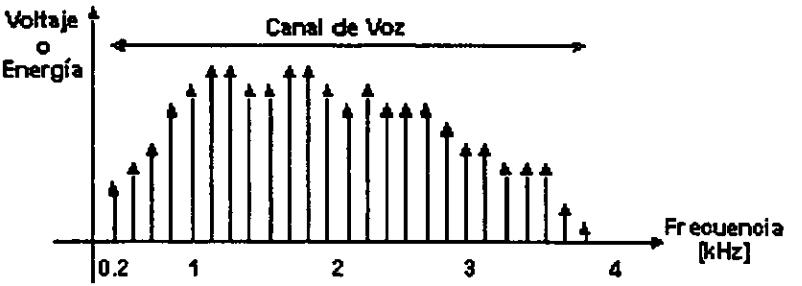


Figura 2.28. Canal de voz analógica.

Medición de la Voz

Cualquier forma de onda puede ser caracterizada en función de sus frecuencias y su potencia. Es por ello que la gran mayoría de la nomenclatura utilizada para medir a las señales de voz están dadas por relaciones que se derivaron de medir la potencia perdida cuando las señales, viajan de un extremo a otro. Las unidades empleadas para las mediciones de los sistemas telefónicos son los hertz (Hz) y los watts (W); pero como el watt resulta ser muy grande, lo que se emplea es el mili-watt (mW) y la ecuación 2.1 define esta notación.

$$1mW = \frac{1}{1000}W = 0.001W = 10e-03W \qquad \textit{Ecuación 2.1.}$$

En transmisiones, estamos más interesados en valores relativos de potencia que en valores absolutos; por esto, una expresión matemática conveniente para indicar la potencia relativa es el decibel (dB). Esta unidad nos permitirá definir tanto la potencia absoluta como la potencia relativa y la pérdida de la misma en un sistema de comunicaciones.

Millliwatt y Hertz. Las frecuencias que son usadas en pruebas usualmente caen dentro de la banda de frecuencia de la voz. Lo que se hace es probar al medio de comunicación con tonos en frecuencias que son representativas de las señales que se manejan en audio: el tono más pequeño, el tono que implica la mayor potencia registrada y el tono más alto. Con base a esto, los tonos son: 404 Hz, 1004 Hz y 2804 Hz. Los 4Hz de offset se usan para compensar los efectos de las centrales sobre los equipos de pruebas.

La intención de las pruebas en el medio de transmisión es básicamente medir la atenuación de las señales dentro del rango de frecuencias de la voz que sufren al pasar por medios de cobre, principalmente. Existe toda una gama de parámetros a medir en estas pruebas, pero la gran mayoría de ellos tienen que ver con medios de transmisión, que aunque están compuestos de cobre, señalizan en forma digital.

En estos casos, la composición de las tramas es lo que se analiza (multi-trama, alineación, sincronía, etc.); no obstante, para el caso de transmisión analógica, las pruebas sólo tienen que ver la pérdida de la potencia en las frecuencias antes mencionadas. La figura 2.29 ilustra de forma muy simplificada como se monta una prueba de tonos en un circuito de transmisión para medir esta pérdida de potencia en términos absolutos. En esta prueba, la intención es medir la pérdida de ganancia del tono de 1004 Hz en la transmisión desde la central identificada como A (la demarcación es una fase del procesamiento de llamadas en redes WAN). Como la medición está hecha tomando una señal de 1mW de potencia, la medición en B es directa y las lecturas marcan 0.5 mW en la llegada.

Con estos datos podemos medir la potencia como si el medio bajo el cual se está realizando la prueba fuera un sistema, y en donde la transferencia se mide como la razón de la salida entre la entrada.

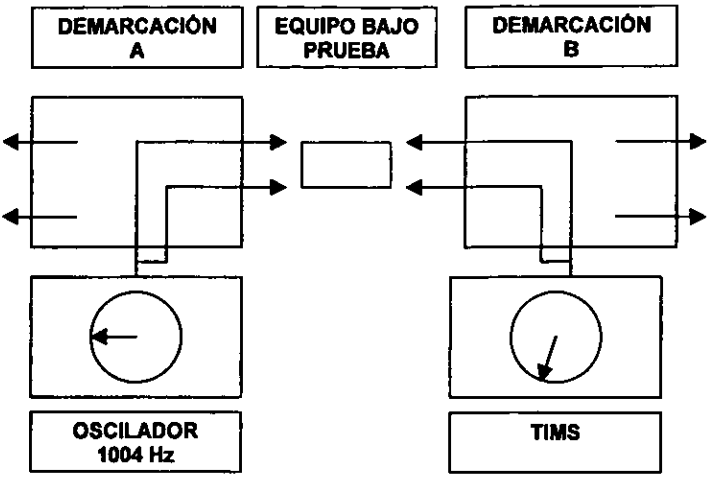


Figura 2.29. Prueba de transmisión de tonos desde la demarcación A hacia la demarcación B.

Tomamos a la potencia de llegada a B como la salida y la potencia que emite A como la entrada al sistema. Las ecuaciones 2.2 a 2.4 muestran el cálculo de la potencia relativa.

$$1mW - 0.5mW = 0.5mW \qquad \textit{Ecuación 2.2.}$$

$$Pérdida\_relativa = \frac{Potencia\_de\_salida(B)}{Potencia\_de\_entrada(A)} \qquad \textit{Ecuación 2.3.}$$

$$Pérdida\_relativa = \frac{0.5x10e-3}{1x10e-3} = 0.5 \qquad \textit{Ecuación 2.4.}$$

En otras palabras, la mitad de potencia introducida en la transmisión a 1004 Hz es perdida al llegar a la demarcación B. Esto nos muestra como la potencia relativa nos puede ser de mucha utilidad para describir la naturaleza de un medio de transmisión sin importar la cantidad de potencia que le inyectemos a dicho circuito.

El decibel

Como se mencionó antes, el decibel es una medida de la tasa de pérdida de la potencia en términos relativos y que nos permite conocer, por medio de un cálculo, la potencia absoluta en algún punto que nos interese. El decibel está representado con base al logaritmo base 10 y para expresar la potencia se usa la ecuación 2.5.

$$dB = 10\log\frac{P2}{P1} \qquad \textit{Ecuación 2.5.}$$

Donde P2 y P1 deben estar en unidades consistentes. Si el número obtenido con esta expresión es positivo, entonces P2 es mayor que P1 y negativo en caso contrario.

La potencia absoluta es medida en miliwatts y la potencia relativa medida en dBs. Estableciendo una relación entre el decibel y el miliwatt, podemos eliminar a este último como unidad operacional y ocupar solamente al decibel como unidad. La unidad de medición que es usada para expresar la potencia absoluta en términos de decibeles es el dBm y se denota por la ecuación 2.6

$$dBm = 10\log\frac{(Potencia\_medida\_en\_mW)}{1mW} \qquad \textit{Ecuación 2.6.}$$

Puesto que la potencia es una onda senoidal y la impedancia puede variar como función de la frecuencia, es necesario establecer en qué frecuencia está basado el estándar o dBm. Esta frecuencia es 1004 Hz para una resistencia también estándar de 600Ω. Por lo anterior, nuestra referencia de 0 dBm es igual a 1 mW de potencia impuesta sobre una impedancia de 600 Ω y utilizando una señal con frecuencia de 1004 Hz.

2.6.2. Técnicas de modulación

Una de las razones por las que los sistemas telefónicos tradicionales fallaban tanto en la transmisión, era la naturaleza de las señales transmitidas por las líneas de cobre y en particular en lo que se conoce como la última milla. Básicamente, la falla residía en las señales analógicas que son muy susceptibles al ruido y que además se atenúan con la extensión de las líneas. Al momento de intentar amplificarlas para su retransmisión, el efecto obtenido sólo era el de crecer también las señales no deseadas, el ruido.

La solución a este problema consistió en la digitalización de las señales para darles un tratamiento discreto y hacer uso de la tecnología binaria que garantizaba la recuperación de errores y controlaba la calidad de transmisión, incluso sobre las viejas líneas de cobre.

La historia de las comunicaciones menciona que para solucionar este problema de transmisión se crearon las técnicas de modulación. De las primeras que se formularon, sobresalen la modulación de amplitud y la modulación por frecuencia. Las cuales se detallan a continuación:

Modulación por Amplitud

Esta técnica se apoya en el uso de una señal portadora para enviar por medio de ella un mensaje, o señal moduladora que contiene la información importante. De esta forma, una señal de audio (analógica) puede ser transmitida por medios alámbricos e inalámbricos montándose sobre otra señal analógica de menor frecuencia. Una técnica relacionada con esta modulación es la modulación *digital ASK (Amplitud Shift Keying, Codificación por Cambio en Amplitud)*. En particular, la señal binaria que contiene la información define una cierta amplitud para representar un "1" y otra amplitud de la

señal senoidal para representar el "0". De esta forma, se puede enviar un mensaje digital en líneas analógicas, tal y como lo muestra la figura 2.30.

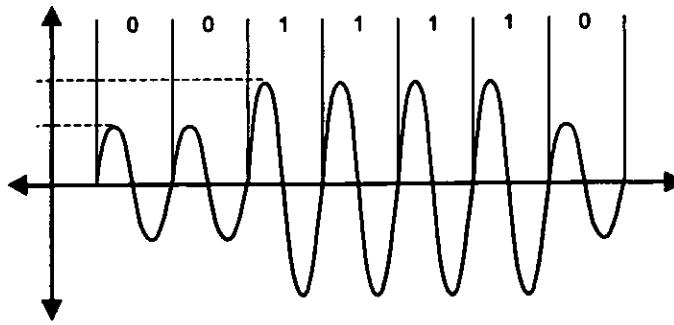


Figura 2.30. Codificación por cambio de Amplitud.

Por su parte, la modulación en frecuencia hace uso del cambio de frecuencia de la señal portadora para indicar la presencia de un cero o un uno binario dentro de la señal analógica. De esta forma, se usan dos frecuencias para indicar los cambios de señal en lo que se conoce *como FSK (Frequency Shift Keying, Codificación por Cambio en la Frecuencia)* y cuyo ejemplo se proporciona en la figura 2.31.

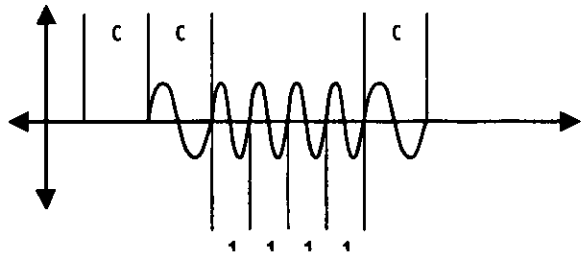


Figura 2.31. Codificación por cambio de frecuencia.

Las modulaciones por amplitud de pulso y por código, *PAM (Pulse Amplitud Modulation, Modulación por Amplitud de Pulso)* y *PCM (Pulse Code Modulation, Modulación por Código de Pulso)* se detallan a continuación:

PCM y PAM. Estas modulaciones están definidas en la especificación ITU-T G.711, y una de las etapas que se requieren antes de codificar por pulsos (PCM) es la modulación por amplitud de pulso (PAM). Como su nombre lo indica, esta modulación usa la señal analógica original para establecer la amplitud de un tren de pulsos a una frecuencia constante. La figura 2.32 bosqueja este tipo de modulación.

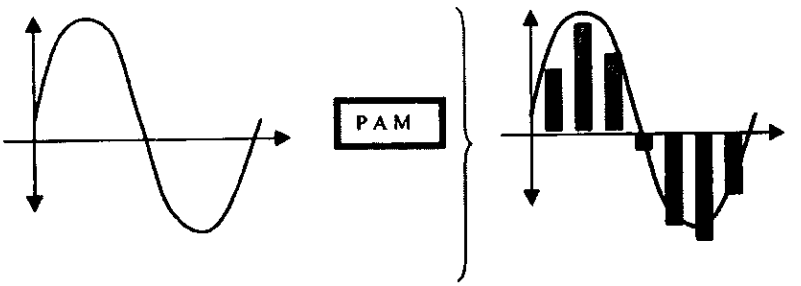


Figura 2.32. Modulación por amplitud de pulso.

El tren de pulsos se mueve a una frecuencia constante, la cual es llamada frecuencia de muestreo. La señal analógica de la voz se puede muestrear un millón de veces por segundo o dos o tres veces por segundo. Lo que determina cuántas veces por segundo se debe muestrear una señal está especificado por los trabajos de Harry Nyquist, que con base en experimentos, estableció que una señal puede ser completamente reconstruida si la frecuencia de muestreo (fm) es por lo menos 2 veces mayor que la frecuencia componente más alta de esa señal. Esto se resume como lo muestra la ecuación 2.7

$$\mathbf{Fm > 2\ (BW)} \qquad \textit{Ecuación 2.7.}$$

donde:

Fm = Frecuencia de muestreo

BW = Ancho de banda (Band Width)

Para el caso de las señales de la voz, la máxima frecuencia utilizada son los 4 kHz, por lo que la frecuencia de muestreo por el teorema de Nyquist debe ser de por lo menos 8,000 Hz.

El siguiente paso en PCM es la digitalización de las señales, que no hace más que tomar muestras de la amplitud de la señal analógica y asignar un valor (código) en forma binaria por cada valor de magnitud existente, y obtener así una codificación en 1's y 0's que representan el valor de la señal analógica. Esto último se conoce como cuantificación y codificación; dependiendo del tamaño del código usado (cantidad de bits por cada muestra) se puede obtener una granularidad muy elevada para describir las señales de entrada. Para el ejemplo de la voz, mencionamos que el teorema de Nyquist recomienda muestrear al doble de la mayor frecuencia encontrada en la señal de la voz (2 x 4 kHz = 8000 Hz), y si consideramos el estándar de codificación en 8 bits obtenemos una tasa de transmisión de 64 kbps para el sistema telefónico usando PCM. Esto lo observamos en la figura 2.33.

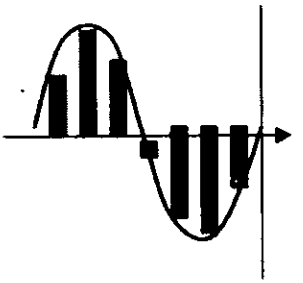


Figura 2.33. La codificación de pulsos arroja un valor primario por cada nivel de amplitud.

Un punto que debe mencionarse con relación a la cuantificación y la codificación está relacionado con el hecho de que la mayoría de los valores analógicos que se muestrean están dentro de un rango que no pertenece a un valor discreto que posea un código binario. Por esta razón se genera lo que se conoce como ruido en la cuantificación y una de las maneras de resolver el problema es elevar el número de niveles por muestra aumentado la cantidad de bits por código, lo que resulta hasta cierto punto inmanejable por los sistemas de comunicación por la carga de procesamiento. Otra solución se basa en que los niveles de cuantificación no sean uniformes en lo que se conoce como *Companding (Compression and Expanding, Compresión y Expansión).* Durante este proceso, las muestras de entrada analógicas son comprimidas en segmentos logarítmicos y entonces cada segmento es cuantificado y codificado usando un esquema uniforme. El proceso de compresión es logarítmico, donde la compresión aumenta tan pronto como la señal de muestra aumente. En otras palabras, la señal de muestra más larga es comprimida más que las señales más pequeñas, provocando que el ruido de cuantificación se incremente conforme las señales crezcan. Un crecimiento logarítmico en el ruido de la cuantificación a lo largo del rango dinámico de una señal de entrada mantendrá constante al *SNR (Signal to Noise Ratio, Tasa de Señal-Ruido)* Los estándares de la *ITU-T (International Telecommunications Union, Unión Internacional de Telecomunicaiones)* que definen las técnicas de companding son llamados A-law y u-law, para Europa y Estados Unidos, respectivamente.

2.6.3. Señalización y control

Las técnicas de señalización y control tiene que ver con la forma en que la red telefónica intercambia mensajes de control e información útil sobre las llamadas de voz. Todas las señalizaciones que se usan en la actualidad deben componerse de tres elementos principales: supervisión, direccionamiento y envío de alertas. Antes de dar una revisión de las técnicas de señalización que se usarán en el proyecto de redes, es importante tener una visión general del procesamiento normal de una llamada desde el estado libre hasta la culminación de una conversación.

Progresión básica de una llamada. Una llamada se compone de cinco estados: libre (on-hook), descolgado y toma de línea (off-hook), marcación-direccionamiento (dialing-addressing), aviso de llamada entrante (ringing) y completado de llamada (talking.) Para

poder visualizar estos estados, la figura 2.34 muestra la secuencia de una llamada desde el estado libre, representando una conexión típica de una central telefónica (CO, Central Office) hacia un servicio residencial común (teléfono).

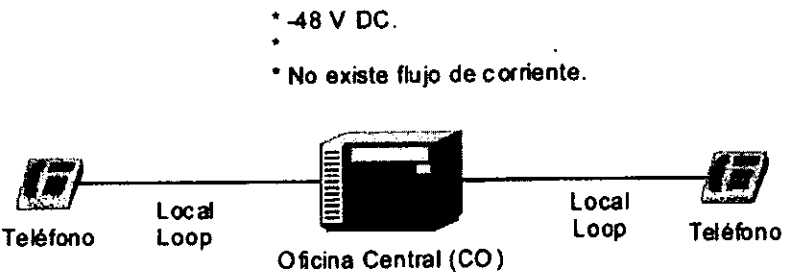


Figura 2.34. Estado libre (on-hook).

Cuando se levanta el auricular (hand-set), el teléfono internamente cierra el circuito provisto por la central telefónica, ya que en todo momento, la CO es la que alimenta al circuito telefónico, haciéndolo independiente de una caída de energía en el área del abonado o suscriptor. Este cierre de circuito es detectado por la central y entonces envía un tono de invitación a marcar (dial-tone) en la frecuencia de 350 – 440 Hz de forma continua. La figura 2.35, muestra esta fase.

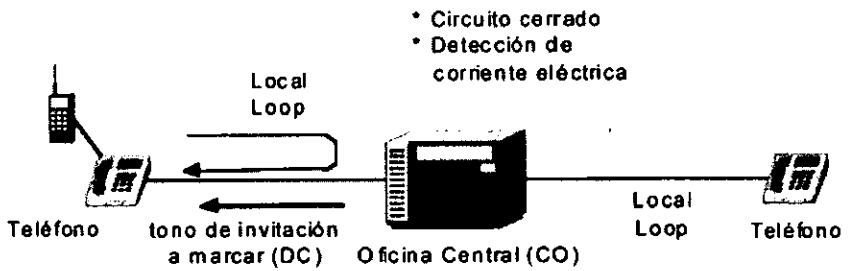


Figura 2.35. Descolgado (off-hook).

En la figura 2.36, se muestra el efecto de la marcación de dígitos. Estos dígitos pueden ser discados, lo que genera un tren de pulsos, o bien por tonos, usando una combinación de dos frecuencias que se calcularon para no estar afectadas por el ruido, esta última técnica se llama *DTMF (Dual Tone Multifrequency, o Tonos Duales de Multifrecuencia.)*.

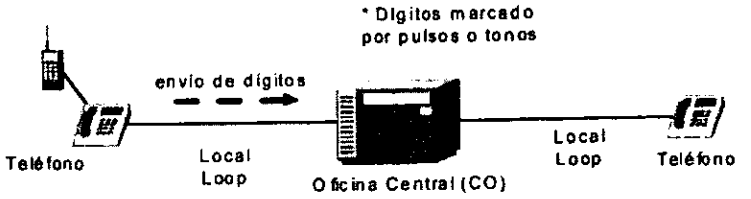


Figura 2.36. Envío de dígitos por pulsos o tonos.

En la marcación existen dos variedades para enviar la cadena de dígitos; por un lado, el sistema antiguo estaba conformado por discos de marcación que abrían y cerraban el circuito de la central por periodos breves y esto indicaba la cadena. El estado de circuito abierto se conocía como "break" y la duración estándar era de 60 ms, mientras que el estado de circuito cerrado correspondía al término "make" y su duración constaba de 40 ms. El periodo máximo para la espera del siguiente dígito era de 700 ms, una duración mayor a esta suponía un error y la progresión se cortaba. La figura 2.37 muestra esta secuencia de pulsos.

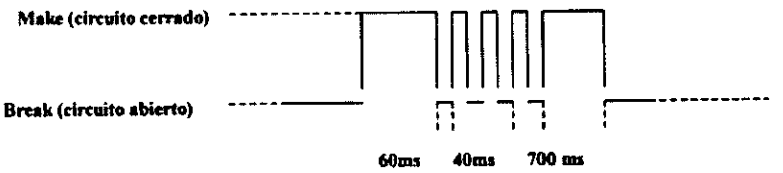


Figura 2.37. Marcación de dígitos por tonos.

Este método de marcación era muy lento y poco eficiente por lo que se creó el sistema de tonos antes mencionado, y las frecuencias que componen al sistema DTMF se muestran en la tabla 2.5, donde se muestra los tonos altos y bajos que conforman los códigos DTMF.

	1209	*1336*	*1477*	*1633*
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

Tabla 2.5. Códigos DTMF.

En la marcación, el usuario ingresa un direccionamiento compuestos por dígitos que permiten la revisión de tablas de ruteo en las centrales para enlazar las llamadas ya sea con el vecino o del otro lado del mundo. Como se verá más adelante, de este hecho parte la importancia de seguir un estándar para los planes de marcación de forma que sean seguidos por todo el mundo. Estos dígitos son transmitidos por dos hilos de cobre

que se conocen como tip y ring y están denotados en la literatura técnica por los colores verde y rojo respectivamente.

Enseguida que los dígitos han sido enviados al *switch* de troncal principal, éstos son revisados para buscar una tabla que contenga la dirección de destino, en forma de grupos que conforman los códigos de país, de área y de estación. Para determinar que código le corresponde a cada país, la ITU-T, con base en la norma E.164, establece el formato y los códigos correspondientes en los planes de numeración, tomando como base que ningún número telefónico puede contener más de 15 dígitos. De estos, los tres primeros corresponde al país, los siguientes tres al código de área designado por cada país y los nueve restantes se reparten de forma ordenada para cada central local. La figura 2.38 describe el enrutamiento de una llamada de larga distancia haciendo uso de los códigos de país, de área, local y número de estación de forma simple cómo se direcciona una llamada internacional.

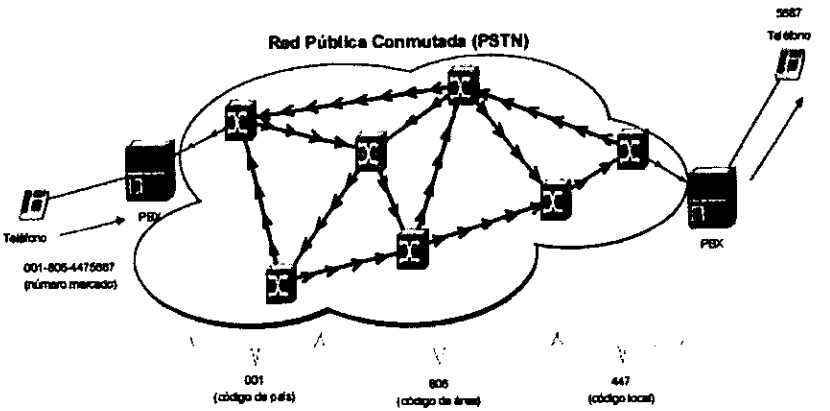


Figura 2.38. Llamada internacional.

El siguiente paso en el progreso de una llamada es la etapa de alertas y que son las que indican cuando el teléfono de destino puede o no completar la llamada. Al igual que en el estado libre, el equipo destino se encuentra en circuito abierto, y la central que le corresponde lo alimenta con un voltaje continuo de –48 V DC.

Al momento de que el switch entre la central y la demarcación determina el equipo destino, éste le envía al mismo un voltaje de alterna de 90 V a 120 Hz (el ring) y alerta al equipo destino de la llamada entrante. Si el usuario de este extremo de la comunicación decide tomar la llamada, al descolgar la bocina, la señal de ring se interrumpe, el circuito de la última milla se cierra y se establece la comunicación. La figura 2.39 indica esta última etapa.

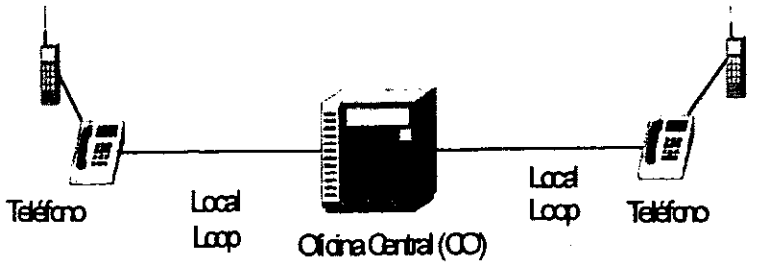


Figura 2.39. Establecimiento de llamada.

Para resumir el progreso de una llamada en un sistema telefónico convencional, la tabla 2.6 define los tonos enviados por la central hacia la parte que llama, la parte llamada y los *switches* que intervienen en la ruta.

Tono	*Frecuencia (Hz)*	*Tiempo arriba*	*Tiempo abajo*
Invitación a Marcar (dial)	350+440	Continuo	
Ocupado (busy)	480+620	0.5 s	0.5 s
Contestación normal (normal ringback)	440+480	2 s	4 s
Contestación PBX (PBX ringback)	440+480	1 s	3 s
Congestión (congestion)	480+620	0.2 s	0.3 s
Volver a marcar (reorder)	480+620	0.3 s	0.2 s
Receptor (of-hook)	1400+2060+2450+2600	0.1 s	0.1 s
Sin destino (no such number)	200 - 400	Continuo	

Tabla 2.6. Tonos para señalizar las llamadas.

2.6.4. Empaquetamiento de Voz

La telefonía es el sistema tecnológico de mayor ayuda particularmente en los negocios hoy en día, en donde se realizan miles de llamadas, lo cual implica un altísimo costo para las empresas.

Para muchas de las compañías este costo es despreciable. Tradicionalmente la voz pública telefónica es un complejo juego de tarifas y subsidios, que frecuentemente converge en situaciones donde llamar de A a B cuesta una fracción si la llamada se realiza de B a A, por ello muchas compañías deciden construir puentes para evitar la

telefonía pública, y contratan líneas privadas, pero eso eleva también los costos y muchas de ellas han buscado nuevas estrategias.
La búsqueda para alternativas de bajo costo nunca había aplicado tanta presión. tenemos un ejemplo: El uso de las redes WAN en Europa creció un 500 % pero los precios disminuyeron sólo un 30%, resultando en un crecimiento del 470% de las expectativas. La presión en la red es construida a raíz de los dos nuevos modelos, Internet/Intranet.

Con el desarrollo de la tecnología las necesidades no son cubiertas y nuevas soluciones se vuelven posibles. Se presenta una reducción dramática en el costo y una creciente acelerada en la funcionalidad. En el área de voz simplemente el precio de los DSP (Digital Signal Processor, Procesadores Digitales de Señal) ha disminuido dramáticamente, mientras que la medida de la voz, utilizando algoritmos de compresión, se ha incrementado considerablemente.

El tamaño y la complejidad del tráfico de datos han ido creciendo. Nuevas aplicaciones como transferencia de ficheros, CAM/CAD, y el explosivo crecimiento de LANs ha requerido la necesidad de que sea posible transmitir grandes volúmenes de datos a altas velocidades y en imprevisibles patrones llamados *Burst* (ráfagas de datos). Al mismo tiempo, la calidad de las líneas de las compañías telefónicas, nodos y redes han impulsado el cambio a la tecnología digital. Al mismo tiempo, el equipo de procesamiento de datos, equipo de comunicación de datos, y software han provocado la busca de nuevos niveles de sofisticación. Teniendo todo esto en cuenta, y que la industria de telecomunicaciones se ha enfrentado con el dilema de mejorar incrementando los niveles de ráfagas en él tráfico de datos, ha reducido costos y ha aumentado las velocidades de transmisión. Todo el sistema de empaquetamiento de voz sigue un modelo común. La red de transporte de paquetes de datos puede estar basada en *IP(Internet Protocol, Protocolo de Internet), FRAME RELAY, o ATM (Asyncronus Transfer Mode, Modo de Transferencia Asíncrono)*. Al final de esta red se encuentran componentes o dispositivos que pueden ser llamados agentes de voz, los cuales tiene la misión de cambiar la información de voz de su tradicional forma telefónica a una nueva forma donde se acepte la transmisión por paquetes. La red entonces desvía los paquetes de datos a un agente de voz que manda los datos a un destinatario. Para llevar a cabo esta integración existen dos modelos básicos para integrar voz y datos, éstos son : Transporte y Traslado, el transporte es el soporte transparente de voz sobre la red existente de datos. Traslado es la conversión de las funciones tradicionales de voz para que puedan ser enviadas por la infraestructura de datos.

2.6.5. Transporte de voz

Frame Relay

Frame relay es un protocolo de transmisión de paquetes de datos en ráfagas de alta velocidad, a través de una red digital, fragmentados en unidades de transmisión llamadas *frame* (tramas). *Frame relay* requiere una conexión exclusiva durante el periodo de transmisión. *Frame relay* es una tecnología de paquete-rápido ya que la detección de errores no ocurre en ningún nodo de la transmisión. Los extremos son los responsables de esta detección. Los errores en redes digitales son extremadamente menos frecuentes en comparación con las redes analógicas. *Frame relay* transmite paquetes en el nivel de envío de datos del modelo de Sistemas de Interconexión Abierta

(*OSI*) antes que en el nivel de red. Distintamente a que un paquete, que es de tamaño fijo, un frame es variable en tamaño y puede ser tan largo como mil bytes o más. Una conexión frame relay es conocida como una conexión virtual. Una conexión virtual permanente es exclusiva al par origen-destino y puede transmitir por encima de 1.544 Mbps, dependiendo de las capacidades del par origen-destino. Una conexión virtual de intercambio es también posible usando la red pública y puede proporcionar elevados anchos de banda.

Topologías de conexión en Frame Relay

Entre las características entre los usuarios de *frame relay* son: Tener una red que interconecta *LANs* usando *routers* para circuitos alquilados o de ancho de banda controlado y se está buscando la reducción de costos y el crecimiento de la red. Las redes están basadas en topología de estrella. Esta topología de estrella puede consistir de una estrella simple, o múltiples estrellas, que pueden estar en una cascada, o estructura de árbol. La razón para la configuración de estrella es doble. Primeramente, esto refleja la estructura organizacional y flujo de datos de los negocios, con administración centralizada y funciones locales. Secundariamente, esto es impuesto por la tecnología de las líneas alquiladas. El uso de frame relay abre las puertas a una gran flexibilidad a la topología de conexión. Mientras la estructura del tráfico podría tender entre configuraciones estrella, La disciplina impuesta por las líneas alquiladas las facilita y el actual flujo de tráfico que podrá se mucho mejor incorporado a la topología. Como se aprecia en la figura 2.40 podemos observar la topología de estrella.

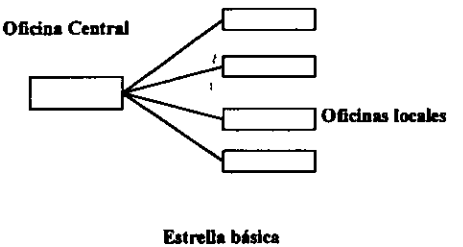


Figura 2.40. Topología de estrella básica.

A continuación se describen algunas de las características más importantes de este protocolo:

Características Técnicas de Frame Relay

- Velocidad de acceso: desde 64 kbps a 2 Mbps.
- Caudal (bidireccional) garantizado. 8, 16, 32, 48, 64, 96, 128, 256, 512, 1024, 1536, 1984 kbps.
- Acceso alternativo *RDSI*: para velocidades de hasta 256 kbps, *back-up* de 64 kbps a través de *RDSI*.
- Gestión de Red: permanente.
- Soporte del Servicio: permanente (ventanilla única).

- Facilidades de Gestión de Cliente.
- PC para Gestión de Cliente.
- Interfaz física: < 2 Mbps. V.35, V.36 = 2 Mbps. G.703/704.
- Destino alternativo para volver al camino en caso de fallo.

Ventajas de Frame Relay

Dentro de las ventajas que tiene esta tecnología tenemos:

Ahorro en los costos de las telecomunicaciones: con el servicio *frame relay* los usuarios podrán transportar simultáneamente paquetes de voz y datos, compartiendo los mismos recursos de red, el tráfico perteneciente a múltiples comunicaciones y aplicaciones, y hacia diferentes destinos.

Solución Compacta de Red: Se realiza en un bajo tiempo dependiendo de las necesiades del cliente.

Servicio gestionado extremo a extremo: Se puede dar mantenimiento , administración y control en general los 365 días del año.

Tecnología de punta y altas prestaciones: *frame relay* proporciona alta capacidad de transmisión de datos por la utilización de nodos de red de alta tecnología y bajos retardos como consecuencia de la construcción de red (*backbone*) sobre enlaces a 34 Mbps y de los criterios de encaminamiento de la Red de Datos, orientados a minimizar el número de nodos de tránsito.

Flexibilidad del servicio: *frame relay* es la solución adaptable a las necesidades cambiantes, ya que se basa en circuitos virtuales permanentes, que es el concepto de Red Pública de Datos, equivalente al circuito punto a punto en una red privada. Sobre una interfaz de acceso a la red se pueden establecer simultáneamente múltiples circuitos virtuales permanentes distintos, lo que permite una fácil incorporación de nuevas sedes a la Red de Cliente.

Servicio normalizado: *frame relay* es un servicio normalizado según los estándares y recomendaciones de UIT -T, ANSI y frame relay forum, con lo que queda garantizada la interoperatividad con cualquier otro producto *frame relay* normalizado.

Aplicaciones de Frame Relay

Después de enumerar y describir las ventajas tenemos las aplicacionesen que puede funcionar el protocolo:

- Intercambio de información en tiempo real, dentro del ámbito empresarial.
- Correo electrónico.
- Transferencia de ficheros e imágenes.
- Impresión remota.
- Aplicaciones host-terminal.
- Aplicaciones cliente-servidor.
- Acceso remoto a bases de datos.

- Construcción de bases de datos distribuidas.
- Aplicaciones de CAD/CAM.

Actualmente, dado el alto grado de informatización que han alcanzado las empresas en los últimos años, es muy común la convivencia de varias de las aplicaciones citadas y otras similares en el entorno de un mismo cliente, lo que hace aún más provechosa la utilización del servicio *frame relay* como medio de transporte único.

ISDN o RDSI: El Estándar Universal

ISDN (Integrated Services Digital Network, Red Digital de Servicios Integrados) es un concepto ligado al de una red totalmente digital que, utilizando unos estándares universales de acceso, permite la conexión de una amplia gama de terminales como teléfonos, servidores, centrales PBX, etc., a los que la red proporciona una gran variedad de servicios entre los que se incluyen voz, datos e imágenes. Siendo rigurosos, cabría matizar la anterior definición diciendo que los estándares no son tan universales como hubiera sido deseable, existiendo serias diferencias entre EEUU, Japón y Europa. También podría considerarse la terna voz, datos e imágenes como poco significativa (a pesar de haberse convertido en un tópico), ya que al tratarse de una red digital de paquetes y de circuitos poco importa el origen de la información codificada, y la lista podría ampliarse indefinidamente con texto, *Hi-Fi(Alta Fidelidad)*, gráficos, etc.

Es decir, la *RDSI* se presenta como la bandera de las redes *RDI*, aunque su oferta es diferente:

- Audio de 7 kHz de ancho de banda, en vez de los 3.1 kHz de la red telefónica actual.
- Canales digitales de 64 kbps de velocidad en vez de las que se alcanzan utilizando modems que difícilmente llegan a los 40 kbps.
- Mayor funcionalidad y servicios gracias al canal común de señalización.
- Un único y estandarizado método de acceso que da paso a toda una red de área extensa, con posibilidad de transferir información tanto en modo circuito como en modo paquete.

La RSDI de banda estrecha (RSDI-BE)

Las comunicaciones hoy en día se configuran como un conjunto de redes separadas:

- Red X.25 para datos.
- Redes de conmutación de circuitos para voz y datos.
- Redes para transmisión de la señal de TV.
- Redes de área local (LAN).
- Redes metropolitanas (MAN).

Es evidente que no existe una red universal donde podamos conectar indistintamente el teléfono, las terminales X.25, ni por supuesto un receptor de TV. Cada uno de estos dispositivos requiere un tipo específico de servicio, contratado, instalado, y gestionado por separado. La *RDSI* pretende ser la gran integradora de los servicios que hasta ahora proporcionaban las compañías telefónicas: desde la red conmutada para voz, redes de paquetes, hasta los enlaces digitales punto a punto, pasando por la mayoría de redes

especializadas en dar un solo servicio. La integración de las LAN y circuitos de TV quedan como objetivo para una futura *RDSI* en banda ancha. En principio, la *RDSI* convivirá y permitirá la conectividad con el resto de redes públicas, aunque éstas progresivamente irán siendo integradas o sustituidas por la *RDSI* hasta llegar a constituirse en una red única.

Para permitir la interconexión de los terminales actuales, que no soportan de forma nativa protocolos *RDSI*, se han diseñado los denominados *TA*(Terminal Adapters, Adaptadores de Terminal). Los TA garantizan de esta forma la conexión de la mayoría de recursos de comunicaciones existentes sin necesidad de cambios notables. Especial énfasis están poniendo las compañías operadoras en captar el máximo número de usuarios en datos, ya que es el sector de mayor crecimiento. Un reciente estudio indica que la red telefónica en voz tiene un crecimiento anual en Europa estimado entre el 2% y el 5%, mientras que la demanda para datos se estima entre el 20% y el 30%. A pesar de que se habla mucho de los nuevos usuarios residenciales y sus aplicaciones típicas, como video bajo demanda y otros, lo cierto es que las fuerzas que van a mover la banda ancha en los próximos años van a ser la industria y los gobierno principalmente. A continuación observamos en la figura 2.41 un esquema básico representando la conexión y ventajas usando RSDI_BE.

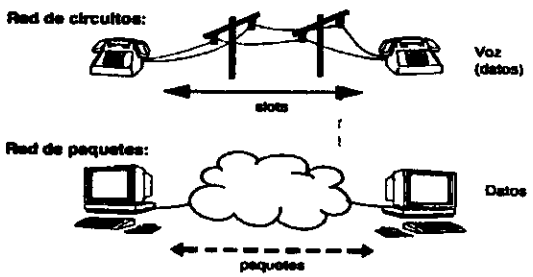


Figura 2.41 La RDSI-BE integra redes de circuitos y redes de paquetes.

RDSI de Banda Ancha (*ATM*)

La *RDSI* de banda ancha (*RDSI*-BA) es el resultado de la evolución de la *RDSI* (conocida ahora como *RDSI* de banda estrecha) para soportar mayores velocidades y posibilitar servicios avanzados como la transmisión de video.

Fue en 1988 cuando el CCITT (Consultative Committe on International Telephony and Telegraphy, Comité de Consulta Internacional en Telegrafía y Telefonía) aprobó la primera recomendación para la RDSI-BA (I.121). En ella se define RDSI-BA como: Un servicio que requiere canales de transmisión capaces de soportar velocidades mayores que la velocidad primaria. Se definió ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrono) como la tecnología de conmutación que utilizaría RDSI-BA y 155 Mbps la velocidad que debía soportar. A pesar de las diferencias entre RDSI-BA y RDSI-BE, ambas mantienen muchos puntos en común, ya que la RDSI-BA es la evolución hacia la alta velocidad de la RDSI-BE. El modelo de referencia para la

configuración es similar, ya que RDSI-BA asumió con algunas modificaciones el de RDSI-BE.Ambas son de naturaleza conmutada y con conexión, utilizando un protocolo de señalización similar.

Para reunir los requisitos para video de alta resolución, se necesitan velocidades de unos 150 Mbps. Además para poder ofrecer uno o más servicios interactivos y distribuidos se necesita una velocidad de línea de abonado de unos 600 Mbps. La única tecnología que permite estas velocidades es la fibra óptica. Por tanto la introducción de la *RDSI*-BA depende del ritmo de introducción del bucle de abonado de fibra. El dispositivo de conmutación debe soportar un amplio rango de velocidades diferentes y de parámetros de tráfico. Por eso se utiliza una tecnología de conmutación de paquetes rápidos que admite fácilmente el protocolo *ATM*.

Arquitectura funcional
En la figura 2.42 podemos observar la arquitectura funcional de *RDSI*-BA:

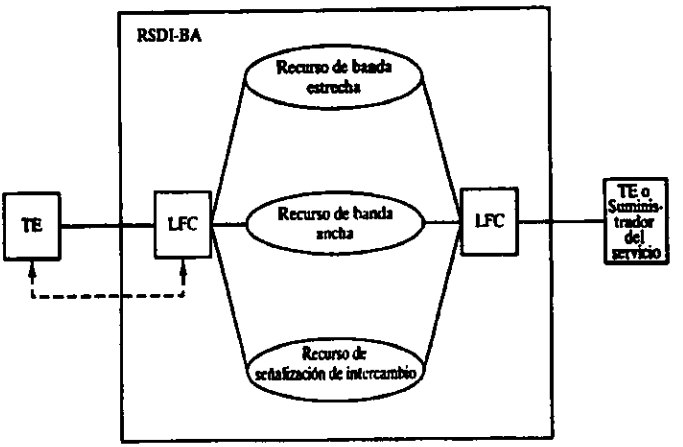


Figura 2.42. Arquitectura funcional de RDSI-BA.

RDSI-BA debe dar soporte a todos los servicios de transmisión a 64 kbps que son admitidos por *RDSI*-BE para facilitar la conexión de *RDSI*-BE a *RDSI*-BA.

También observamos como el control de *RDSI*-BA se basa en señalización de canal común. Se usa un protocolo SS7 mejorado para admitir capacidades suplementarias de red de mayor velocidad. En cuanto al protocolo de señalización, dos son los organismos que han definido estándares utilizados en *ATM*. El *ITU-T (International Telecommunications Union, Unión Internacional de Telecomunicaciones)* definió el estándar *Q.2391*, versión mejorada del *Q.391* utilizado en *RDSI*-BE. Por otro lado, el ATM FORUM (asociación de fabricantes) propuso la señalización *UNI 3.0*, basado precisamente en el *Q.2391*, que permite la interoperatividad entre distintos fabricantes.

Las diferencias entre *Q.391* y *Q.2391* son:

En *Q.2391* no existe un canal común para la señalización (canal D), sino un canal virtual independiente para cada terminal.

En vez de negociar el acceso a un canal B, se negocia una conexión de canal virtual entre extremos de la comunicación.

VoIP

Desde hace tiempo, los responsables de comunicaciones de las empresas tienen en mente la posibilidad de utilizar su infraestructura de datos, para el transporte del tráfico de voz interno de la empresa. No obstante, es la aparición de nuevos estándares, así como la mejora y abaratamiento de las tecnologías de compresión de voz, lo que está provocando finalmente su implantación.

Después de haber constatado que desde una *PC (Personal Computer, Computadora Personal)* con elementos multimedia, es posible realizar llamadas telefónicas a través de Internet, podemos pensar que la telefonía en *IP* es poco más que un juguete, pues la calidad de voz que obtenemos a través de Internet es muy pobre. No obstante, si en nuestra empresa disponemos de una red de datos que tenga un ancho de banda lo bastante grande, también podemos pensar en la utilización de esta red para el tráfico de voz entre las distintas áreas de la empresa. Las ventajas que obtendríamos al utilizar nuestra red para transmitir tanto la voz como los datos son evidentes:

- Ahorro de costos de comunicaciones pues las llamadas entre las distintas áreas de la empresa saldrían gratis.
- Integración de servicios y unificación de estructura.

Realmente la integración de la voz y los datos en una misma red es una idea antigua, pues desde hace tiempo han surgido soluciones desde distintos fabricantes que, mediante el uso de multiplexores, permiten utilizar las redes *WAN* de datos de las empresas (típicamente conexiones punto a punto y *frame-relay*) para la transmisión del tráfico de voz. La falta de estándares, así como el largo plazo de amortización de este tipo de soluciones no ha permitido una amplia implantación de las mismas. Figura 2.43

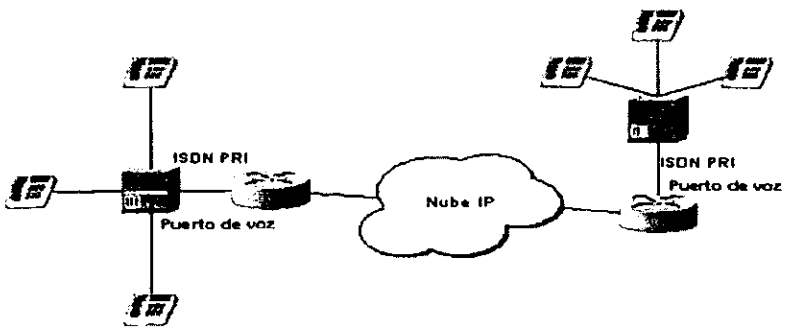


Figura 2.43 Ejemplo de red con conexión de centrales a routers que disponen de soporte VoIP.

Es innegable la implantación definitiva del protocolo IP desde los ámbitos empresariales a los domésticos y la aparición de un estándar, el VoIP, no podía hacerse esperar. La aparición del VoIP junto con el abaratamiento de los *DSP's (Digital Signal Procesor, Procesador Digital de Señal*), los cuales son claves en la compresión y descompresión de la voz, son los elementos que han hecho posible el despegue de estas tecnologías. Para este auge existen otros factores, tales como la aparición de nuevas aplicaciones o la apuesta definitiva por VoIP de fabricantes. Por otro lado los operadores de telefonía están ofreciendo o piensan ofrecer en un futuro cercano, servicios IP de calidad a las empresas.

Por lo dicho hasta ahora, vemos que nos podemos encontrar con tres tipos de redes IP:

- **Internet**. El estado actual de la red no permite un uso profesional para el tráfico de voz.
- **Red IP pública**. Los operadores ofrecen a las empresas la conectividad necesaria para interconectar sus redes de área local en lo que al tráfico IP se refiere. Se puede considerar como algo similar a Internet, pero con una mayor calidad de servicio y con importantes mejoras en seguridad. Hay operadores que incluso ofrecen garantías de bajo retardo y/o ancho de banda, lo que las hace muy interesante para el tráfico de voz.
- **Intranet**. La red IP implementada por la propia empresa. Suele constar de varias redes *LAN (Ethernet conmutada, ATM, etc..)* que se interconectan mediante redes *WAN* tipo *Frame-Relay/ATM*, líneas punto a punto, *RDSI* para el acceso remoto, etc. En este caso la empresa tiene bajo su control prácticamente todos los parámetros de la red, por lo que resulta ideal para su uso en el transporte de la voz.

A finales de 1997 el *VoIP* forum ha llegado a un acuerdo que permite la interoperabilidad de los distintos elementos que pueden integrarse en una red VoIP. Debido a la ya existencia del estándar H.323 del *ITU-T*, que cubría la mayor parte de las necesidades para la integración de la voz, se decidió que el H.323 fuera la base del *VoIP*. De este modo, el *VoIP* debe considerarse como una clarificación del H.323, de tal forma que en caso de conflicto, y a fin de evitar divergencias entre los estándares, se decidió que H.323 tendría prioridad sobre el *VoIP*. El *VoIP* tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, y estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia *(DTMF: Digital Tone Multifrecuency, Tonos Digitales Multifrecuencia)*.

El VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

- Direccionamiento:
  RAS (Registration, Admision and Status , Registro Adminitration and Status).
  Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través de el Gatekeeper.

DNS (Domain Name Service, Servicio de Nombre de Dominios). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS

- Señalización:
  Q.931 Señalización inicial de llamada
  H.225. Control de llamada: señalización, registro y admisión, y paquetización / sincronización del stream (flujo) de voz
  H.245. Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz

- Compresión de Voz:
  Requeridos: G.711 y G.723
  Opcionales: G.728, G.729 y G.722

- Transmisión de Voz:

UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.

RTP (Real Time Protocol, Protocolo en Tiempo Real). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

- Control de la Transmisión:
  RTCP (Real Time Control Protocol, Protocolo de Control en Tiempo Real). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

Hasta ahora sólo hemos visto la posibilidad de utilizar nuestra red IP para conectar las centrales a la misma, pero el hecho de que VoIP se apoye en un protocolo de nivel 3, como es IP, nos permite una flexibilidad en las configuraciones que en muchos casos está todavía por descubrir. Una idea que parece inmediata es que el papel tradicional de la central telefónica quedaría distribuida entre los distintos elementos de la red VoIP. En este escenario, tecnologías como *CTI (Computer-Telephony Integration, Integración Servidora Teléfono)* tendrán una implantación mucho más simple. Será el paso del tiempo y la imaginación de las personas involucradas en estos entornos, los que irán definiendo aplicaciones y servicios basados en VoIP. En la siguiente tabla observamos la pila de protocolos manejados en VoIP

<table>
<tr><td colspan="6">Establecimiento de llamada y Control</td></tr>
<tr><td colspan="6">Presentación</td></tr>
<tr><td colspan="2">Direccionamiento</td><td colspan="2">Compresión de audio G.711 ó G.723</td><td>DTMF</td><td>Direcciona-miento</td></tr>
<tr><td>RAS(H.225)</td><td>DNS</td><td colspan="2">RTP/RTCP</td><td>H.245 Q.931 (H.225)</td><td>DNS</td></tr>
<tr><td colspan="4">Transporte UDP</td><td colspan="2">Transporte TCP</td></tr>
<tr><td colspan="6">Red (IP)</td></tr>
<tr><td colspan="6">Enlace</td></tr>
<tr><td colspan="6">Físico</td></tr>
</table>

Tabla 2.7. Pila de protocolos en VoIP.

Actualmente podemos partir de una serie de elementos ya disponibles en el mercado y que, según diferentes diseños, nos permitirán construir las aplicaciones VoIP. Estos elementos son:

Teléfonos IP. Adaptadores para PC. Hubs Telefónicos.Gateways (pasarelas RTC / IP). Gatekeeper. Servicios de Directorio.

Dentro de los componentes de una red por IP podemos considerar los siguientes elementos que están ilustrado en la figura 2.44, de la cual podemos describir algunas características:

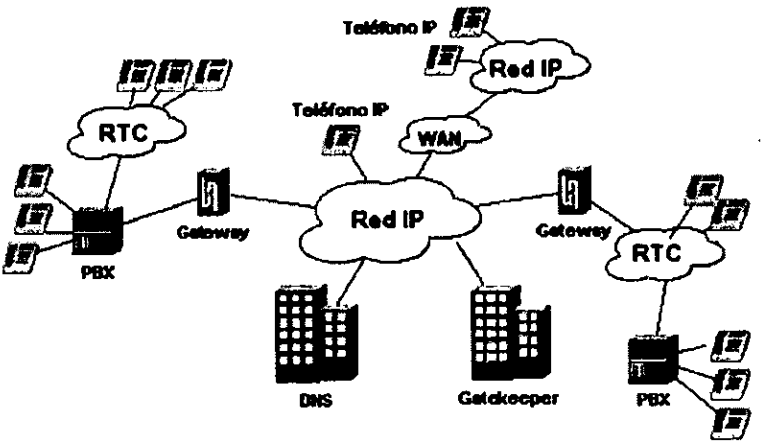


Figura 2.44. Elementos de una red VoIP.

El *Gatekeeper* es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de él. Su función es la de gestión y control de los recursos de la red, de manera que no se produzcan situaciones de saturación de la misma.

El *Gateway* es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica o *RDSI*. Podemos considerar al *Gateway* como una caja que por un lado tiene un interface LAN y por el otro dispone de uno o varios de los siguientes interfaces:

- FXO(Foreing Exchange Office). Para la conexión a extensiones de centrales ó a la red telefónica básica.
- FXS (Forein Exchange Station). Para conexión a enlaces de centrales o a teléfonos analógicos.
- E&M (Ear and Mouth). Para conexión específica a centralitas.
- BRI (Basic Rate Interface). Acceso básico *RDSI* (2B+D)
- PRI (Primary Rate Interface). Acceso primario *RDSI* (30B+D)
- G703/G.704 (E&M digital). Conexión especifica a centralitas a 2 Mbps.

Los distintos elementos pueden residir en plataformas físicas separada, o nos podemos encontrar con varios elementos conviviendo en la misma plataforma. De este modo es bastante habitual encontrar juntos *Gatekeeper* y *Gateway*.

Ventajas de la tecnología de VoIP

Dentro de las ventajas de este protocolo podemos mencionar las siguientes:

- Integración sobre su Intranet de la voz como un servicio más de su red, tal como otros servicios informáticos.
- Las redes IP son la red estándar universal para la Internet, Intranets y Extranets.
- Estándares efectivos (H.323).
- Interoperabilidad de diversos proveedores.
- Uso de las redes de datos existentes.
- Independencia de tecnologías de transporte (capa 2), asegurando la inversión.
- Menores costos que tecnologías alternativas (voz sobre TDM, *ATM*, Frame Relay)
- No paga servicio medido ni Larga Distancia en sus llamadas sobre IP.

2.7. Seguridad

En la actualidad la seguridad es parte importante de la administración de toda red, y es primordial, para aquellas que transportan información confidencial y crítica; llevándola al máximo cuando se debe hacer uso de la red pública por obvias razones de exposición. La filosofía de todo sistema de seguridad es reducir el riesgo a un nivel mínimo u aceptable, tomando las medidas apropiadas. La seguridad en una red de datos comprende los siguientes servicios generales:

- Identificación
- Autentificación
- Control de Acceso
- Confidencialidad
- Integridad
- No repudiación

A continuación se explica en forma breve cada uno de estos servicios.

Identificación

La identificación es la habilidad de saber quién es el usuario que solicita hacer uso del servicio. Una identificación ID (IDentification) de usuario es empleada para su reconocimiento.

Autentificación

La autentificación es la habilidad de probar que alguien es quien dice ser, es la prueba de identidad. El método más común de autentificar a un usuario es con el uso de una contraseña secreta que sólo el debe conocer.

Control de Acceso

Una vez identificado y autentificado un usuario, el sistema de seguridad decide qué se le permite hacer. Para ello se le otorgan derechos para el acceso a recursos de la red.

Confidencialidad

Es la protección de la información para que no pueda ser vista y entendida por un usuario no autorizado. La protección se proporciona de en dos modos:

- Mediante acceso restringido, limitando el acceso a sólo los usuarios autorizados.
- Mediante el uso de un código especial llamado de encriptación que modifica la estructura de la información haciéndola ininteligible.

Integridad

Es la cualidad que asegura que el mensaje es seguro, que no ha sido alterado. La integridad provee la detección del uso no autorizado de la información y de la red.

No repudiación

La no repudiación es la prevención de la negación de que un mensaje ha sido enviado o recibido y asegura que no se niegue esta acción. La propiedad de no repudiación de un sistema de seguridad de redes de datos se basa en el uso de firmas digitales.

2.7.1 Criptografía

La mayoría de los servicios de un sistema de seguridad pueden ser implementados usando técnicas de criptografía, también llamadas de encriptación.

La criptografía se define como la técnica que hace ininteligible (no legible) la información cuando es transmitida, convirtiéndola a un texto cifrado. En el receptor se restaura el texto cifrado a la forma original o texto claro con el proceso de criptografía inversa. En el proceso de encriptación se usa un algoritmo que transforma los datos a un texto cifrado, empleando una o más llaves de encriptación durante el proceso de transformación. El texto cifrado no es entendido por cualquier receptor sin el uso del algoritmo de encriptación y de la llave correcta para desencriptar la información.

Existen dos métodos básicos de encriptación:

- Modelo Simétrico o de llave privada
- Modelo Asimétrico o de llave pública

Modelos asimétricos, simétricos y one time hash

Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el cripto-sistema es simétrico o de clave secreta (ver figura 2.45). Estos sistemas

son mucho más rápidos que los de clave pública, y resultan apropiados para el cifrado de grandes volúmenes de datos.

Esta es la opción utilizada para cifrar el cuerpo del mensaje. Para ello se emplean algoritmos como IDEA, RC5, DES, 3DES, etc.

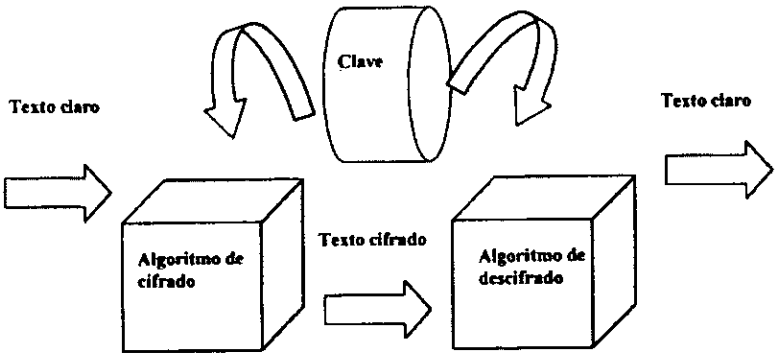


Figura 2.45. Modelo simétrico.

Por otro lado, cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el cripto-sistema es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, es conocida por todos. El sistema posee la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada ni descifrar el texto con ella cifrado. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión y firmas digitales, como se explicará posteriormente. Se utilizan los algoritmos de RSA.

En general, el cifrado asimétrico se emplea para cifrar las claves de sesión utilizadas para cifrar el documento, de modo que puedan ser transmitidas sin peligro a través de la Red junto con el documento cifrado, para que en recepción éste pueda ser descifrado. La clave de sesión se cifra con la clave pública del destinatario del mensaje, que aparecerá normalmente en una libreta de claves públicas. El cifrado asimétrico se emplea también para firmar documentos y autenticar entidades, como se describe a continuación en las firmas digitales.

Firma Digital

En principio, basta con cifrar un documento con la clave privada para obtener una firma digital segura, puesto que nadie excepto el poseedor de la clave privada puede hacerlo. Posteriormente, cualquier persona podría descifrarlo con la clave pública, demostrándose así la identidad del firmante. En la práctica, debido a que los algoritmos de clave pública son muy ineficaces a la hora de cifrar documentos largos, los protocolos de firma digital se implementan junto con funciones unidireccionales de resumen (hash), de manera que en vez de firmar un documento, se firma un resumen del

mismo. Este mecanismo implica el cifrado, mediante la clave privada del emisor, del resumen de los datos, que serán transferidos junto con el mensaje. Dentro de este procedimiento llamaremos A al usuario y B al servidor que realiza las transacciones. Éste se procesa una vez en el receptor, para verificar su integridad. Por lo tanto, los pasos del protocolo son:

1. A genera un resumen del documento.
2. A cifra el resumen con su clave privada, firmando por tanto el documento.
3. A envía el documento junto con el resumen firmado a B.
4. B genera un resumen del documento recibido de A, usando la misma función unidireccional de resumen. Después descifra con la clave pública de A el resumen firmado. Si el resumen firmado coincide con el resumen que él ha generado, la firma es válida.

De esta forma se ofrecen conjuntamente los servicios de no repudio, ya que nadie excepto A podría haber firmado el documento, y de autenticación, ya que si el documento viene firmado por A, podemos estar seguros de su identidad, dado que sólo él ha podido firmarlo. En último lugar, mediante la firma digital se garantiza asimismo la integridad del documento, ya que en caso de ser modificado, resultaría imposible hacerlo de forma tal que se generase la misma función de resumen que había sido firmada

Lo anterior se observa en la figura 2.46:

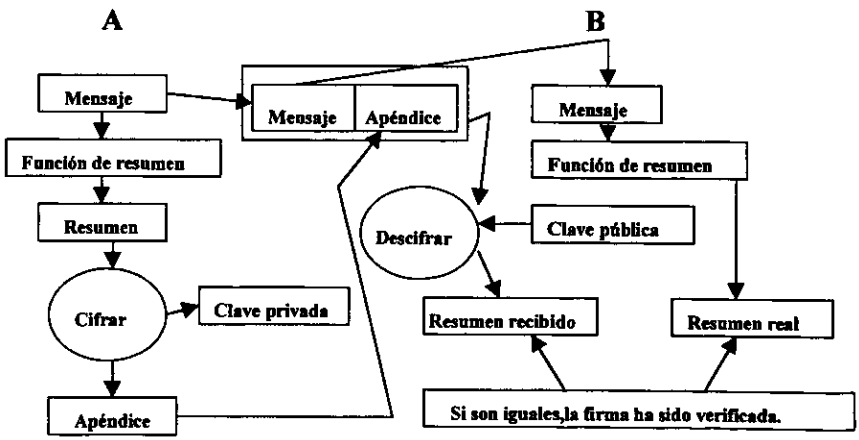


Fig. 2.46. Protocolo firma digital.

Protocolo SSL (Secure Socket Layer)

Un ejemplo comercial de la utilización de certificados es el SSL o (Secure Socket Layer,) que se basa en la utilización de certificados y que garantiza al día de hoy, si se realiza correctamente el comercio electrónico en internet. Este protocolo funciona de la forma que lo muestra la figura 2.47:

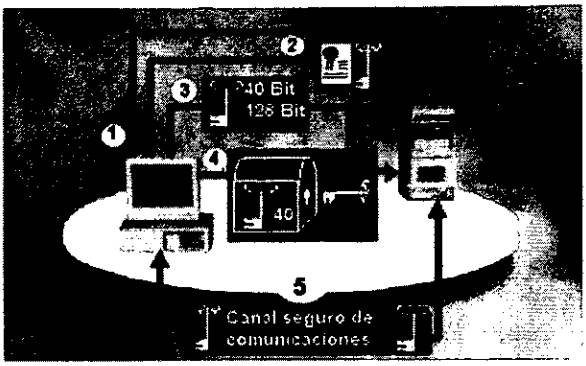


Figura 2.47. Esquema de funcionamiento del protocolo SSL.

El servidor de la Derecha podría ser el de un banco o para nuestro ejemplo una tienda de discos que vende sus productos por internet. Antes de comenzar con su negocio, crea un par de llaves una pública y otra privada y solicita un certificado a una autoridad de certificación, de manera que no haya dudas de que la llave pública de la empresa de discos es de la empresa de discos, esta llave pública sólo sirve para encriptar, y cualquier persona puede estar en posesión de ella. De hecho cada vez que un usuario quiere hacer una compra por primera vez, debe haberse bajado el certificado con la llave pública de la empresa de venta de discos. Una vez visto el contexto, veamos un ejemplo de compra por internet:

Paso 1: El usuario de la servidora de la izquierda, quiere comprar un CD de música por internet, para ello pondrá la dirección en su programa navegador, por ejemplo **http://www.musica-online.com,**el navegador conectará y pondrá **https://www.musica-online.com** en vez de: **http://www.musica-online.com.** Hay que darse cuenta que ha puesto **https** en vez de http, la **s** significa que estamos en un sitio seguro.

Paso 2: Pero como es la primera vez que nos conectamos, el navegador nos dará un mensaje, informándonos que no confiamos en esa empresa, puesto que no tenemos ningún certificado que la acredite, seguramente en la propia página web encontraremos algún vínculo donde *bajaremos* el certificado. Aparecerá una pantalla donde podremos leer el certificado, y nos pedirá si confiamos en él y si queremos instalarlo. Si el certificado es de nuestra garantía, es decir conocemos la autoridad certificadora, por ejemplo la Cámara de comercio electrónico de Madrid, la Agencia de Comercio electrónico o incluso nuestro Banco o Caja de ahorros entonces lo instalaremos. Aún estamos en el paso 2, hemos bajado el certificado de la empresa de discos, ahora pasamos al paso 3.

Paso 3: Ya tenemos la llave pública de la empresa de discos, podemos mandarle información confidencial, como por ejemplo nuestro numero de VISA. Pero la empresa no puede mandarnos información confidencial a nosotros puesto que no tiene nuestra llave pública ni ningún certificado que asegure que nosotros somos quien decimos ser. Para solucionarlo nuestro navegador empieza a negociar con el ordenador de la tienda de discos. Nuestro ordenador le pregunta al ordenador de la tienda de discos ¿Qué llave pública te mando, la de 40 o la de 128 bits. Acuerdan utilizar la de 40 bits por lo que nuestro navegador genera dos pares de llaves de 40 bits, una pública y otra privada. Nótese que en el dibujo se ven dos clases de llaves, son las públicas, las privadas no se ven puesto que son eso, privadas. Pasamos al paso 4.

Paso 4: Nuestro navegador, utilizando la llave pública de la empresa de discos, que sólo sirve para encriptar, es decir para cerrar, manda encriptada la llave pública de 40 bits que ha generado aleatoriamente nuestro navegador, puesto que es pública se podría haber mandado sin encriptar, pero aún así este proceso mejora la intimidad y la manda encriptada, para que nadie más que la tienda de discos conozca la transacción.

Paso 5: A la tienda de discos le llega la llave pública generada para esa transacción, puesto que ambas partes tienen la llave pública del otro, pueden establecer un canal seguro como se puede ver en el ejemplo de encriptación de datos del principio. El usuario mandará los datos de su VISA y verá en pantalla un recibo que podrá imprimir y utilizar en caso de reclamación. La empresa por su parte tendrá que comprobar los datos de la VISA por otro sistema, puesto que nadie le asegura a la empresa que el que compra es quien dice ser.

2.7.2. Integridad

El control de la integridad de la información se basa en el empleo de firmas digitales, que son resúmenes de mensajes cifrados. El resumen o procesamiento de un mensaje es un número, típicamente de entre 128 y 512 bits, obteniendo de la aplicación al mensaje de un algoritmo de resumen. Los algoritmos de resumen son básicamente funciones *hash*, es decir, toman una entrada (un mensaje), generalmente de longitud indefinida, y generan un pequeño número de longitud mucho menor de forma determinística (mensajes iguales generan siempre el mismo resultado). Lógicamente, puesto que el espectro de posibles resultados es mucho menor que el de posibles entradas, habrá muchos mensajes que generen el mismo resultado. Las funciones *hash* se usan normalmente en mecanismos de búsqueda (tablas de símbolos, compiladores, etc.) Los buenos algoritmos de resumen son funciones *hash* con dos propiedades adicionales:

Son irreversibles e impredecibles: es decir, dado un resumen no se puede encontrar un mensaje que le genere, ni invirtiendo el algoritmo ni intuyendo la naturaleza del mensaje que lo produjo.

Pequeños cambios en el mensaje producen cambios significativos en el resumen. Un simple cambio de un bit en el mensaje hace que aproximadamente la mitad de los bits del resumen cambien.

El mecanismo de control de integridad de un texto es el siguiente: una vez escrito el texto el autor genera el resumen mediante un algoritmo de resumen públicamente

conocido. Luego cifra ese resumen con su clave privada e incluye el resumen cifrado al final del texto. Cuando alguien va a leer el texto, para asegurarse de que no ha sido alterado toma el resumen cifrado del autor y lo descifra con su clave pública. Luego él mismo aplica el algoritmo de resumen sobre el texto y compara su resumen con el obtenido en su día por el autor. Si son distintos el mensaje ha sido alterado. En este mecanismo hemos de notar dos aspectos fundamentales:

Es esencial que el resumen esté cifrado por el autor, ya que si no alguien podría modificar el texto y generar un nuevo resumen. De este modo sin embargo el supuesto atacante al desconocer la clave privada del autor no tiene posibilidades de cifrar el nuevo.

La seguridad del mecanismo depende de que a partir de un resumen no se puedan encontrar mensajes que lo generen, ya que los posibles atacantes tienen acceso al resumen y se pueden encontrar más mensajes que lo generen y podría sustituir el mensaje original por cualquiera de dichos mensajes sin que lectores posteriores detectarán la alteración.

El ataque por fuerza bruta contra los algoritmos de resumen es improbable porque su tamaño de resumen de 128 bits, ya que por término medio habría que probar con 2128 mensajes antes de dar con uno que generara un resumen dado. Para hacernos una idea de lo que esto significa es poco probable que dos documentos escritos al azar durante toda la historia de la humanidad tengan el mismo resumen. Sin embargo estos algoritmos son sensibles al llamado ataque del cumpleaños, descrito por Yuval. Se basa en que efectivamente dado un resumen de "n" bits necesitan generar 2n/2 mensajes para dar con dos que generen el mismo resumen. Así, si trabajamos en una organización que utilice para la autenticación del correo electrónico resumen de 64 bits podríamos escribir dos mensajes completamente distintos, uno de ellos intrascendente (un permiso para salir una hora antes, por ejemplo) y otro más interesante (un permiso de tres meses de vacaciones pagadas). En cada uno de esos mensajes seleccionamos 32 palabras y buscamos un sinónimo para cada una de ellas generado después por ordenador los dos grupos de 232 posibles mensajes con sus correspondientes resúmenes. Lo normal según hizo notar Yuval es que encontramos al menos una pareja intrascendente, le pedimos a nuestro jefe que lo firme y luego lo sustituimos por el del otro grupo. El truco está hecho y la alteración es indetectable. Con resúmenes de 128 bits aun este ataque es hoy día improbable, pero no lo suficiente como para no crear inseguridad y hacer que se prefieran resúmenes más largos. Los algoritmos de resúmenes más comunes son:

- *MD2, MD4 y MD5*
- *SHA*
- *DES*

MD2, MD4 y MD5 (MD quiere decir procesamiento de mensaje o "*Message Digest*") son funciones de "*hash*" de amplia utilización que fueron diseñadas por Ron Rivest específicamente para su uso en criptografía. Producen resúmenes de 128 bits y no se conoce ningún ataque más rápido que supere en eficiencia a la búsqueda exhaustiva. *MD2* es la más lenta de las tres. *MD4* es la más rápida. *MD5* fue llamada por Rivest "*MD4* con cinturón de seguridad", ya que tiene un diseño más conservador que *MD4*. Su diseño proporciona mayor seguridad contra los ataques, pero es alrededor de un 33%

más lenta que *MD4*. *MD5* es, de los tres, el algoritmo más usado. *MD4* y *MD5* están disponibles al público para uso normal. Los detalles acerca de *MD2*, *MD4* y *MD5* con código de fuente están disponibles en los Internet RFCs (*Request For Comment*, Solicitud de Comentarios) 1319, 1320 y 1321 respectivamente.

SHA (*Secure Hash Algorithm*, *Algoritmo de Seguridad Hash*) fue desarrollado en el *NIST* (*National Institute of Standars and Technology*, *Instituto Nacional de Estandares y Tecnologia*) con ayuda de la *NSA* (*National Security Agency*, *Agencia de Seguridad Nacional*). Está relacionado con el *MD4*, y la principal mejora es que usa resúmenes de 160 bits en lugar de 128.

DES es el Estándar de Encriptado de Datos (*Data Encryption Standard*), un encriptado por medio de cifrado en bloque definido y endosado por el gobierno de los Estados Unidos en 1977 como estándar oficial. Los detalles se encuentran en la publicación oficial *FIPS* (*Federal Information Process System*, Sistema Federal de Transporte de Información). Fue desarrollado originalmente por *IBM*. *DES* se estudió extensivamente durante los últimos 15 años y es el sistema criptográfico más conocido y utilizado en el mundo. *DES* es un sistema criptográfico simétrico de clave secreta. Cuando se utiliza para comunicaciones, tanto el remitente como el receptor deben conocer la misma clave secreta que se usa tanto para encriptado como para el desencriptado del mensaje. El *DES* puede ser utilizado también por un solo usuario para encriptado: se pueden guardar archivos encriptados en un disco rígido. Si se utiliza en un medio de usuarios múltiples, distribuir la clave con seguridad puede llegar a ser un serio inconveniente; la criptografía con clave pública se ideó justamente para resolver este problema . *DES* opera en bloques de 64 bits con una clave de 56 bits. Fue diseñado para ser implementado en hardware y opera con relativa rapidez. Funciona para encriptar grandes cantidades de información. El *NIST* ha certificado cada 5 años al sistema *DES* como un estándar oficial de gobierno de los Estados Unidos, la última certificación fue efectuada en 1993. *NIST* indicó, sin embargo, que podrá no recertificar al sistema nuevamente.

Nunca se ha quebrantado el sistema *DES* a pesar de los esfuerzos de los investigadores durante los últimos años. El método obvio de ataque consiste en forzar una exhaustiva búsqueda del espacio de la clave lo cual toma operaciones de promedio. Tiempo atrás, se sugirió que un enemigo rico y poderoso podría construir una servidora especial para quebrantar el sistema *DES* en un lapso razonable. Más tarde, Hellman presentó un compromiso tiempo y memoria que permite mejorar las búsquedas exhaustivas si el espacio en memoria es abundante, luego de un exhaustivo procesamiento. Estas ideas sembraron dudas en cuanto a la seguridad del sistema *DES*. También ha habido dudas de que la *NSA* habría debilitado intencionalmente a *DES*. El costo de una servidora especial para realizar una búsqueda exhaustiva se calcula en un millón de dólares. Sin embargo, recientemente, Eli Biham y Adi Shamir, anunciaron el primer ataque a *DES* que es mejor que la búsqueda exhaustiva, utilizando una nueva técnica que se conoce como criptoanálisis diferencial. Este ataque requiere un encriptado de textos planos elegidos cuidadosamente, es decir elegidos por el atacante. Aunque es solamente un avance teórico, este ataque no podría llevarse a cabo en la práctica bajo circunstancias normales porque requiere que el atacante tenga fácil acceso al dispositivo *DES* para encriptar los textos por él elegidos. Otro ataque, conocido como criptoanálisis lineal no requiere de estos textos elegidos.

El consenso indica que *DES*, utilizado de forma apropiada, es seguro contra todo enemigo, excepto los más poderosos. En realidad, el encriptado 3 *DES* puede ser seguro absolutamente contra todos. Biham y Shamir han establecido que consideran seguro al *DES*. Se utiliza en una gran variedad de sistemas criptográficos, y prácticamente todos los sistemas criptográficos con clave pública lo utilizan en algún nivel.

Cuando se utiliza el sistema *DES*, existen diversas consideraciones prácticas a tener en cuenta que pueden afectar la seguridad de la información encriptada. Se deben cambiar las claves con frecuencia para prevenir ataques que requieran un sostenido análisis de la información. En un contexto de comunicaciones, se debe encontrar la forma de transmitir las claves con seguridad entre el remitente y el receptor. El uso del sistema de técnica de administración de clave, resuelve ambos problemas: se genera una clave *DES* diferente para cada sesión y la administración de claves segura lo proporciona el encriptado de la clave *DES* con la clave pública *RSA* del receptor. Bajo estas circunstancias, el sistema *RSA* se puede usar como una herramienta para mejorar la seguridad del *DES* . Si se desea encriptar archivos guardados en un disco rígido con el *DES*, no es posible cambiar las claves con frecuencia, ello significaría desencriptar y re-encriptar todos los archivos con cada cambio de clave. En cambio hay que tener una clave *DES* maestra con la cual encriptar la lista de claves utilizadas para encriptar los archivos, luego se podrá cambiar la clave maestra con frecuencia y poco esfuerzo.

Una técnica poderosa para mejorar la seguridad del *DES* radica en el encriptado triple, es decir, encriptar cada bloque de mensaje bajo tres claves *DES* diferentes. El encriptado triple se considera equivalente al doble del tamaño de la clave de *DES*, a 112 bits, y con ello se evita que cualquier enemigo sea capaz de buscar una sola clave y pueda desencriptar mensajes . Por supuesto, utilizar el encriptado triple lleva el triple de tiempo que un encriptado simple.

Aparte de las aplicaciones mencionadas, *DES* se puede usar para encriptado en diferentes formas oficialmente definidas, algunas son más seguras que otras. El modo *ECB* (*Electronic Code Book, Libro de Código Electrónico*) encripta cada bloque de texto plano de 64 bits uno después de otro bajo la misma clave de 56 bits. En el modo *CBC* (*Cipher Block Chaining, Cadena de Bloque Cifrado*), cada bloque de texto plano de 64 bits se encadena mediante la operación

2.7.3. Firewalls

La seguridad ha sido el principal punto a tratar cuando una organización desea conectar su red privada al Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el número de usuarios de redes privadas por la demanda del acceso a los servicios de Internet, tal es el caso del *World Wide Web* (WWW), *Internet Mail* (e-mail), Telnet, y FTP (*File Transfer Protocol, Protocolo de transferencia de archivos*). Adicionalmente los corporativos buscan las ventajas que ofrecen las paginas en el WWW y los servidores FTP de acceso público en el Internet.

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que de no ser así se expone la organización privada de sus datos, así como la infraestructura de su red a los expertos de Internet o mejor conocidos como hackers o piratas. Para superar estos temores, y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el

acceso *no-autorizado* de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información. Todavía, aun si una organización no está conectada al Internet, ésta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta.

Un *firewall* en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El *firewall* determina cual de los servicios de la red interna pueden ser accesados por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un *firewall* sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo, donde será inspeccionada la información. El *firewall* podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a éste.

Esto es importante, ya que debemos de notar que un *firewall* de Internet no es justamente un *router*, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El *firewall* es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. En la figura 2.48 se muestra por medio de un diagrama de bloques donde el *firewall* toma acción, éste se ubica entre la red y el acceso a Internet y deberá ser capaz de permitir el acceso a usuarios a Internet. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento.

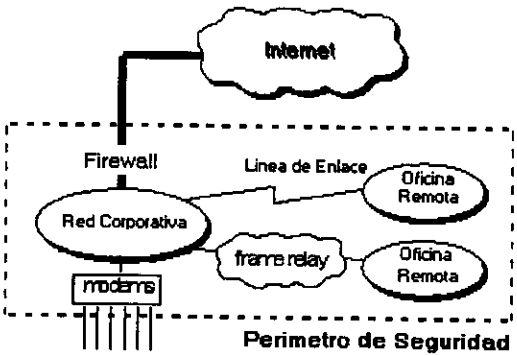


Figura 2.48. Diagrama a bloques de un Firewall.

Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

Los *firewalls* en Internet administran los accesos posibles del Internet a la red privada. Sin un *firewall*, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. El *firewall* permite al administrador de la red definir un

"*checkpoint*" (lugar de inspeccion), manteniendo al margen los usuarios no-autorizados fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un *firewall* en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema *firewall*, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

El *firewall* como lo muestra la figura 2.49. ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa , éste generará una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el tránsito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es "si", pero, cuándo? ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del tráfico significativo a través del *firewall*, también, si el administrador de la red toma el tiempo para responder a una alarma y examinar regularmente los registros de base.

Un sistema *firewall* de seguridad concentra la seguridad, centraliza los accesos, genera alarmas de seguridad, traduce direcciones, monitorea y registra servicios de WWW e Internet.

Con el paso de algunos años, el Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona. Por este medio se organizan las compañías conectadas al Internet, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios. Un *firewall* es un lugar lógico para desplegar un NAT(*Network Address Translator*,Traductor de Direcciones de Red), esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para re-enumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISPs, *Internet Service Providers.*).

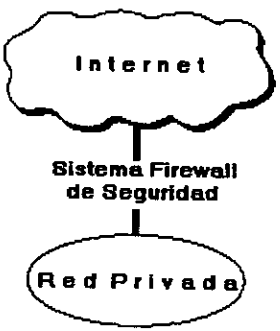


Figura 2.49. Monitoreo de seguridad.

La preocupación principal del administrador de red son los múltiples accesos al Internet, que se pueden registrar con un monitor y un *firewall* en cada punto de acceso que posee la organización hacia el Internet. Estos dos puntos de acceso significa dos puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente. Un *firewall* no puede protegerse contra aquellos ataques que se efectúen

fuera de su punto de operación. Por ejemplo, si existe una conexión sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una conexión al Internet. Los usuarios con sentido común suelen "irritarse" cuando se requiere una autenticación adicional requerida por un FPS (*Firewall Proxy Server* , *Servidor Apoderado del Proxy).* Este tipo de conexiones derivan la seguridad provista por el *firewall* construido cuidadosamente, creando una puerta de ataque como se muestra en la figura 2.50; donde los usuarios pueden estar consientes de que este tipo de conexiones no son permitidas como parte de integral de la arquitectura de la seguridad en la organización. El *firewall* no puede proteger contra los ataques provenientes del interior de la empresa, por ejemplo un *Hacker* que pretende ser un supervisor o un nuevo empleado despistado, persuade al menos sofisticado de los usuarios a que le permita usar su contraseña al servidor del corporativo o que le permita el acceso "temporal" a la red. Para controlar estas situaciones, los empleados deberían ser educados acerca de los varios tipos de ataque social que pueden suceder, y a cambiar sus contraseñas si es necesario periódicamente.

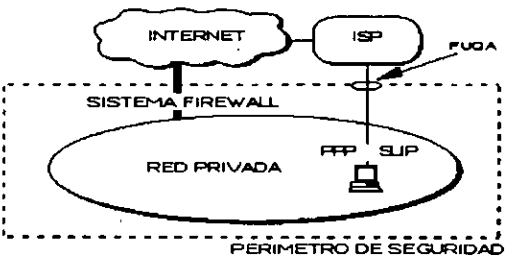


Figura 2.50. Creación de una puerta de ataque.

El *firewall* no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, el *firewall* de Internet no puede contar con un sistema preciso de SCAN (*System Control Antivirus Network*, Sistema de Control de Antivirus en la Red) para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él.

La solución real está en que la organización debe ser consciente en instalar software anti-virus en cada despacho para protegerse de los virus que llegan por medio de *disquetes* o cualquier otra fuente. Finalmente, el *firewall* de Internet no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparéntente datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando un ataque. Por ejemplo, una transferencia de datos podría causar que un servidor modificara los archivos relacionados a la seguridad haciendo mas fácil el acceso de un intruso al sistema. Como nosotros podemos ver, el desempeño de los servidores *Proxy* en un servidor de defensa es un excelente medio de prohibición a las conexiones directas por agentes externos y reduce las amenazas posibles por los ataques con transferencia de datos.

Un firewall típico se compone de uno, o una combinación, de los siguientes obstáculos.

- Router *Filtra-paquetes.*

- Gateway *a Nivel-aplicación.*
- Gateway *a Nivel-circuito.*

A continuación se discutirá cada una de las opciones para la edificación de obstáculos y se describirá como se puede trabajar junto con ellos para construir un efectivo sistema *firewall* de Internet.

Router filtra-paquetes

Este router toma las decisiones de rehusar ó permitir el paso de cada uno de los paquetes que son recibidos. El router examina cada datagrama para determinar si éste corresponde o no a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado, el puerto fuente , el puerto destino , el tipo de mensaje, la interface de entrada del paquete, y la interface de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, este será desplazado de acuerdo a la información a la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado. Si estos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete. En la figura 2.51. se muestra una representación en bloques del router filtra paquetes.

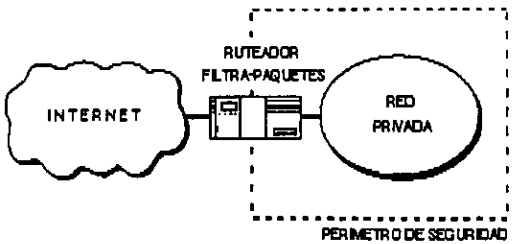


Figura 2.51. Esquema de un router filtra paquetes.

Este tipo de ataques ciertamente son difíciles de identificar usando la información básica de los encabezados debido a que estos son independientes al tipo de servicio. Los *routers* pueden ser configurados para protegerse de este tipo de ataques, pero son más difíciles de especificar por ello las reglas para el filtrado, ya que estas requieren de información adicional que pueda ser estudiada y examinada por la tabla de ruteo, inspeccionando las opciones específicas IP, revisando fragmentos especiales de edición, etc. Algunos ejemplos de este tipo de ataques incluye:

- Agresiones Originadas Por El Direccionamiento IP.
- Agresiones Originadas En El Router.
- Agresiones Por Fragmentación.

Agresiones Originadas por el Direccionamiento IP. Para este tipo de ataque, el intruso trasmite paquetes desde afuera pretendiendo pasar como servidor interno - los paquetes poseen una dirección fuente IP falsa de un servidor interno del sistema -. El agresor espera que usando este impostor se pueda penetrar al sistema para emplearlo seguramente como dirección fuente donde los paquetes que trasmita sean autentificados y los del otro servidor sean descartados dentro del sistema. Los ataques por seudo-fuentes pueden ser frustrados si descartamos la dirección fuente de cada paquete con una dirección fuente "interno" si el paquete llega en una de las interfaces del router "externo".

Agresiones Originadas en El Router. En un ataque de ruteo, la estación de origen especifica la ruta que un paquete deberá de tomar cuando cruce a través del Internet. Este tipo de ataques son diseñados para cuantificar las derivaciones de seguridad y encauzan al paquete por un inesperado camino a su destino. Los ataques originados en el router pueden ser frustrados simplemente descartando todos los paquetes que contengan fuentes de ruteo opcionales.

Agresiones Por Fragmentación. Por este tipo de ataques, los intrusos utilizan las características de fragmentación para crear fragmentos extremadamente pequeños y obligan a la información del encabezado TCP a separarse en paquetes. Estos pequeños fragmentos son diseñados para evitar las reglas definidas por el filtrado de un router examinando los primeros fragmentos y el resto pasa sin ser visto. Aunque si bien únicamente es explotado por sencillos decodificadores , una agresión pequeñisima puede ser frustrada si se descartan todos los paquetes donde el tipo de protocolo es TCP y la fragmentación de compensación IP es igual a 1.

Gateways a nivel-aplicación

Los gateways a nivel-aplicación permiten al administrador de red la implementación de una política de seguridad más estricta que la que permite un router filtra-paquetes. Mucho mejor que depender de una herramienta genérica de filtra-paquetes para administrar la circulación de los servicios de Internet a través del firewall, se instala en el gateway un código de propósito-especial (un servicio Proxy) para cada aplicación deseada. Si el administrador de red no instala el código Proxy para la aplicación particular, el servicio no es soportado y no podrán desplazarse a través del firewall. Aun cuando, el código Proxy puede ser configurado para soportar únicamente las características específicas de una aplicación que el administrador de red considere aceptable mientras niega todas las otras. Un aumento de seguridad de este tipo incrementa nuestros costos en términos del tipo de *gateway* seleccionado, los servicios de aplicaciones del Proxy, el tiempo y los conocimientos requeridos para configurar el *gateway*, y un decrecimiento en el nivel de los servicios que podrán obtener nuestros usuarios, dando como resultado un sistema carente de transparencia en el manejo de los usuarios en un ambiente "amigable". Como en todos los casos el administrador de redes debe de balancear las necesidades propias en seguridad de la organización con la demanda de "fácil de usar" demandado por la comunidad de usuarios. Es importante notar que los usuarios tienen acceso por un servidor Proxy, pero ellos jamás podrán seccionar en el *Gateway* a nivel-aplicación. Si se permite a los usuarios seccionar en el

sistema de *firewall*, la seguridad es amenazada desde el momento en que un intruso puede potencialmente ejecutar muchas actividades que comprometen la efectividad del sistema.

Un *router* filtra-paquetes permite la circulación directa de los paquetes dentro y fuera del sistema, diferente a esto el *Gateway* a nivel-aplicación deja que la información circule entre los sistemas pero no permite el intercambio directo de paquetes. El principal riesgo de permitir que los paquetes se intercambien dentro y fuera del sistema se debe a que el servidor residente en los sistemas de protección de la red podrá ser asegurado contra cualquier amenaza representada por los servicios permitidos, esto es el administrador debe cuidar a quien le concede privilegios para navegar sobre la red.

Un *Gateway* a nivel-aplicación por lo regular es descrito como un "servidor de defensa" porque es un sistema diseñado específicamente blindado y protegido contra cualquier ataque. Hay varias características de diseño que son usadas para hacer más seguro un servidor de defensa, éstas se definen a continuación:

Telnet proxy

La Figura 2.52. ilustra la operación de un Telnet Proxy en un servidor de defensa. Para este ejemplo, un cliente externo ejecuta una sesión Telnet hacia un servidor integrado dentro del sistema de seguridad por el *Gateway* a nivel-aplicación. El Telnet Proxy nunca permite al usuario remoto que se registre o tenga acceso directo al servidor interno. El cliente externo ejecuta un telnet al servidor de defensa donde es autorizado por la tecnología de contraseña de "una sola vez". Después de ser autentificado, el cliente obtiene acceso a la interface de usuario del Telnet Proxy. Este únicamente permite un subconjunto de comandos Telnet y además determina cual de los servidores son disponibles para el acceso vía Telnet.

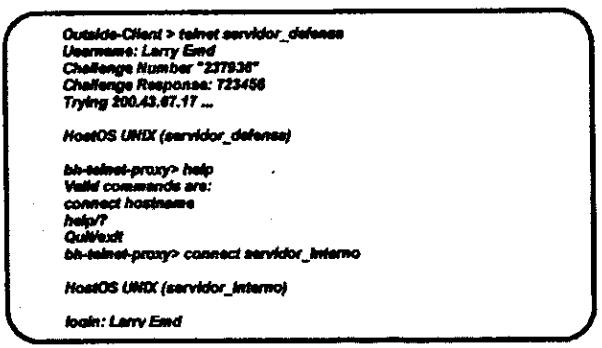


Figura 2.52. representación de un Telnet Proxy.

Los usuarios externos especifican el servidor de destino y el Telnet Proxy una vez hecha la conexión, los comandos internos son desplazados hacia el cliente externo. El cliente externo cree que el Telnet Proxy es el servidor interno real, mientras el servidor interno cree que el Telnet proxy es un cliente externo.

***Gateway* a nivel-circuito**

Un *Gateway* a nivel-circuito es en si una función que puede ser perfeccionada en un *Gateway* a nivel-aplicación. A nivel-circuito simplemente trasmite las conexiones sin cumplir cualquier proceso adicional en filtrado de paquetes. En la figura 2.53 se muestra la operación de una conexión típica Telnet a través de un *Gateway* a nivel-circuito. Tal como se mencionó anteriormente, este *gateway* simplemente trasmite la conexión a través del *firewall* sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de Telnet. El *gateway* a nivel-circuito acciona como una cable copiando los *bytes* antes y después entre la conexión interna y la conexión externa. De cualquier modo, la conexión del sistema externo actúa como si fuera originada por el sistema de *firewall* tratando de beneficiar el encubrir la información sobre la protección de la red.

El *Gateway* a nivel-circuito se usa frecuentemente para las conexiones de salida donde el administrador de sistemas somete a los usuarios internos. La ventaja preponderante es que el servidor de defensa puede ser configurado como un *Gateway* "híbrido" soportando nivel-aplicación o servicios Proxy para conexiones de venida y funciones de nivel-circuito para conexiones de ida.

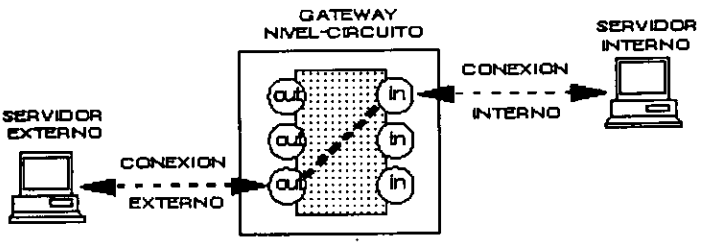


Fig. 2.53. Conexión típica a Telnet.

Después de hablar de la creación de partes que conformaran el modo de seguridad necesitamos hablar sobre los protocolos de seguridad a utilizar, dentro de estos tenemos los conocidos como Ipsec y Opsec los cuales describiremos a continuación:

IPSec(Internet Protocol Security, seguridad de Protocolo de Internet). Es un grupo de extensiones de la familia del protocolo IP. *IPSec* provee servicios criptográficos de seguridad. Estos servicios permiten la autenticación, integridad, control de acceso, y confidencialidad. *IPSec* provee servicios similares a SSL (*Secure Socket Layer*), pero a nivel de redes, de un modo que es completamente transparente para sus aplicaciones y mucho más robusto. Es transparente porque sus aplicaciones no necesitan tener ningún conocimiento de *IPSec* para poder usarlo. Puede usar cualquier protocolo IP sobre *IPSec*. Puede crear túneles cifrados VPNs(VirtualPrivate Networks, Redes Privadas Virtuales), o simple cifrado entre servidoras . Debido a que dispone de tantas opciones, *IPSec* es más bien complejo.
De un modo lógico, *IPSec* funciona en cualquiera de estos tres modos:

- Huésped-a-Huésped
- Huésped-a-Red
- Red-a-Red

En cualquier escenario en el que haya una red, el concepto de enrutamiento está implícito, como en Huésped-a-Enrutador (y este enrutador controla y cifra el tráfico para una *Red* particular).

IPSec se puede usar como túnel de tráfico para conexiones de VPN. Sin embargo, su utilidad va más allá de las VPNs. Con un registro central de IKE (*Internet Key Exchange, Intercambio de Claves de Internet*), cada máquina en internet podría comunicarse con otra y usar cifrado y autenticación fuerte.

OPSEC): *Open Plattform for Security* (Amplía las capacidades de la arquitectura *Secure Virtual Network* de *Checkpoint* con una amplia gama de soluciones certificadas *OPSEC* Certified. La arquitectura *OPSEC* permite la perfecta integración de soluciones de seguridad de múltiples fabricantes y la capacidad de gestión centralizada. Los productos y servicios certificados con *OPSEC* incluyen seguridad del contenido, detección de intrusiones, autentificación, alta disponibilidad, realización de informes y análisis de eventos, aplicaciones anti-virus, dispositivos de red y mucho más. Sin embargo es un servicio muy limitado en comparación con *IPSEC*,

2.7.4. VPNs

En una VPN (*Virtual Private Network, Red Privada Virtual*) todos los usuarios parecen estar en el mismo segmento de LAN, pero en realidad están en varias redes (generalmente públicas) a distancia. Para esta funcionalidad, la tecnología de redes seguras, privadas, y virtuales debe completar tres tareas: primero, deben ser capaces de pasar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos de LAN remotos no aparezcan estar separados por una red pública; segundo, la solución debe agregar encriptación, de manera que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado; y por último, la solución debe ser capaz de autentificar positivamente cualquier extremo del enlace de comunicación, de modo que un adversario no pueda acceder a los recursos del sistema.

Las razones que impulsan al mercado en ese sentido son, fundamentalmente, de costos: es mucho más barato interconectar filiales utilizando una infraestructura pública que desplegar una red físicamente privada. Por otro lado, como es lógico, es necesario exigir cierto criterios de privacidad y seguridad, por lo que normalmente debemos recurrir al uso de la criptografía.

Una VPN conecta los componentes de una red sobre otra red. Las VPN logran esto al permitir que el usuario haga un túnel a través de internet y/u otra red pública, de manera que permita a los participantes del túnel disfrutar de la misma seguridad y funciones que antes sólo estaban disponibles en las redes privadas. Esto lo observamos en la figura 2.54

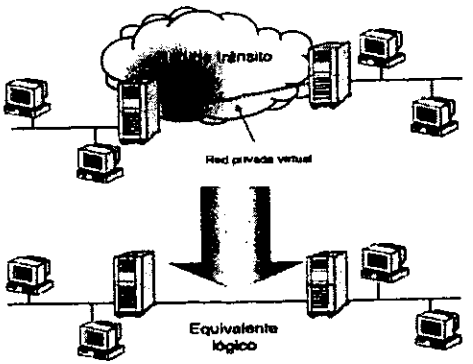


Figura 2.54. Red Privada Virtual.

Las VPN permiten a los usuarios que trabajan en el hogar o a los usuarios móviles conectarse en una forma segura a un servidor corporativo remoto, mediante la infraestructura de enrutamiento que proporciona una red pública (como Internet.)

Desde la perspectiva del usuario, la VPN es una conexión de punto a punto entre la servidora del usuario y un servidor corporativo. Por su parte, la naturaleza de la red intermedia es irrelevante para el usuario, debido a que aparece como si los datos se estuvieran enviando sobre un enlace privado dedicado.

La tecnología VPN también permite que una compañía se conecte a las sucursales o a otras compañías (extranet) sobre una red pública (como Internet), manteniendo al mismo tiempo comunicaciones seguras. La conexión de las VPN a través de Internet opera de manera lógica como un enlace de red de área amplia entre los sitios.

En ambos casos, una conexión segura a través de la red parece ante el usuario como una comunicación de red privada, no obstante que esta comunicación sucede sobre una red pública, de ahí el nombre de Red Privada Virtual.

La tecnología de la VPN está diseñada para tratar temas relacionados con la tendencia actual de negocios hacia mayores telecomunicaciones, operaciones globales ampliamente distribuidas, y operaciones con una alta interdependencia de socios, donde los trabajadores deben conectarse a recursos centrales y comunicarse entre sí.

Las redes privadas virtuales pueden ser relativamente nuevas, pero la tecnología de túneles está basada en estándares preestablecidos. La tecnología de túneles es un modo de transferir datos entre 2 redes similares sobre una red intermedia. También se llama encapsulamiento, a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de túneles VPN, añade otra dimensión al proceso ya que los paquetes están encriptados de tal forma que los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autentificación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor.

En general existen dos tipos de VPNs :

Enlaces Cliente-Red

En estos enlaces se encapsulan, típicamente utilizando el protocolo *PPP (Point-to-Point Protocol, Protocolo Punto a Punto)*. Las tramas del cliente se encapsulan en PPP, y el PPP resultante se encapsula para crear el VPN. Se aplican para:

- Acceso seguro de un cliente a la red.
- Clientes móviles (para independizarlos de la topología física).
- Puntos de acceso remoto. Por ejemplo, un "pool" de modems en otra ciudad, o clientes nuestros entrando por otro ISP.
- Rutado de tramas no utilizables en Internet. Por ejemplo, tramas NetBEUI, IPX, SNA o DECNET.

Enlaces Red-Red:

En este caso se está encapsulando el tráfico de una red local, por lo que nos ahorramos el paso PPP anterior. Las tramas de la LAN se encapsulan directamente para crear el VPN. Este tipo de enlace se utiliza para:

- Fundir dos redes locales a través de Internet, para que parezcan una sola.
- Establecer canales con privacidad, autenticidad y control de integridad, entre dos redes independientes.
- Rutado de tramas no utilizables en Internet. Por ejemplo, tramas NetBEUI, IPX, SNA o DECNET.

Por último, la solución debe garantizar la privacia y la integridad de los datos al viajar a través de una red corporativa. Por tanto, como mínimo, una solución de VPN debe proporcionar los siguientes aspectos:

Autenticación de usuario: La solución deberá verificar la identidad de un usuario y restringir el acceso de la VPN a usuarios autorizados. Además, deberá proporcionar registros de auditoría y contable para mostrar quién accedió a qué información y cuándo.

Administración de dirección: La solución deberá asignar una dirección al cliente en red privada, y asegurarse de que las direcciones privadas se mantengan así.

Encriptación de datos: Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.

Administración de llaves: La solución deberá generar y renovar las llaves de encriptación para el cliente y para el servidor.

Soporte de protocolos múltiple: La solución deberá manejar protocolos comunes utilizados en las redes públicas; éstos incluyen Protocolo de Internet (IP), Central de paquete de Internet (IPX), etc.

Una solución de VPN de Internet basada en un protocolo de túnel de punto a punto (PPP) o un Protocolo de túnel de nivel 2 (L2TP) cumple con todos estos requerimientos básicos, y aprovecha la amplia disponibilidad de Internet a nivel mundial.

Otra soluciones, incluido el Protocolo de seguridad IP (IPSec), cumplen con algunos de estos requerimientos, y siguen siendo útiles para situaciones específicas. Mas adelante vamos a analizar conceptos, protocolos y componentes de VPN con mayor detalle.

2.7.5. Protocolos de Seguridad

A continuación se listan los principales protocolos de seguridad utilizados en la tunelización o encapsulamentos de datos:

PPTP (Point-to-Point Tunneling Protocol)

Encapsulado de tramas PPP en datagramas IP, utilizando una versión extendida del GRE (Generic Routing Encapsulation, protocolo IP 47). La conexión de control se realiza sobre TCP, puerto 1723.
Actualmente este protocolo, aunque muy popular en el mundo Microsoft, está siendo sustituido por el L2TP. La implementación de Microsoft, además, sufre de varios importantísimos errores de diseño que hacen que su protección criptográfica sea inefectiva para alguien más motivado que un simple observador casual. No debería ser utilizada, por tanto.

L2TP (Layer 2 Tunnelling Protocol)

Encapsulado de tramas PPP sobre cualquier medio, no necesariamente redes IP. En el caso IP se usa UDP, puerto 1701. Tras un largo proceso como borrador, L2TP pasó a ser una propuesta de estándar en Agosto de 1999.

L2F (Layer 2 Forwarding)

Este sistema es el precursor del L2TP, y es utilizado en los routers CISCO, pero los trabajos en el L2TP lo han dejado obsoleto. Resulta útil, no obstante, si tenemos routers CISCO a nuestra disposición. Como L2TP, encapsula tramas PPP sobre medios arbitrarios.

IPSec

IPSec es el nuevo marco de seguridad IP, definido con el advenimiento del IPv6. Aunque IPv6 está muy poco difundido en este momento, la tecnología marco IPSec se está utilizando ya, lo que asegura, entre otras cosas, la interoperatividad de los sistemas de diversos fabricantes. Al menos en teoría. IPSec integra confidencialidad, integridad y autentificación en un mismo marco interoperante

IPIP (IP-in-IP)

IPIP define un encapsulado mínimo de los data gramas IP ya que, esencialmente, sólo se les añade una cabecera al principio. Este sistema es utilizado en redes "mobile-IP",

para independizar las direcciones IP de la topología física de la red en un momento dado. No define ningún mecanismo de cifrado o autentificación.
Linux soporta IP-in-IP de forma nativa a partir de los Kernel 2.0.x y 2.1.x, usando los LKM (Loadable Kernel Module)

Hemos concluido el capítulo donde se describen los conceptos básicos que se utilizarán en nuestro proyecto, a continuación procedemos a la fase de analizar la propuesta de proyecto.

CAPÍTULO 3

Análisis de la propuesta

La etapa del análisis, tiene como objetivo principal el conocimiento de las necesidades de la empresa y posteriormente la presentación de la propuesta de solución a la problemática planteada. El punto principal de esta etapa del proyecto es conocer detalladamente las necesidades de comunicación y transmisión de datos. Tomando como base lo anterior, estudiaremos los requerimientos y la implementación de servicios de voz y datos, para mejorar el desempeño de los procesos de la compañía y reducir costos de los servicios usados en la actualidad, para mantener comunicadas todas y cada una de las sucursales de WideCom con la central ubicada en el D. F.

El análisis de los sistemas es un proceso de descubrimiento, refinamiento y especificación en donde nosotros como desarrolladores del proyecto, el cliente, y sus usuarios jugamos un papel fundamental. Esta etapa nos facilitará el desarrollo del proyecto y nos permitirá ver claramente la función y rendimiento de los sistemas de comunicaciones y transmisión de voz y datos, la descripción de todos los elementos que componen las redes y las restricciones de diseño que debemos considerar en la implantación de los equipos.

En la etapa de análisis identificamos tres áreas importantes: (1) definición y análisis de los requerimientos, (2) evaluación de alternativas y (3) la selección de la propuesta final.

En principio debemos adquirir conocimientos de la empresa y de su operación, para entender perfectamente el papel que tendrá la red de voz y datos en la interacción de las sucursales de WideCom en el interior de la República Mexicana y la central. Nuestro objetivo aquí es reconocer los elementos básicos de los problemas tal como los percibe el cliente y el usuario final.

3.1. Análisis y Definición de los Requerimientos

En el análisis y definición de requerimientos de la red en cuestión es necesario el estudio de la red actual de la empresa WideCom, a fin de identificar y determinar los problemas para solucionarlos o mejorar los procesos. Un requerimiento es una característica que debe incluirse en la nueva red y puede consistir en una forma de transmitir o manejar datos, la manera en como se llevan las comunicaciones entre las sucursales, la central y los clientes.

Nuestro estudio se divide en tres partes, (1) red y datos, (2) voz y (3) seguridad, donde revisaremos su interacción con los procesos actuales del corporativo, para evidenciar los puntos débiles y definir los requerimientos.

3.1.1. Red de Datos

En la actualidad, en WideCOM existen redes locales aisladas en las sucursales, al igual que en la red de las oficinas centrales, con la diferencia de que en esta última se cuenta con una conexión a la Internet mediante una PC que posee un MODEM externo.

El crecimiento de la red es importante, pero la necesidad principal de la empresa es la integración de un sistema de administración de recursos corporativos. La red debe soportar aplicaciones que demanden grandes cantidades de ancho de banda, para ejecutar tareas de transferencia de archivos de forma precisa y segura. De manera general podemos englobar los requerimientos de la red de datos en dos grandes grupos: aquellos que están relacionados con la compartición de recursos y aquellos que tienen que ver con la segmentación de la red.

Compartición de recursos

Los problemas que dieron origen a la creación de las redes de computadora se trataron de manera general en el capítulo 2, donde la teoría e historia de las redes describe la manera en que la necesidad de compartir recursos en forma globalizada derivó en la creación de diferentes tecnologías, que permitieron la interconexión de lo que hasta ese momento trabajaba de forma independiente.

Para WideCOM, la integración de las redes locales para compartir recursos, no sólo implica la interconexión de las mismas en un ambiente general, sino que también representa una adecuación en la organización de archivos e impresoras, puesto que ahora, el corporativo debe contar con un esquema mejorado de redes cliente-servidor, para poder realizar las tareas de gestión y transferencias de archivos desde la central.

Segmentación de la red

La segmentación de la red es una característica de las redes modernas, que permite la eficiencia en el uso del ancho de banda dentro de las redes locales, que coopera con el transporte a nivel WAN, porque en los enlaces dedicados sólo viaja el tráfico necesario. De forma local, WideCOM cuenta actualmente tan sólo con concentradores, que repiten las tramas de datos provenientes de algún equipo a todos los puertos disponibles, y

aunque el número de equipos por sucursal no es muy elevado, las aplicaciones futuras requerirán que el tráfico que viaja (incluso a nivel local) esté bien justificado.

La red actual también carece de switches, que mejoran la segmentación en las redes locales, además de que poseen mecanismos para la creación de *VLANs (Virtual Local Area Network*, Redes de Área Local Virtual*)*.

3.1.2. Red de Voz

Por un lado está el problema de la Larga Distancia, que a pesar de los planes actuales de descuento y métodos de facturación simplificada, impide el control sobre la calidad del servicio.
La naturaleza del negocio de WideCOM, hace que la comunicación entre sucursales sea constante y requiere de la implementación de un sistema de voz que permita tener un control sobre el número de llamadas, y toda una serie de reportes completos sobre quién, cuándo y a dónde se han hecho las llamadas. El proyecto se complementará con un elemento de conectividad hacia la *PSTN* en cada sucursal, con un enlace dedicado y esto permitiría la integración de la antigua red conmutada con la que se propondrá. Los requerimientos anteriores encuentra una aplicación importante en WideCOM, porque los enlaces dedicados que se instalarán permitirán que la implementación de la voz sea un valor agregado que representa ahorros en servicios de comunicación entre sucursales y servicios *DISA (Direct Inward System Access*, Sistema de Acceso Entrante Directo*)*, estos últimos permitirán la asignación dinámica de extensiones telefónicas remotas mediante un código y que habilitarán los recursos del mismo tipo como si el usuario estuviera presente en la sucursal que accede.

3.1.3. Seguridad

En el aspecto de seguridad, WideCOM carece completamente de un esquema que implante políticas o restricciones de algún tipo. No podemos hablar de una problemática actual que se deba resolver, sino más bien de la ausencia total de un esquema de confiable de seguridad. Por ello, la justificación más importante en ese sentido, es la integración del sistema de administración de recursos y facturación en línea que debe garantizar, por un lado, la autenticación de los usuarios que gestionan al sistema, por otro, la integridad con la que los datos viajan y llegan a su destino sin haber sufrido cambios en tránsito; por último, la confidencialidad que asegura que sólo las partes involucradas en los mensajes pueden interpretar la información en forma correcta.

3.2. Evaluación de Alternativas

En esta sección revisaremos algunas de las tecnologías más usadas en la actualidad para la comunicación y transporte de datos en redes LAN y WAN, así como las opciones para montar esquemas de voz y de seguridad en las mismas.

3.2.1. Red de Datos

En el análisis de la red de datos hemos dividido el estudio de las redes de área local de las de área extensa, por lo que consideramos en primera instancia los protocolos de capa dos del Sistema OSI (Enlace de Datos) para WANs y posteriormente para las LANs

.Capa de Enlace de Datos para WAN

Entre los protocolos de Red (WÁN) más comunes necesarios para conectar una red local a otras redes remotas, y en otros casos para conectar una simple computadora personal a la red principal de WideCOM, encontramos los siguientes:

- Serial Line IP Protocol (SLIP).
- Point to Point Protocol (PPP).
- Frame Relay.
- ATM.

SLIP

El protocolo SLIP y su sucesor el protocolo PPP se diseñaron para proveer conexión telefónica (Dial Up) entre redes que usan el protocolo TCP/IP.
Las características más importantes de SLIP son:

- Fácil de implementar..
- Adiciona muy pocos bytes en el encabezado.
- No es un protocolo estandarizado para la internet.
- No efectúa detección ni corrección de errores (No verificación autenticidad).
- No es capaz de hacer transferencias simultáneas de múltiples protocolos. Sólo funciona con IP.
- Debe conocerse la dirección IP de cada extremo.
- Dos implementaciones hechas con SLIP no pueden trabajar juntas.

PPP

Este protocolo fue diseñado por la *IETF* (*Internet Engineering Task Force*, Fuerza de Tareas de Ingeniería para la Internet) para el direccionamiento de llamadas cortas con SLIP. PPP puede realizar las siguientes funciones:

- Podemos decir que su implementación no es muy compleja, aunque sí un poco más que la de SLIP.
- Incluye un encabezado de regular tamaño.
- Es un protocolo estandarizado para la Internet.
- Tiene suma de verificación (CRC) en cada marco según el entramado.
- Permite el direccionamiento dinámico de direcciones IP.
- Soporta múltiple protocolos en el mismo enlace (usando un campo que identifique los paquetes de protocolos de capas superiores).
- Provee acceso por contraseñas (verificación de autenticidad).
- Usa tecnología síncrona.
- Es configurable a través de LCP (*Link Control Protocol*, Protocolo de Control de Enlace).

Frame Relay

Fue diseñado para proveer transmisión estandarizada de paquetes de datos a gran velocidad en redes digitales. Algunas de sus características principales son:

- No hace revisión de errores al transmitir, por ello es tan rápido. La revisión de errores se hace en el punto receptor.
- Aplicaciones Frame Relay se pueden implementar en Ethernet y Token Ring.
- Puede ofrecer velocidades de 56 kbps hasta 1.544 Mbps.
- Es un protocolo orientado a paquetes diseñado únicamente para tráfico de datos. También puede funcionar como protocolo de control de acceso en ambientes de circuitos conmutados.
- Trabaja con X.25 y la red digital de servicios integrados. Puede además ser implementado como simple línea de interfaz de alto rendimiento para puentes y routers de redes locales.
- Puede implementarse en líneas de 56k, T-1 ó T-3.

ATM

La tecnología llamada ATM (*Asynchronous Transfer Mode*, Modo de Transferencia Asíncrona) es el corazón de los servicios digitales integrados que ofrecerán las nuevas redes digitales de servicios integrados de Banda Ancha (B-ISDN), para muchos ya no hay cuestionamientos; el llamado tráfico del "Cyber espacio", con gran crecimiento, impone a los operadores de redes públicas y privadas una voraz demanda de anchos de banda mayores y flexibles con soluciones robustas. La versatilidad de la conmutación de paquetes de longitud fija, denominadas celdas ATM, son las tablas más calificadas para soportar los requerimientos de la banda ancha. Otras de sus características principales son:

- Fue diseñado para ser independiente tanto como fuera posible de requerimientos de dispositivos físicos específicos con alta velocidad de proceso. Puede operar sobre enlaces T-1 y T-3, usando fibra en modo simple, multimodo, cableado STP o UTP.
- Su tasa de bits pre-especificada es de 155 Mbps y 622 Mbps.
- Normalmente ATM es considerado como protocolo de LANs y WANs.
- Toda la información se transporta en la red en pequeños bloques de 53 bytes llamados celdas.
- El flujo de datos es por rutas llamadas canales virtuales.
- Utiliza hardware simple basado en conmutación.
- Usa una unidad interredes (IWU, InterWorking Unit) para conectar diferentes redes. Una IWU incluye repetidores, puentes, ruteadores y gateways.
- La transmisión es del tipo síncrona.
- Tiene detección y control de errores.

Además es necesario tomar en cuenta el tipo de transmisión, por ello hacemos las siguientes referencias.

La transmisión asíncrona es una tecnología madura y poco complicada, típicamente es un 20 o 30 % del encabezado de cada transmisión de tramas y detección errores. No necesita hardware costoso en comparación con la transmisión síncrona, porque el transmisor y el receptor no necesariamente necesitan tener la misma señal de control. Debemos considerar que puede generar fallas de bits y que tiene una lenta transferencia de datos en comparación con la síncrona.

La transmisión síncrona es más eficiente que la transmisión asíncrona, capaz de trabajar con altas velocidades e incluir detección de errores, pero requiere de circuitería más costosa tanto en el transmisor como en el receptor.

En la tabla 3.1 se muestran algunas de las características más sobresalientes de las tecnologías mencionadas, en este apartado se presenta de manera clara, un comparativo de características relevantes de los cuatro protocolos analizados para las redes de área extensa. Nuestra mejor opción es el Protocolo PPP, porque se adapta completamente a nuestras necesidades de transferencia de datos, además que cuenta con notificación de errores y es muy confiable. Frame Relay adolece de la detección y corrección de errores y no es capaz de transportar voz por si mismo. Por su parte, ATM requiere de los servicios de la red de servicios integrados (RDSI).

	Frame Relay	ATM	PPP	SLIP
Trans. Síncrona	SI	SI	SI	SI
Trans. Asíncrona	NO	NO	SI	SI
Notificación de errores	NO	SI	SI	NO
Arquitectura en Entramado (relación con la capa inferior y superior)	NO	NO	SI	NO
Costo de instalación	Normal	Alto	Normal	Normal

Tabla 3.1. Comparativo de protocolos para redes WAN.

Capa 2 del modelo OSI (LAN)

En esta parte debemos tomar en cuenta le tipo de LAN que usaremos para la red global de WideCOM y para sus sucursales en el interior de la república incluyendo la LAN del corporativo en el D.F. Uno de los principales problemas en la red es el medio de acceso o las reglas que usaremos en nuestras LANs, para controlar los permisos de transmisión de datos. Es inimaginable una red con un gran número de computadoras sin un medio de acceso. Si todas las estaciones transmitieran al mismo tiempo, dando como resultado la combinación de señales y con ello la pérdida de los datos, existirán colisiones que destruirán los datos. Por esto es necesario controlar el medio de acceso para eliminar este fenómeno. A continuación se describen brevemente algunas características de las diferentes configuraciones de redes:

Ethernet

Algunas características del fenómeno de contención son: software relativamente simple, produce encabezados muy cortos, permite un control completo e inmediato del medio, el tiempo de acceso no predecible (probabilístico).

TokenRing

El paso del *token* produce carga predecible y retraso (determinístico), requiere software interactivo y relativamente complicado, ofrece la habilidad de asignar niveles de prioridad a las transmisiones de datos, lo que acelera el acceso al medio. Para esto es necesario ajustar los parámetros cada vez que se agrega o quita un dispositivo del medio, elimina las colisiones y ofrece una tasa alta de transmisión de datos en condiciones de cargas elevadas. Requiere de un control central para detectar y recobrar fallas.

FDDI

(Fibre Distributed Data Interface, Interface de Distribución de Datos por Fibra*)* consiste básicamente en un anillo de fibra óptica por paso de testigo. El paso de testigo "token-ring" se refiere al método por el que un nodo conectado al anillo FDDI accede a él. La topología en anillo se implementa físicamente con fibra óptica.

Los nodos no pueden transmitir datos hasta que toman el testigo. Este testigo es realmente una trama especial que se usa para indicar que un nodo libera el testigo. Cuando un nodo detecta esa trama y tiene datos que transmitir, captura a trama eliminándola del anillo, y lo libera cuando termina o cuando finaliza su tiempo de posesión del testigo.
FDDI proporciona interconexión a alta velocidad entre redes de área local (LAN), y entre éstas y las redes de área ancha (WAN). Las principales aplicaciones se han centrado en la interconexión de redes LAN Ethernet y de éstas con redes WAN X.25. Tanto en la conexión de estas tecnologías de red como con otras, todas se conectan directamente a la red principal FDDI (*backbone*). Otra aplicación es la interconexión de periféricos remotos de alta velocidad a equipos tipo *mainframe*.

Para garantizar el funcionamiento, cuando un equipo está desconectado, averiado o apagado, un conmutador óptico de funcionamiento mecánico realiza un puenteo del nodo, eliminándolo del anillo. Esta seguridad, unida al hecho de operar en velocidades de 100 Mbps bajo distancias de 100 km hacen de la FDDI una tecnología óptima para gran número de aplicaciones.

En la siguiente tabla se resumen las características referentes a Ethernet, TokenRing y FDDI.

	Ethernet	Token ring	FDD1
Determinístico	NO	SI	SI
Colisión	SI	NO	NO
Ocupación del Medio	Contención	Paso de Testigo	Paso de testigo

Tabla 3.2. Características de Ethernet, Token Ring, FDDI.

A continuación y después de haber descrito los procedimientos correspondientes al modelo OSI, capa 2, procederemos a describir los protocolos aplicables al modelo OSI capa 3.

Capa 3 del Modelo OSI

IP

- Actualmente, el conjunto de protocolos TCP/IP es el más popular juego de protocolos de comunicaciones y aplicaciones para conectar sistemas heterogéneos en diversos ambientes de la capa física.

- Son dos los protocolos más conocidos del juego de protocolos TCP/IP: el TCP, encargado de establecer la comunicación entre sistemas, y el IP, cuya tarea es la transferencia de datos.

- La porción IP provee direccionamiento y servicios de conexión para el envío de paquetes, también provee servicios de conmutación de paquetes.

- TCP/IP tiene características que lo hacen único para el uso en redes complejas; por ejemplo, una red IP puede dividirse en grupos lógicos que comúnmente son llamados sistemas autónomos. Estos grupos pueden ser administrados por la misma autoridad.

- Existen otras ventajas tales como los servicios *HTTP , FTP(File Transfer Protocol,* Protocolo de Transferencia de Archivos*), y SMTP(Simple Mail Transfer Protocol,* Protocolo Simple de Transferencia de Correo*),* por otro lado, todos las computadoras que accesan o que tienen acceso al uso de internet usan TCP/IP.

- TCP/IP es un juego de protocolos abiertos para la industria estándar que puede ser agregado para las más comunes arquitecturas de internet.

IPX

Lo que se conoce como IPX/SPX consiste realmente en una variedad de protocolos tales como: *IPX (Internetworking Packet Exchange,* Intercambio de Paquetes Interredes*), SPX (Sequential Packet Exchange,* Intercambio de Paquetes Secuencialmente*), NCO (Netware Core Protocol,* Protocolo de Red Core*), SAP (Service Advertising Protocol,* Protocolo de Servicio de Advertencia*), RIP (Router Information Protocol,* Protocolo de Información de Ruteo*),* y otros.
A continuación se describen las características más importantes de IPX/SPX que se utilizan en el presente trabajo.

- IPX es un protocolo de conexión de la capa de red, sus funciones son el direccionamiento y el ruteo dentro de la red, mientras que SPX es un protocolo de la capa de transporte que ofrece conexión orientada a la liberación de paquetes, usando circuitos virtuales llamados conexiones.

- El uso de este protocolo no garantiza la entrega de paquetes de datos, es decir que cada paquete se trata como una entidad individual, sin considerar ninguna relación lógica o secuencial con cualquier otro paquete.

- Es un protocolo sin conexión, es decir, transmite datos a un nodo remoto, pero no espera una respuesta o una confirmación indicando si los datos han sido recibidos con éxito.

- Es un protocolo direccionable.

- Cuenta con código de redundancia para corrección de errores.

- Aunque IPX tiene bastantes ventajas al igual que TCP/IP, no es un protocolo abierto, por ello su auge ha venido a menos, porque su uso se cierra a las aplicaciones de internet.

- La aplicación de este protocolo fundamentalmente es el intercambio de paquetes de datos, no se usa con aplicaciones de video o voz.

En la siguiente tabla hacemos un resumen de las características analizadas anteriormente.

	IP	IPX
Grupos	SI	SI
Ruteables	SI	SI
Ruteados	SI	SI
Std. Abierto	SI	NO

Tabla 3.3. Características IP e IPX.

3.2.2. Red de Voz

Las alternativas para el manejo de la voz en la red que se implantará, están basadas en los esquemas tradicionales de voz, cuyos orígenes se hallan ubicados en los sistemas de modulación introducidos en el capítulo de conceptos básicos. La forma en que se evaluarán las soluciones a considerar consiste en comparar parámetros de señalización y empaquetamiento que, dependiendo de las condiciones de los enlaces de comunicación del diseño de datos, definirán cuando unos son más convenientes que otros. En particular, se debe hacer notar que no habrá una decisión como tal en cuanto a la elección de interfaces analógicas sobre digitales, ya que ambas son requeridas por el tipo de sucursales y el volumen de llamadas esperado. Para ahondar en este punto, el diseño de la red de voz estará dividido de la siguiente forma: por un lado, las sucursales en su totalidad emplearán un esquema de voz analógica; mientras que las oficinas centrales recibirán los enlaces digitales, los descanalizarán, los descomprimirán y finalmente los enrutarán hacia un conmutador telefónico más grande en forma digital. La figura 3.1 muestra el primero de dos esquemas generales de voz para dar solución a la red empleando el transporte de datos que se instalará para WideCom.
Este modelo no propone ningún tipo de reemplazo en una red telefónica convencional, ya que los equipos de comunicaciones al borde (equipos instalados al equipo de comunicaciones del carrier sin pertenecer a su red) de la red WAN emulan pequeñas centrales telefónicas, con la capacidad de proveer los tonos y la señalización adecuada

para que los conmutadores pequeños en las oficinas crean que se están enlazando a la nube PSTN. De hecho, este modelo puede incluir conexiones a esta última red con el objetivo de conectarse al resto del mundo, al igual que conservan el tendido del cableado telefónico por separado para la conexión a cada uno de los dispositivos telefónicos.

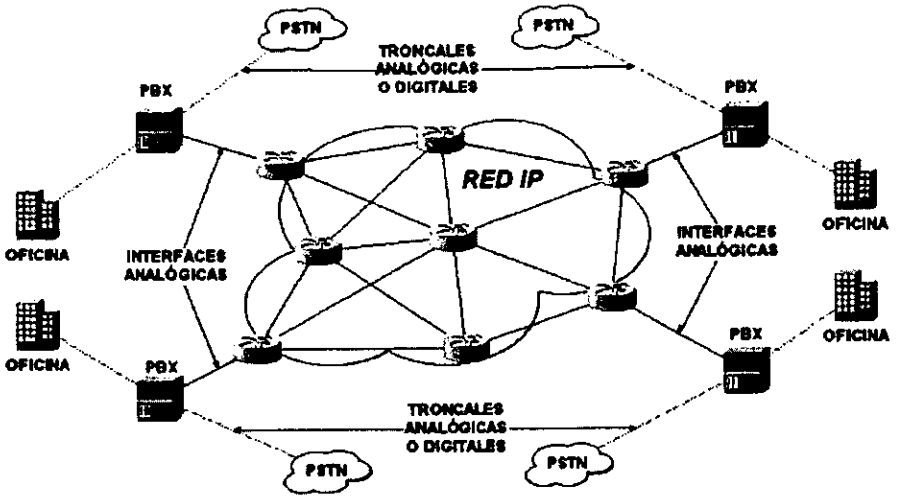


Figura 3.1. Esquema analógico-digital para la red de voz.

El otro esquema es completamente digital, y está bosquejado en la figura 3.2, en él se eliminan por completo los equipos convencionales al igual que el cableado telefónico. Además se incluye el manejo de datos.

Como se observa en la figura 3.2, se introducen nuevos dispositivos conocidos como Gateways de voz, debido a que son capaces de interpretar la señalización telefónica tanto analógica como digital, transmiten por protocolo IEEE 802.3 a través de un switch de capa 2, y de ahí se distribuyen al resto de la red de datos aprovechando el cableado ya instalado. Aunque no se muestra en la figura, esta propuesta plantea la conexión en línea de los equipos de cómputo a los teléfonos IP por medio de cable UTP, y a través de la implementación interna de hubs de datos dentro de los teléfonos. Esta solución se muestra en la figura 3.3.

De los dos modelos, el de la figura 3.2 es más atractivo por las ventajas que ofrece el usar un solo cableado y por las características digitales que puede aportar toda esta instalación; no obstante, representa una mayor inversión y está proyectado para su implementación en proyectos nuevos, porque descarta de entrada el tendido del cableado telefónico. De esta forma, el resto de esta sección del capítulo se concentrará en la comparación de las técnicas de señalización de voz para el modelo analógico digital, debido a que es el esquema que mejor se ajusta a las redes locales y telefónicas que actualmente existen en el corporativo WideCom. Como se apuntó al inicio de esta sección, no hay una exclusión entre las técnicas analógicas y digitales de la modulación para las señales analógicas, ya que éstas estarán presentes en la solución final del

proyecto; sin embargo, es conveniente retomar los mecanismos existentes para después hacer una decisión basada en sus características más fuertes y sus desventajas más perjudiciales. Desde este momento, nuestro análisis se dividirá en tres partes, por un lado la modulación, en donde mencionaremos las técnicas actuales y la elección hecha con su justificación. Después avanzaremos al aspecto de señalización para enlaces de voz en sus ramas, digital y analógica. Finalmente, el aspecto de paquetización de voz en redes de datos en donde mencionaremos el porque de la elección de voz sobre el protocolo IP.

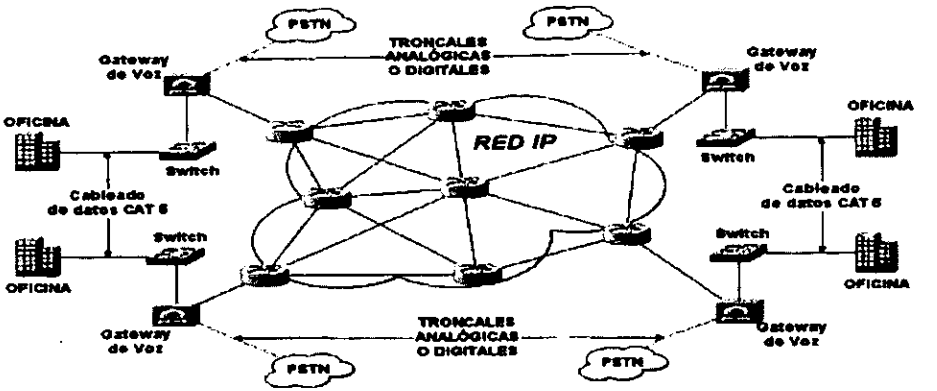


Figura 3.2. Modelo de redes convergentes para voz y datos.

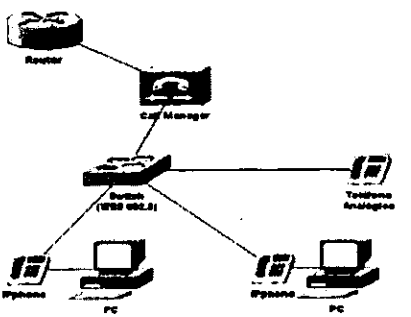


Figura 3.3. Implementación de Ipphones con Call Manager.

Modulación

En el sentido estricto, la modulación analógica como tal es empleada actualmente en la transmisión de señales de radio comerciales, y el rango de frecuencias está completamente dividido y repartido para todas las asociaciones, desde las no lucrativas hasta las organizaciones militares y gubernamentales. El explicar como está conformado completamente el espectro cae fuera del presente trabajo; no obstante, las modulaciones más usadas están dentro de las bandas de AM (Amplitud Modulada) o bien dentro de

las bandas de FM (Frecuencia Modulada.) En ambos casos, la intención es emplear una señal de alta frecuencia como portadora y modularla mediante la amplitud o la frecuencia, según se desee.

Para nuestro caso se hará uso de la modulación por codificación de pulso, que con base en el estándar G.711 permite tomar muestras a 8000 veces por segundo, y de donde se deriva el ancho de banda mínimo para transportar la voz, que además sirve de base para la estructura de las jerarquías de PDH, tanto en la norma europea como en la americana. Desde luego, las implementaciones modernas no envían la voz con este requerimiento de ancho de banda, sino que emplean técnicas de compresión (estándar G.749) para reducir el requerimiento hasta en 8000 kbps y hacer un uso más eficiente de los enlaces existentes para transportar datos, voz y en algunas ocasiones hasta video.

En cuanto al aspecto de transmisión de datos por líneas conmutadas a 33,600 kbps, nos interesa la modulación digital para el envío de señales digitales por medio de la red PSTN, que es una red completamente analógica. En ese aspecto, existen tres opciones de modulación a considerar: ASK, FSK y PSK, las tres son conocidas como *keying* (llaveos o modulaciones) conforme lo establezca la amplitud, la frecuencia o el cambio de fase. La elección para este caso, es la modulación por cambio de fase, la cual ha demostrado ser mucho más confiable, porque es menos susceptible al ruido de las líneas y la inductancia eléctrica inherente en los postes donde viajan conjuntamente tanto líneas eléctricas como telefónicas. Una prueba que demuestra la eficacia de este mecanismo es que, a nivel de redes locales, la señalización eléctrica para la norma IEEE 802.3 (Ethernet), utiliza codificación Manchester Diferencial, la cual consiste de indicaciones de estados binarios mediante el cambio de voltajes referenciados entre sí y no a una tierra en común, lo que explica la naturaleza del cableado de par trenzado y que ha sido probado satisfactoriamente por cierto tiempo.

Señalización

Los esquemas de señalización de voz sirven como protocolos de comunicación entre las centrales telefónicas y los equipos privados PBX o residenciales y establecen estados para el progreso de una llamada común. Estos estados se detallaron en el capítulo 2 y la mayoría de las técnicas de señalización existentes, se implementan con ciertas variaciones según se trate del país donde opera. Para el proyecto de WideCom, debemos hacer de nuevo una división entre las técnicas analógicas y digitales. En las primeras, habremos de hacer una elección entre el tipo de arranque de las señales de supervisión ya sea para LS (Loop Start) o para GS (Ground Start); mientras que en la señalización digital simplemente describiremos el funcionamiento básico de *MR2 (Modified R2, R2 Modificado)*.

En cuanto a los arranques de la señalización analógica, existe una clara ventaja de GS sobre LS, ya que esta última supone un estado libre que preceda el inicio de llamadas, lo cual no siempre ocurre porque es posible que, al momento de descolgar el auricular de un equipo que está por recibir una llamada, puede entrar la llamada del otro extremo, lo que provoca que el voltaje de AC que emplea la central para indicar la llamada se le regrese y pueda producir daños a los circuitos. El arranque GS resuelve este problema simplemente agregando un componente de detección de tierra, al cual se conmutan las líneas TIP y RING para indicar el cierre del loop y evitar que exista un voltaje de retorno por la indicación del timbrado en las llamadas entrantes. De esto se desprende

que la elección del tipo de arranque precise que los equipos soporten esta señalización. En general, los equipos en donde se instalarán las tarjetas de voz son capaces de manejar ambas señalizaciones y la conexión de las líneas TIP y RING debe hacerse con el cuidado de enlazar al detector de tierras cada circuito que corresponda y que recibe dicha conexión.

La señalización MR2 está especificada por las normas Q.400 a Q.490n de la ITU-T y su conexión física está determinada por el estándar G.704 (cable coaxial RG-59 a 75ohm, balanceados o desbalanceados.) para recibir un enlace E1 que contiene 2.048Mbps. Este E1 está controlado por *CAS (Channel Associated Signaling, Señalización por Canal Asociado)*, lo que significa que dentro de cada trama de 2 megas se utiliza el canal o *time slot* 0 para sincronización y el canal 16 para llevar el control de los bits de progreso de llamada.

Dentro de la MR2 existen dos tipos de señalización involucrados: la señalización en línea y la señalización Inter registros. La primera se usa para indicar los estados de la llamada basados en los valores de los bits ABCD, según sea hacia delante la comunicación o hacia atrás; mientras que la segunda indica el contenido de la llamada y guarda en su entramado los datos del origen de la llamada, el tipo (tránsito, mantenimiento, etc.) categorías, etc.

La señalización MR2 se ocupará para enlazar al conmutador central el enlace E1 que proviene del equipo de datos y que contiene los canales de voz descomprimidos desde cada una de las sucursales. Por lo mismo, aunque existen señalizaciones modernas como Qsig para la recepción de enlaces digitales, su adecuación a los tonos de México aún está en etapa de pruebas por lo que se elige la técnica probada.

Empaquetamiento

La etapa de encapsulado de la voz por algún protocolo de transporte merece especial atención, ya que ésta determinará la calidad de voz que se prueba de forma subjetiva tal y como se mencionó en el capítulo 2. Realmente, de las opciones de que se dispone para el transporte de la voz (IP, Frame Relay y ATM) ninguno de estos protocolos corresponde a la capa de transporte en el modelo OSI; de hecho, sólo uno de ellos se refiere a la red como tal, mientras que el resto se basa en el medio asegurado para transportar la voz. A continuación haremos un análisis del manejo de los servicios especiales para cada protocolo que se tiene opción.

Básicamente, y tal como se mencionó en el capítulo 2, Frame Relay presupone que el medio es altamente confiable, y las tramas que viajan a nivel 2 son muy ligeras, lo que aminora el tiempo de retraso en las redes. El problema con los servicios sensibles al retraso (como la voz) es que en la mayoría de las topologías ofrecidas por los proveedores, este retraso no puede ser garantizado del todo por las rutas dentro de la infraestructura Frame Relay de dicho proveedor. En ese sentido, estamos apegados a la disponibilidad de la red en picos de demanda que pueda soportar la red del proveedor y eso implica una falta de control en la voz.

Por su parte, ATM es una técnica moderna basada en el switcheo de celdas muy pequeñas y que preestablece una ruta (al igual que Frame Relay) antes de enviar la carga útil. ATM puede variar la tasa con la que envía a estas celdas según se trate de un servicio "del mejor esfuerzo" o "garantizado" y esta es la clave que nos permite diferenciar con las otras dos opciones de empaquetamiento de la voz. ATM contempla de forma implícita un nivel de servicio adecuado para la voz y posee una infraestructura (medio) más que adecuada para este tipo de datos, porque los switches ATM etiquetan las celdas que contienen la voz y éstas reciben el mejor servicio (mejor incluso que en una red IP.) A pesar de todas las bondades presentadas por esta red de alta velocidad, ATM es una red demasiado cara de implementar y de mantener, lo que no justifica sus canales casi ilimitados para el tipo de aplicación que requiere WideCom.

El empaquetamiento de la voz por IP resulta ser la mejor elección para el transporte, por las características de calidad de servicio configurables en los nodos de conmutación por donde viaja la voz. El protocolo IP en particular permite definir niveles de distribución de los paquetes aún dentro de su mecanismo del mejor esfuerzo (la confiabilidad se lleva a cabo en las capas superiores) y esto da flexibilidad a los requerimientos de cada sucursal donde se implementará la voz por encapsulado. Las características de los equipos que soportarán a la voz y a los datos, no solo tienen una variedad amplia en el manejo de la compresión de la voz, sino también en el tipo de encolamiento en los routers, lo que permite cambiar dinámicamente el apilamiento de los paquetes en espera, para dar paso a los datos que son sensibles al retraso. Además, una característica novedosa es el control de contenidos que permite hacer todavía más selectivo el orden con el cual se despachan los paquetes en una red de datos no solamente con aquellos marcados como de alta prioridad.

3.2.3. Seguridad

El aspecto de seguridad, como se implantará en la red de WideCom, está compuesto por tres secciones principales, y de las cuales se derivan el resto de los detalles que tienen por objeto el proveer autenticidad, integridad y confidencialidad, que son los bloques principales con los que se construye cualquier arquitectura de seguridad. Estos aspectos consisten en:

- La seguridad entre sucursales y oficina central por enlace dedicado.
- La seguridad en al accesos hacia y desde la Internet.
- La seguridad entre sucursales y oficina central por dial-up.

La figura 3.4 muestra estos aspectos, indicando que la conexión por dial-up puede realizarse tanto por los enlaces privados como por los enlaces públicos, esto es por la PSTN.

A continuación se detallarán estos tres aspectos mencionados, de forma que se pueda realizar una comparación entre las diferentes soluciones para cada enlace y para cada tipo de servicio que protegerán los datos en la red WideCOM.

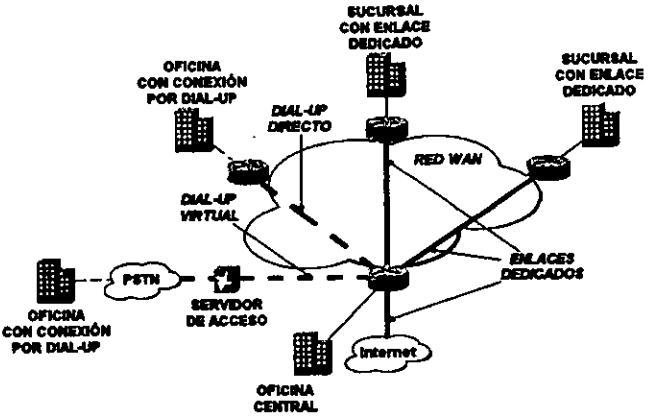


Figura 3.4. Esquema básico de conexiones para implementar seguridad en el tráfico de datos.

Seguridad corporativa

La seguridad del transporte de datos por las redes locales del corporativo WideCOM, y por la red WAN, estará soportada por una arquitectura que estará integrada en todos los dispositivos de comunicaciones (switches, routers, firewalls y servidores de acceso), y que estará compuesta por cinco elementos que hacen menos riesgosa la fuga de información, al mismo tiempo que restringe al acceso de forma interna.

Identidad: La técnica más común para cubrir este requisito es la configuración de usuarios y contraseñas, de ser posible estas últimas encriptadas o no visibles en pantalla. En este sentido, no existe una elección entre usuarios y contraseñas, ya que ambas están presentes como método de autenticación, usando alternativamente un servidor dedicado con una base de datos con todas las parejas usuario-contraseña. Existen varias alternativas para estos servidores, tales como Kerberos, RADIUS (*Remote Address Dial In User Service*, Servicio de Usuario de Dirección Remota por Marcación) y TACACS+ (*Terminal Access Controller Access Control System Plus*, Sistema de Control de Acceso por Controlador de Acceso Terminal Plus), de las cuales se implementará TACACS+ por sus características de mejoramiento en la gestión de Autenticación, Autorización y Manejo de Cuenta. Por otro lado, la administración de los equipos está empezando a ser manipulada por interfaces gráficas basadas en Web y, por lo mismo, es necesario implementar barreras de seguridad en el acceso por peticiones http.

Integridad: La integridad puede ser implementada mediante técnicas de suma de verificación y algoritmos de funciones Hash, los cuales garantizan que la información que viaja en la red llega a su destino sin haber sufrido ningún daño. La suma de verificación mencionada trabaja mediante la generación de un número, el cual se recalcula a su arribo en el destino para comparación y aprobación del mensaje o rechazo del mismo, según el resultado de esta comparación. Las funciones Hash son más

elaboradas y están provistas para el envío de datos críticos que requieren de mayor confianza en su transporte y constan de un algoritmo, que aplica ciertas funciones matemáticas al contenido de los mensajes, para encriptar la información tomando como referencia un valor en particular, lo que se conoce como llave de encripción.

Confidencialidad: La confidencialidad asegura que solo las partes a las que está destinada la información son capaces de interpretarla de forma correcta. A nivel de equipos de comunicaciones, es posible implementar la confidencialidad por medio de la configuración de mecanismos en los puertos de datos, que sólo transmiten información desde las direcciones que están previamente autorizadas; de esta forma, en un switch, los puertos pueden ser configurados para que sólo se abran para aquellas tramas que contengan ciertas direcciones MAC o bien, cuando se exceda cierta cantidad de direcciones aprendidas en el mismo puerto. También es adecuado implementar encripción en las sesiones que se establezcan con las terminales de configuración de los equipos de comunicaciones, por medio de servidores de autenticación como RADIUS y TACACS+., o por medio de IPsec y SSH.

Disponibilidad: La alta disponibilidad es una característica que aporta un elemento de las redes conocidas como "redes del 99%", porque indican que casi todo el tiempo, los enlaces y los servicios de red están disponibles. Esto también se conoce como redundancia, y existen varios aspectos para implementarla. Por un lado, el aspecto más urgente de redundancia reside en la alimentación eléctrica de los equipos y está solucionada mediante el uso de *UPS (Uniterrumplible Power Systems, Sistemas de Energía sin Interrupción)* y Plantas de energía emergentes. En el caso de los UPSs, por medio de un rectificador, un inversor y un sistema de baterías estos dispositivos permiten alimentar a los equipos como si estuvieran conectados a las acometidas de CFE (Comisión Federal de Electricidad), al momento de presentarse un corte de energía. Los UPSs proveen la corriente necesaria para mantener la operación de forma transparente hacia los equipos por un intervalo de tiempo (20 a 30 minutos), adecuado para preparar actividades de contingencia. Por otro lado las plantas de energía trabajan con Diesel por lo general y hacen la función de generadores que alimentan los circuitos de la misma fase a los que están conectados los equipos de comunicaciones.

La redundancia en estos equipos también está orientada a resolver problemas de conectividad o de falla de operación interna en los mismos. La práctica común es duplicar los equipos y configurar características de redundancia en ellos, con la intención de trabajar en dos planos: uno de operación y otro de respaldo. La configuración activa es actualizada al equipo en respaldo para que ésta pueda entrar en operación sin problemas. De nuevo, a nivel de switches la redundancia estará presente por medio *del STP (Spanning Tree Protocol, Protocolo de Expansión de Árbol)* que permitirá tener rutas alternas en redes locales por medio del bloque y habilitación de puertos que forman parte de la interconexión de switches y bridges, y que de manera natural proveen redundancia.

Auditoría: Los métodos para auditar la actividad de las redes en los aspectos de seguridad incluyen las herramientas para obtener: los diagramas de la topología actual y marcar los cambios que se gestionen de forma rápida, los servicios disponibles en cada host, las vulnerabilidades potenciales y existentes en los sistemas de defensa y la detección de intrusos e intentos de ataque. Para obtener estos resultados existen paquetes que, montados sobre plataformas de propósito general, revisan cada dirección

lógica y en cada una en la que se encontró actividad, hacen una nueva revisión montando peticiones para servicios específicos.

Seguridad en el acceso a la Internet

Cuando se ha tomado la decisión de habilitar los servicios de conexión hacia y desde la Internet, es muy importante contar con equipos que permitan controlar el tráfico de paquetes de una zona que consideramos segura (la Intranet) hacia otra que consideramos menos segura (la Internet) y viceversa. Además, la mayoría de las redes contemporáneas cuenta con algunas pocas direcciones homologadas para su acceso hacia la red de redes, de manera que se requiere de mecanismos que permitan dar acceso a muchos usuarios con pocas direcciones. Estas funciones tradicionalmente están resueltas con equipos de traducción conocidos como *proxies (promiscuos)* y reciben las peticiones de los equipos de la Intranet para traducir las direcciones originales por direcciones globales (homologadas) según estén disponibles en el proxy. Esta asignación puede tomar muchas formas, de las cuales destacan la toma por rango disponible en round robin o por traducción estática, en donde la asignación ya está predefinida y se hace uno a uno. En nuestro caso, la seguridad en el acceso a la Internet se basará en un Firewall que posee funciones de proxy pero que además permite hacer una asignación dinámica más eficiente, de forma que se puede, incluso, crear una asignación por puerto y no por direcciones para ocupar una sola dirección global, y se reparta a la misma por un puerto diferente para cada usuario de la red interna.

Esta función de implementar seguridad por medio de traducción de direcciones se conoce como *NAT (Network Address Translation, Traducción de Dirección de Red)* y se refiere a la función proxy antes mencionada, con la variante de traducir por puerto (ya mencionada también) que se conoce como *PAT (Port Address Translation,* Traducción de Dirección por Puerto*)*, con una capacidad de hasta poco más de 64000 traducciones por puerto utilizando una sola dirección IP homologada. La figura 3.5 muestra la conexión típica de una Firewall para proveer seguridad hacia y desde la Internet.

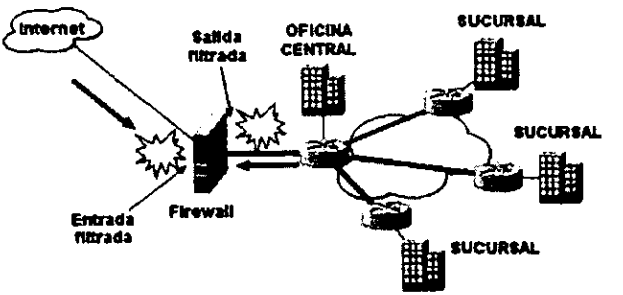


Figura 3.5. Aseguramiento de la conexión a Internet por medio de un equipo Firewall.

Además de la traducción de direcciones, el *Firewall* posee más recursos para aportar a la seguridad en el acceso a la Internet, por medio dos técnicas: filtrado de paquetes, que como se mencionó en el capítulo 2, examina los elementos de datos de las capas 3 y 4

con respecto al modelo OSI y determina la negación o aprobación de tráfico hacia la Intranet o hacia la Internet; y la otra, filtrado de aplicaciones, que determina las acciones a seguir en el cumplimiento de políticas más detalladas y que están basadas en elementos de aplicación de la capa 7 del modelo OSI. De estas dos técnicas se elige a la primera por ofrecer una velocidad de procesamiento de casi el triple con respecto a su competidor, por soportar un mayor número de conexiones simultáneas, por poseer un sistema operativo propietario que lo hace menos vulnerable a ataques en la plataforma, por contar con un soporte técnico especializado y disponible en línea en un esquema de 7x24, y por soportar la integración de soluciones de terceros para las herramientas complementarias en el filtrado de *URLs (Universal Resource Location,* Ubicación Universal de Recurso*)*, antivirus, detección de intrusos, etc.

Dentro de los mecanismos para implementar la seguridad en la conexión a la Internet, no es posible hacer una separación de funciones básicas, ya que la operación más importante reside en dejar pasar o no a los paquetes montados en IP; esto es, las direcciones de origen y destino se verifican junto con los servicios requeridos (montados en TCP o UDP) y se toma una decisión en uno de dos sentidos. Esto es todo lo que se debe hacer con la seguridad en Internet de forma básica; los complementos que ayudan a afinar la configuración de las políticas de seguridad están provistos por terceros y pueden estar o no implementados en hardware (como es el caso del detector de intrusos), aunque la mayoría está instalada como software.

Es importante señalar que algunas de las características básicas mencionadas anteriormente pueden implementarse con ciertas limitaciones en otros equipos de comunicaciones; sin embargo, como estas barreras están ligadas al nombre del producto y en particular al modelo usado, no es posible profundizar mucho en este capítulo.

Seguridad en el acceso a la Red por marcación

Por la naturaleza del proyecto que contempla conexiones hacia la oficina central, provenientes de sucursales que no cuentan con enlaces dedicados, es importante tener una sección en la implementación de seguridad que defina las opciones existentes para lo que se conoce como conexión por *Dial-In (marcación de entrada),* y que describa además las ventajas de cada una de ellas y la adecuación para los casos que requerirán de aseguramiento en el transporte de datos.

Antes de hablar de las opciones para el Dial-In, es bueno mencionar las actividades que se desea realicen las sucursales remotas sin enlace dedicado, y algunos ejecutivos de cuenta de la empresa. Se debe tener presente que todas las sucursales proveerán la información necesaria para realizar la facturación mensual, correspondiente a todas las operaciones de venta realizadas, y que esta información deberá protegerse contra la observación de terceros en las redes públicas (PSTN e Internet). También, algunos ejecutivos de cuenta de la empresa deben tener acceso a los inventarios de equipos y estatus de ordenes de servicio que se encuentren en la base de datos de las oficinas centrales, para poder dar información sobre productos y servicios en línea y dentro de las instalaciones de los clientes que tengan asignados en su cuenta.

Con esto en cuenta, existen dos opciones para implementar la conexión de las sucursales remotas a la oficina central: Dial-In directo y Dial-In virtual. En la primera modalidad, la marcación se realiza empleando líneas dedicadas que forman parte de una

red semi-privada, esto es, los enlaces son propiedad del carrier pero éste debe garantizar que la ruta de conmutación esté siempre disponible y, lo más importante, no hay una garantía implícita sobre la inexistencia de algún visor a lo largo de dicha ruta. La figura 3.6 muestra las opciones para lo que es el Dial-In directo.

En esta figura se observan algunos elementos nuevos como son: *NAS (Network Access Server, Servidor de Acceso de Red)*, el cual se refiere al equipo que recibe las llamadas por conexión analógica, *ISDN (Integrated Services Digital Network, Red Digital de Servicios Integrados)*, un término para definir toda la gama de servicios en una red pública completamente digitalizada, *POTS (Plain Old Telephone Network, Red Telefónica de Marcación Antigua)*, un concepto antiguo que describía el plan de marcación hasta antes de la norma E.164, *ADSL (Asynchronous Digital Suscriber Line, Línea de Abonado Digital en modo Asíncrono)*, una técnica para incrementar la velocidad de descarga desde la Internet para proveer servicios digitales, *Wireless (inalámbrico)*, otra técnica de solución para la última milla basada en la emisión de microondas para la conexión a la Internet.
La otra opción de conexión por marcación se realiza por líneas conmutadas y viaja completamente a través de las redes públicas, tal y como se mencionó anteriormente, lo que le da el nombre de virtual, porque establece una ruta lógica dentro de los canales conmutados de la PSTN y de su conexión al ISP. La ventaja de esta conexión radica en su independencia de ubicación, puesto que puede realizarse prácticamente desde cualquier lugar, con la sola condición de contar con una línea telefónica y un número para acceder ya sea a los modems de la Intranet o al proveedor de Internet. La figura 3.7 bosqueja de forma simple la forma en que un usuario móvil puede conectarse a la red corporativa mediante este mecanismo conocido como Dial-In virtual.

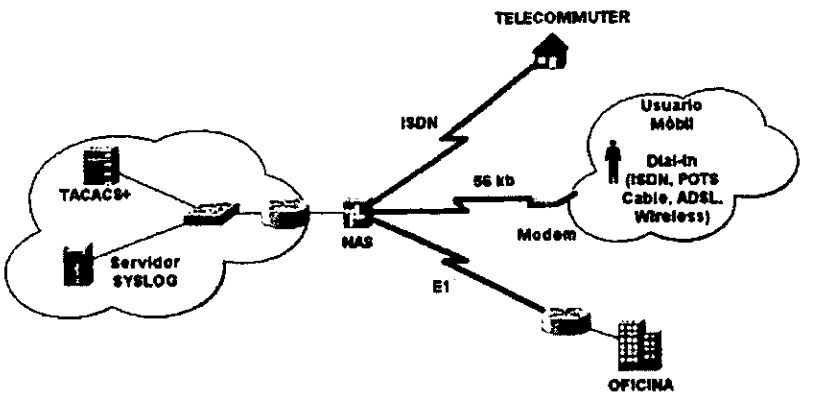


Figura 3.6. Configuraciones de conexión por Dial-In directo.

Los aspectos a cubrir en la seguridad, al momento de habilitar las conexiones remotas por marcación, son muy similares a los empleados para asegurar el acceso de la Internet; por lo que es buena idea la implementación de un Firewall que defina los flujos, además de equipos de autenticación como servidores TACACS+ y Radius.

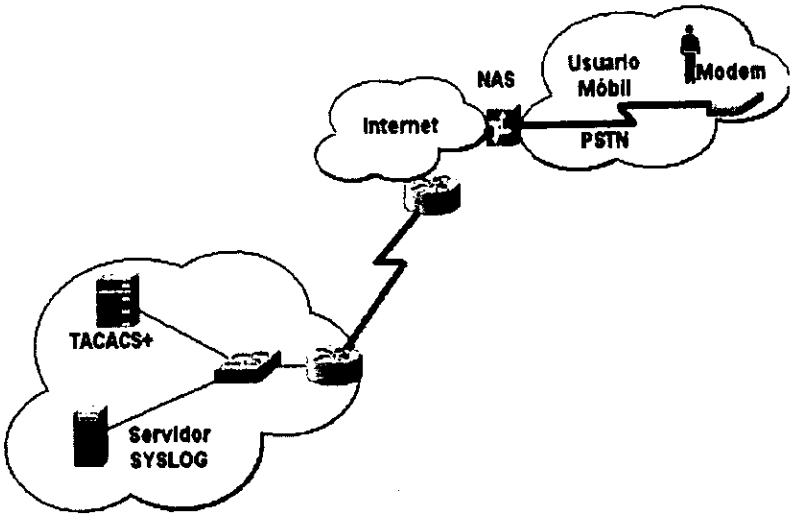


Figura 3.7. Esquema básico de conexión a la red corporativa usando una conexión virtual.

Independientemente de la opción a elegir cuando se defina el tipo de medio en la marcación, existen ciertos aspectos a cubrir en su implementación que conciernen a la seguridad, los cuales son:

- Identificación del origen de la llamada.
- Identificación de la persona que hace la llamada.
- Identificación del destino de la llamada.
- Supervisión del rastreo de los datos y aplicaciones accedidas.
- Supervisión del rastreo de la duración de la conexión.
- Aseguramiento de la comunicación autenticada.
- Aseguramiento de la privacidad de la comunicación.

La elección de la conexión remota por línea conmutada estará inclinada hacia la modalidad virtual, que comercialmente se conoce como VPDN (Virtual Private Dial-Up Network) y que está estrechamente relacionado con las VPNs estudiadas en el capítulo 2. Se piensa que la conexión en las puntas remotas se realizará por modem y marcarán un número local para ingresar a la Internet de donde brincarán a la red corporativa. Dentro del equipo que se conectará a la Internet existen dos variedades de protocolos para la comunicación asíncrona: SLIP (Serial Line Internet Protocolo, Protocolo de Internet por Línea Serial) y PPP, este último ya discutido con anterioridad. La elección de PPP en los enlaces dedicados de las sucursales remotas se planteó como una solución

eficiente por las características de control de calidad y seguridad implícitas y configurables en dicho protocolo. Por la misma razón se elige al PPP sobre SLIP para la conexión asíncrona.

Cuando se usa una VPDN, en la cual la Internet se usa como transporte, existen algunas consideraciones extra que deben contemplarse en lo concerniente a seguridad. Estos aspectos adicionales de seguridad se implementan combinando algunas técnicas de tuneleo como GRE *(Generic Routing Encapsulation,* Encapsulamiento de Ruteo Genérico*)*, L2F, L2TP, IPsec y CET. Las combinaciones mencionadas pueden ser: *GRE con CET (Cisco Encryption Technology,* Tecnología de Encripción de Cisco*)*, L2TP con IPsec. De estas dos, la elección de L2TP con IPsec resulta ser la más conveniente por la naturaleza de estándar abierto que implica IPsec.

3.3. Definición de la Propuesta Final

Después de listar las características más sobresalientes para el desarrollo del proyecto de la red de datos y voz para WideCom, se tomó la decisión de usar el estándar IEEE 802.3 para las redes locales. A nivel WAN implementaremos enlaces dedicados con el protocolo PPP en modo multipunto. El protocolo dominante para el transporte de datos será el conjunto de protocolos TCP/IP y el protocolo de ruteo EIGRP.

La etapa de voz será compuesta por conexiones FXS-FXO en las sucursales remotas (en formato analógico y arranque por tierra.) La parte correspondiente a la oficina central descanalizará los enlaces de voz como parte del enlace multipunto y los enlazará al PBX central para su enrutamiento final (esto último se realiza empleando la señalización MR2 en su modalidad CAS.)

El aspecto de seguridad se basará en el desarrollo de tres etapas. La primera implantará las políticas de seguridad para la comunicación interna del corporativo (Intranet), la segunda etapa propone la instalación de barreras de seguridad para la conexión a la Internet por medio de un Firewall. Por último, la tercera etapa establecerá que las conexiones por marcación remota (Dial-In) serán en la modalidad de virtuales, ya que emplearán como transporte a las redes públicas (Internet ó PSTN.)

CAPÍTULO 4

Definición y segmentación de la red

El diseño es el primer paso de la fase de desarrollo de cualquier sistema de ingeniería. Su objetivo principal es producir el modelo de una entidad que se construirá más adelante. El diseño normalmente es creado en base a la experiencia de construir entidades similares, un conjunto de principios que guían la forma de desarrollo que conduce finalmente a una representación del diseño final.

El diseño de la Red de WideCOM se integra por cuatro partes: iniciamos con la definición y segmentación de la Red, donde hablamos de las redes locales, enlaces, la segmentación de la red y del protocolo de ruteo a usar. Posteriormente describiremos el plan de marcación y la compresión de datos. En la tercera parte abordaremos uno de los punto medulares del diseño de la red, la Estrategia de Seguridad, haciendo énfasis en los firewalls, políticas de seguridad y la definición llaves de acceso. Por último en la sección de Selección del Hardware se hará un comparativo, donde se toman en cuenta diferentes marcas de equipo necesario para la implementación de nuestro proyecto.

4.1. Definición y Segmentación de la Red

El proceso de definición de nuestro proyecto, es parte fundamental del presente trabajo, dado que será el medio por donde se llevará a cabo la comunicación de la Central de WideCOM con todas y cada una de sus sucursales, y por donde también se hará la transferencia de datos. Por ello dedicamos esta parte a los cálculos y consideraciones necesarias para cubrir las necesidades de comunicación y transporte de datos del corporativo.

4.1.1. Redes Locales

La red que se diseñará es una WAN, con subredes LAN en la central y las sucursales. El direccionamiento se realizara utilizando el protocolo IP. Trabajaremos con una red clase B, dado el número de subredes necesario y considerando el número de términales de la central en el Distrito Federal (que suman más de 300 equipos) Por lo anterior no se pensó en trabajar con una red clase C, ya que en esta clase, el número máximo de hosts es de 255.

Para el desarrollo del esquema de direcciones IP debemos cumplir los siguientes pasos:

1. Determinar el número de subredes que necesitamos.
2. Determinar la máscara de subred y las submáscaras.
3. Asignar las direcciones IP a cada host en la subred.

Número de Subredes

Para determinar las subredes consideraremos los datos que se presentan en la tabla 4.1, la cual nos muestra el número de segmentos de red necesarios para las LAN que se ubicarán en las diferentes plazas del corporativo WideCOM.

	No. De Segmentos
México	4
Guadalajara	1
Monterrey	1
Queretaro	1
León	1
San Juan del Río	1
Toluca	1
Gómez Palacio	1

Tabla 4.1. LANs necesarias en las plazas del corporativo WideCOM.

Además existirán siete enlaces dedicados y serán necesarias cincuenta VPDNs para usuarios móviles.

Cada una de las LAN deberá tener un estimado de treinta nodos para los usuarios.
Si tomamos en cuenta que las 50 VPDNs conforman una red y contamos cada uno de los enlaces con una red, tenemos un total de 19 subredes.

Para calcular el número total de subredes debemos tomar en cuenta también el crecimiento estimado a futuro.

En este proyecto se planea integrar a tres o cuatro plazas más, en un lapso no mayor de dos años, por lo que el número de subredes será de 23.

Usando la formula de (2^n-2), el total de redes disponibles es (2^8-2) o 254. Por lo que el crecimiento potencial es de 19 hasta 254 subredes.

Máscara y Direcciones de Subred

Para asignar la máscara y las direcciones debemos considerar lo siguiente:

Determinar el número de direcciones de subred disponibles y los números de las direcciones de los hosts disponibles para la subred.

$$\text{Subredes Disponibles} = 2^n-2$$
$$\text{Hosts Disponibles} = 2^m-2$$

En las formulas anteriores, la "n" es el número de bits de la dirección de la máscara y "m" es igual al numero bits de direcciones sin máscara.

Para WideCOM hemos decidido usar los primeros siete bits del tercer byte para definir la subred. La subred es:

255.255.254.0

$$\text{Subredes Disponibles} = 2^7 - 2 = 126$$
$$\text{Hosts Disponibles} = 2^9 - 2 = 510$$

Dirección para la Máscara de Subred Tipo B

255.255.254.0

254.0 = 1111111 0.00000000

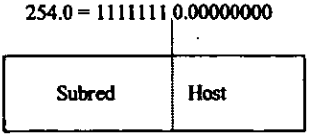


Figura 4.1. Calculando Subredes Hosts para una red claseB.

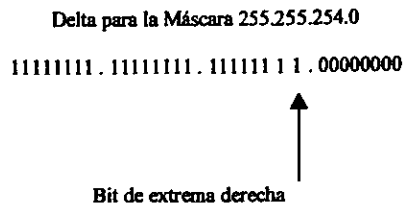
Para calcular el valor de la dirección de sub red tenemos lo siguiente:

Primero identificamos el bit de extrema derecha en la máscara de subred y convertimos el valor binario en decimal. El número obtenido se denomina Delta.

Sumamos Delta al número original de la dirección de red para obtener el primer valor de dirección de red.

Sumamos delta a la última dirección para determinar el siguiente valor de dirección de red y así sucesivamente.

La dirección de red que usaremos es la 172.16.0.0 de la clase B.



En la tabla 4.2 se muestran los valores de direcciones de subred calculados.

Número de Subred	Subredes Adicionales (suma de delta)
2	172.16.(2+2).0 = 172.16.4.0
3	172.16.(4+2).0 = 172.16.6.0
4	172.16.(6+2).0 = 172.16.8.0
5	172.16.(8+2).0 = 172.16.10.0
6	172.16.(10+2).0 = 172.16.12.0
7	172.16.(12+2).0 = 172.16.14.0
8	172.16.(14+2).0 = 172.16.16.0
9	172.16.(16+2).0 = 172.16.18.0
10	172.16.(18+2).0 = 172.16.20.0
11	172.16.(20+2).0 = 172.16.22.0
12	172.16.(22+2).0 = 172.16.24.0
13	172.16.(24+2).0 = 172.16.26.0
14	172.16.(26+2).0 = 172.16.28.0
15	172.16.(28+2).0 = 172.16.30.0
20	172.16.(38+2).0 = 172.16.40.0
25	172.16.(48+2).0 = 172.16.50.0
30	172.16.(58+2).0 = 172.16.60.0
35	172.16.(68+2).0 = 172.16.70.0
40	172.16.(78+2).0 = 172.16.80.0
45	172.16.(88+2).0 = 172.16.90.0
50	172.16.(98+2).0 = 172.16.100.0

Tabla 4.2. Direcciones de Subred para WideCOM.

Direcciones IP a cada Host en la Subred

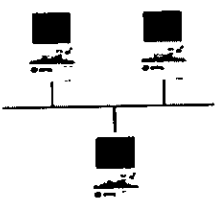
Después de tener los valores para las subredes de la red global, debemos asignar las direcciones IP a cada host tomando en cuenta las siguientes reglas.

1. Tomaremos en la red número dos (172.16.4.0) de la tabla 4.2, para el calculo de las direcciones IP de los host.

2. Los primeros dos bytes de la dirección deben ser 172.16.(Cabe señalar que estos datos se representan en notación decimal, lo cual es común en el ambiente de redes cuando se realiza el mapping)

3. Los primeros siete bits del tercer byte deben ser (0000010) en binario y su equivalente en decimal (4). Por lo que el número que asignemos al tercer byte debe caer dentro del rango de 2 (**00000100**) a 5 (**00000101**).

4. Las dos direcciones 172.16.4.0 y 172.16.5.255 no pueden usarse (todos los nodos de bit dentro de 172.16.4.0 son ceros y todos los bits de nodo dentro de 172.16.5.255 son unos).



Dirección IP = 172.16.X.Y
X = 4 - 5
Y = 0 - 255

Ejemplos de Direcciones
172.16.4.1
172.16.4.10
172.16.5.100
172.16.5.200

Figura 4.2. Asignaciones de IP para la subred 2.

De igual manera, para calcular las demás direcciones hacemos uso de las reglas anteriores. En la tabla 4.3 se muestra algunos de los rangos de direcciones IP que podemos asignar a cada uno de los hosts de la red de WideCOM, de acuerdo a la red a la que pertenezcan.

Tomando en cuenta la tabla 4.3, se hace la siguiente asignación para las LAN de México, y cada una de las sucursales. En la Tabla 4.4 se listan las direcciones IP para las subredes para el control y administración de las mismas

Subred	Dirección Inicial	Dirección Final
1	172.16.2.0	172.16.3.255
2	172.16.4.0	172.16.5.255
3	172.16.6.0	172.16.7.255
4	172.16.8.0	172.16.9.255
5	172.16.10.0	172.16.11.255
6	172.16.12.0	172.16.13.255
7	172.16.14.0	172.16.15.255
8	172.16.16.0	172.16.17.255
9	172.16.18.0	172.16.19.255
10	172.16.20.0	172.16.21.255
11	172.16.22.0	172.16.23.255
12	172.16.24.0	172.16.25.255
13	172.16.26.0	172.16.27.255
14	172.16.28.0	172.16.29.255
15	172.16.30.0	172.16.31.255
20	172.16.40.0	172.16.41.255
25	172.16.50.0	172.16.51.255
30	172.16.60.0	172.16.61.255
35	172.16.70.0	172.16.71.255
40	172.16.80.0	172.16.81.255
45	172.16.90.0	172.16.91.255
50	172.16.100.0	172.16.101.255
100	172.16.200.0	172.16.201.255
126	172.16.252.0	172.16.253.255

Tabla 4.3. Rango de Direcciones IP para los hosts de la WAN de WideCOM.

Subred	Ciudad	Dirección Inicial	Dirección Final
1	Enlace1	172.16.2.0	172.16.3.255
	Enlace2	172.16.3..0	
2	Enlace3	172.16.4.0	172.16.5.255
	Enlace4	172.16.5.0	
3	Enlace5	172.16.6.0	172.16.7.255
	Enlace6	172.16.7.0	
4	Enlace7	172.16.8.0	172.16.9.255
	Asignación Futura	172.16.9.0	
5	México1	172.16.10.0	172.16.11.255
6	México2	172.16.12.0	172.16.13.255
7	México3	172.16.14.0	172.16.15.255
8	México4	172.16.16.0	172.16.17.255
9	Asignación Futura	172.16.18.0	172.16.19.255
10	Guadalajara	172.16.20.0	172.16.21.255
11	Asignación Futura	172.16.22.0	172.16.23.255
12	Asignación Futura	172.16.24.0	172.16.25.255
13	Asignación Futura	172.16.26.0	172.16.27.255
14	Asignación Futura	172.16.28.0	172.16.29.255
15	Monterrey	172.16.30.0	172.16.31.255
20	Querétaro	172.16.40.0	172.16.41.255
25	Leon	172.16.50.0	172.16.51.255

Continua.

30	San Juan del Río	172.16.60.0	172.16.61.255
35	Toluca	172.16.70.0	172.16.71.255
40	Gómez Palacio	172.16.80.0	172.16.81.255
45	Asignación Futura	172.16.90.0	172.16.91.255
50	VPDNs	172.16.100.0	172.16.101.255
100	Asignación Futura	172.16.200.0	172.16.201.255
126	Sin Asignación	172.16.252.0	172.16.253.255

Tabla 4.4. Asignación de direcciones IP para las subredes del las WAN de WideCOM.

Las direcciones que se asignen a cada uno de los hosts deberán estar comprendidas dentro de las listadas en la tabla 4.4, dentro de la subred que se le asigne de acuerdo a la plaza donde esté ubicado.

4.2. Plan de marcación

En el sector de las telecomunicaciones existen ciertos recursos, esto es, medios cuyo empleo es indispensable para la explotación de actividades de telecomunicación, y que, sin embargo, por su propia naturaleza, no pueden ser utilizados indiscriminadamente por los operadores.

Nos referimos a los recursos limitados, los cuales, al restringir la concurrencia de operadores, constituyen un impedimento para la introducción de la libre competencia formal en el sector. Los dos principales de esos recursos limitados en materia de telecomunicaciones son: el espacio radioeléctrico y la numeración.

La numeración es, al igual que el espectro radioeléctrico, un recurso limitado, no–obviamente- por la naturaleza de los números, sino por el uso práctico que de éstos pueda hacerse. Sin embargo, más que un bien, la numeración es un instrumento, que permite identificar los distintos terminales de telecomunicaciones.

En efecto, la numeración es el elemento fundamental que permite el establecimiento de las comunicaciones entre los usuarios de los servicios de telefonía, pues es a través de la numeración que se identifica de manera suficiente cada terminal de telefonía, permitiendo a los usuarios dirigir sus comunicaciones a los destinatarios deseados.

Podemos definir la numeración como "la representación unívoca, a través de identificadores, de los equipos terminales de redes de telecomunicaciones, elementos de redes de telecomunicaciones o a redes de telecomunicaciones en sí mismas".

Es de hacer notar que los planes de marcación están orientados a la adecuada distribución de los recursos numéricos entre los abonados al servicio, de manera que además de cubrir las necesidades presentes y futuras de recursos numéricos, permita a aquellos una utilización lo más sencilla posible. En efecto, dado que la numeración es un recurso limitado, se debe hacer una distribución y uso eficiente de la misma, a los fines de garantizar proveer a los usuarios existentes, a los potenciales usuario y a los futuros usuarios, números suficientes para la satisfacción de sus necesidades de comunicación por el período de tiempo más largo posible.

4.2.1 Definición de cadenas y flujo de llamadas

En el proyecto que nos ocupa para realizar el plan de marcación la definición de cadenas corresponde a la asignación de los dígitos a ocupar para lograr que las comunicaciones sean establecidas correctamente. Existirán en este plan dos tipos de métodos de marcaje y numeración:

- Red telefónica conmutada
- Red Interna WideComm

Para el primer punto se realizará una solicitud ante la compañía de teléfonos local, en nuestro caso TELMEX (Teléfonos de México), para que se asigne a nuestro proyecto una cantidad de 500 DID (Direct Inward Dial, números directos) bidireccionales , en este caso los usaremos para proporcionar extensiones tanto analógicas (para los enlaces de modem, fax, líneas privadas) como digitales (que serán usadas para las extensiones del conmutador). Se realiza la petición para que el rango vaya desde el 4247000 hasta el 4247499, de esta manera ubicaremos los servicios de la siguiente manera:

Rango	Tipo de Servicio
4247000	Consola del conmutador (operadora)
4247001-4247100	Extensiones
4247101-4247500	Servicios generales

Tabla 4.5. Asignación de DIDs.

Ahora bien, en el caso de las llamadas que se realizarán por la red interna, para evitar los altos costos por larga distancia, debemos desarrollar una tabla de ruteo que en un principio se limitará a mostrar los dígitos, en este caso se colectarán 4, a marcar para alcanzar los diferentes destinos en las plazas.

Tomando en cuenta que las ciudades donde tendremos red interna serán las siguientes:

- Monterrey
- Guadalajara
- Gómez Palacio
- Querétaro
- León
- Toluca

Por lo tanto realizaremos nuestra marcación de la siguiente manera:

Dígitos para tomar línea	Dígitos para conectar	Ciudad
77	7880	Gómez Palacio, Durango
77	7881	Toluca
77	7882	Guadalajara
77	7883	León
77	7884	Monterrey
77	7885	Querétaro

Tabla 4.6. Marcación en red.

De esta manera se contactarán las diferentes llamadas, para hacer más comprensible este flujo de llamadas realizamos los siguientes ejemplos, donde observaremos a grandes rasgos los equipos utilizados.

En la gráfica 4.3 observamos como se realizaría una llamada desde un usuario externo utilizando la PSTN y haciendo contacto con el PBX para , ya sea hablar con la operadora de la consola del conmutador o buscar algún contacto en la lista de extensiones.

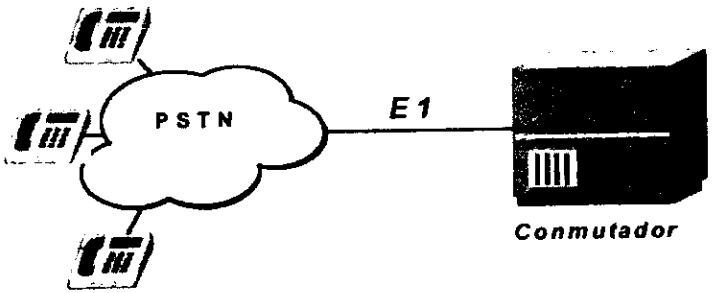


Figura 4.3. Marcado externo.

En la figura 4.4. observamos la forma en la que se realizara el marcado por red interna. Donde observamos al usuario conectado al PBX, iniciando la llamada y viajando por la WAN hasta su destino final.

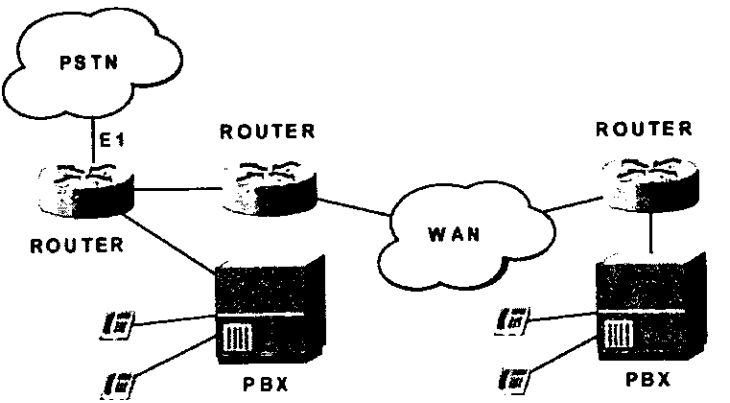


Figura 4.4. Marcación por red interna.

A continuación se describirá la forma de compresión a ser utilizada en el proyecto de implementación de la red WideComm

4.2.2. Compresión

La calidad de la voz sobre Internet ha sido muy criticada en los últimos años, pero sí podemos afirmar que ha ido mejorando constantemente. En estos momentos se considera que es un tema de éxito la calidad de voz sobre Internet, y esto gracias a la compresión de datos. El término compresión de datos se refiere al proceso de reducir la cantidad de datos requeridos para representar una cantidad dada de información. Ya que distintas cantidades de datos pueden ser usadas para representar la misma información, consideramos con ello a la redundancia de datos como elemento central en la compresión de datos. De las diferentes alternativas y gracias a sus características seguiremos utilizando un sistema de compresión G729 con el cual el nivel de aceptación de voz sobre Internet tendrá nivel de 4.2, mientras que en el estándar normal que se ha usado el G711 en el sistema PCM, es de 4.4, así la calidad de voz sobre Internet será mejorada día a día. Dentro del este proceso de compresión en el proyecto WideComm utilizaremos compresión 4 a 1 utilizando el protocolo G729.

4.3. Estrategias de seguridad

El diseño de la seguridad para el corporativo WideCom, se puede resumir en tres aspectos: la autenticidad, la integridad y la confidencialidad de los datos en tránsito. La estrategia se complementará con cada una de las etapas que se configurarán en los equipos y en los cuales el software de programación permitirá la conexión autorizada de cada sucursal al sitio central en las oficinas de la ciudad de México. Los aspectos a cubrir en el diseño son los siguientes:

- Redundancia de energía y autenticidad por servidor.
- Diseño de políticas de seguridad en el FireWall.
- Diseño de túneles virtuales para acceso por la Internet.

A continuación se detallarán cada una de estas configuraciones, y se integrará su diseño a la red de datos por estar vinculada con los enlaces entre sucursales.

4.3.1. Redundancia de energía y autenticidad por servidor

La redundancia se considera pocas veces como parte de la seguridad de una empresa; sin embargo, para WideCom, el hecho de contar con sistemas redundantes a nivel lógico y físico es muy importante, puesto que las operaciones contables e inventarios manejados a nivel nacional se consideran de misión crítica y los equipos deben ser capaces de soportarla. El diseño de la redundancia abarca el reemplazo en caliente de equipos dañados, lo que permite la operación continua sin que las interrupciones se hagan aparentes para los usuarios. Dentro del esquema de redundancia y alta disponibilidad, se abren dos aspectos que aportarán estas características: la redundancia física, en la cual, los servidores centrales deben estar soportados por equipos de energía ininterrumpible, que permiten mantener la operación cuando existe una falla de energía

por parte del proveedor eléctrico y siguen funcionando por medio de un mecanismo de baterías y cuya duración está en dependencia directa con la cantidad de carga que suministra. Por otro lado, la redundancia lógica se refiere a la implementación de enlaces conmutados redundantes para la operación mínima requerida entre las sucursales cuando los enlaces principales están caídos. Este mecanismo se conoce como Dial-Backup y consiste en la marcación automática de números conmutados desde la oficina central o desde las sucursales para mantener la operación. En estos estados de emergencia, los enlaces de voz por red interna son dados de baja de forma automática para dedicar el ancho de banda por completo al envío de datos. Esta idea se expresa en la figura 4.5 donde se puede observar claramente que los modems entrarán en funcionamiento en caso de que el router, que maneja el enlace de la sucursal o de la oficina central, sufra algún desperfecto, en ese momento el enlace se restablece automáticamente utilizando la línea conmutada.

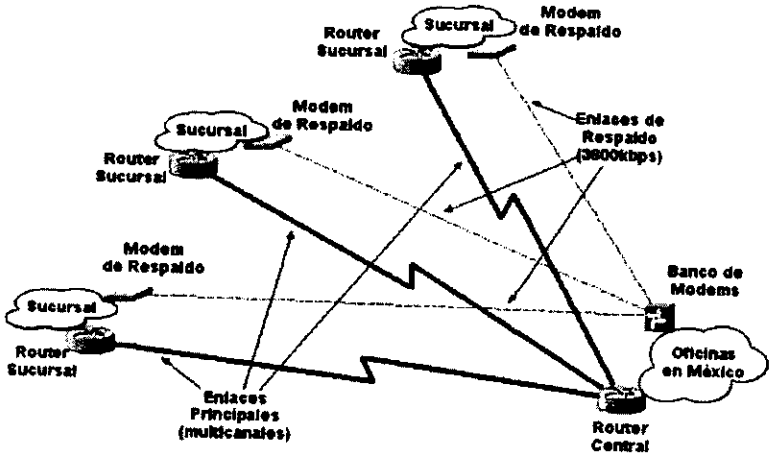


Figura 4.5. Esquema básico de redundancia de enlaces dedicados.

La diferencia entre un enlace y otro es muy notoria; no obstante no hay que dejar de tomar en cuenta la alta disponibilidad en enlaces que esto representa, ya que las caídas de enlaces por el proveedor aunque no son muy frecuentes, cuando suceden, pueden representar pérdidas considerables por la falta de información.

El esquema de redundancia implica la contratación de líneas comerciales adicionales a las empleadas por la sucursal misma o por las oficinas centrales (éstas pueden implementarse mediante extensiones analógicas dentro del conmutador central.)

Una vez concluida la etapa de redundancia de enlaces, el siguiente punto a tratar dentro del primer aspecto de seguridad corporativa es la implantación de un servidor de logeo, que en nuestro caso será mediante el estándar conocido como TACACS+ , que mantiene una base de datos actualizada de todos los usuarios autorizados con una tabla relacionada de nombre_usuario – contraseña, que debe verificarse para cualquier tipo de

acceso, ya sea de uso de recursos o de administración de equipos. La figura 4.6. muestra la operación típica de este servidor único en las oficinas centrales (no se espera que en las sucursales existan conexiones desde fuera de la red; sin embargo la administración remota está protegida con niveles de usuarios y contraseñas locales en los equipos.)

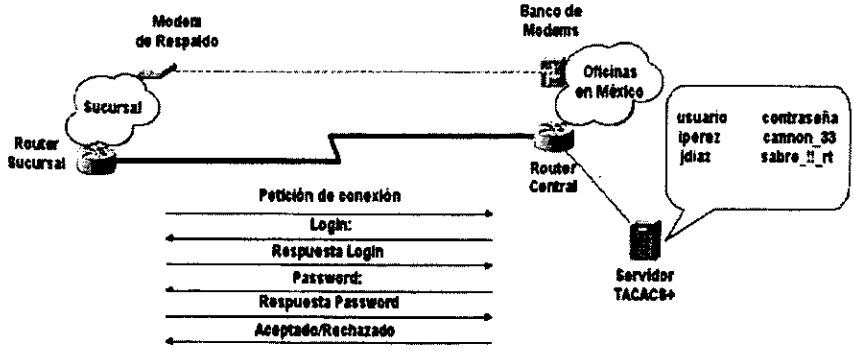


Figura 4.6. Método de autenticación por servidor TACACS+.

Como una característica de seguridad más, dentro de los enlaces se configurará la opción de protocolo CHAP, el cual toma a otros usuarios a autenticar de una pequeña base de datos que se aloja en los routers y que es verificada cuando se intenta hacer una conexión de administración. Este elemento aporta un punto más seguridad dentro de la administración de los equipos de comunicaciones, puesto que sólo los usuarios autorizados pueden ingresar a cualquiera de las consolas de gestión de los dispositivos y cualquier operación dentro de ellos está altamente restringida.

4.3.2. Diseño de Políticas de seguridad en el Firewall

Las políticas de seguridad en el Firewall son quizás el punto más importante en la implementación de seguridad en lo que concierne al acceso a la Internet, porque son las que determinan los flujos de información que están autorizado. Para el diseño de seguridad, las políticas de seguridad pueden ser expresadas de forma abstracta por condiciones y acciones a tomar y así, crear un esquema completo de flujos. En la mayoría de los Firewalls, los equipos constan por lo menos de dos interfaces de red locales que les permiten crear igual número de zonas de seguridad. Es común también, que a estas zonas se les asigne un valor de seguridad conocido como "peso" y conforme la interfaz posea el mayor peso, mayor será la seguridad que aporte a todos los equipo que estén conectados a su interfaz (la cual es extendida por la conexión de un switch de capa 2.)

Como se mencionó en el capítulo anterior, el mecanismo que habrá de implementar el Firewall de WideCom trabaja con la filosofía de filtrado de paquetes, lo que significa que para cada inicio de conexión (en el contexto de IP) el equipo hará una revisión de

los paquetes, haciendo uso de las características que estos poseen en capa 3 y opcionalmente en capa 4 (relacionados al modelo OSI). Ahora bien, como ya se mencionó la existencia de un grupo de servidores que publicarán información comercial sobre WideCom, esto supone la existencia de tres perímetros de seguridad, cuyas características se detallan en la tabla 4.7.

Nombre Interfaz	*Peso de seguridad*	*Tipo de Interfaz*	*Comentario*
Outside	0	10BaseT	Conexión a la Internet por medio del router de Internet.
Inside	100	10BaseT	Conexión a la red interna de WideCom, lo cual incluye la conexión al router de Red WAN.
Public	80	10/100BaseT	Conexión a la zona pública donde se hospedarán las páginas web comerciales.

Tabla 4.7. Características generales de las interfaces del Firewall.

Como política implícta, el firewall tiene predeterminadas dos tipos de reglas que no pueden alterarse y que sirven de base para la configuración de los flujos de datos mencionados. Partiendo del hecho de que no puede haber dos perímetros que posean el mismo peso de seguridad, los flujos sólo pueden ser en dos sentidos: de una zona de mayor peso a una zona de menor peso y viceversa. Para el primer caso, la regla predeterminada indica que todo el flujo está permitido excepto lo explícitamente negado; para el segundo caso, la regla es contraria, esto es, todo el flujo de información está prohibido excepto lo explícitamente permitido, lo cual es congruente con el concepto de zonas y lo que entendemos por seguridad o confianza. La figura 4.7. nos muestra las conexiones del Firewall para cumplir con los requerimientos expresados anteriormente. Para la conexión a los servidores Web, lo que se habilitará en el Firewall son todos los puertos para los servicios de web, ftp, dns y pop3, los cuales entran en el rango de puertos "bien conocidos" y deben ser configurados así en las listas (políticas) del flujo que va desde la Internet hasta la zona pública. Los detalles de estas políticas, junto con aquellas que habilitan la conexión hacia la Internet, se especifican en el capítulo siguiente que trata de la implementación de los equipos y su configuración final.

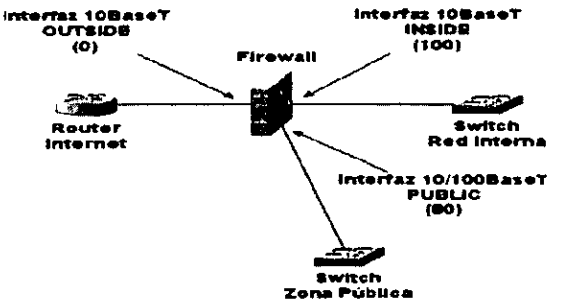


Figura 4.7. Definición de zonas de seguridad.

4.3.3. Diseño Túneles virtuales para acceso por Internet

Los túneles virtuales serán empleados básicamente para las conexiones remotas que demandan recursos de la red central y a la cual se enviarán los datos de la facturación. Estos túneles, tal y como se advirtió en el capítulo 3, serán del tipo Dial-In y constarán de una conexión, desde las sucursales que carecen de enlace dedicado hacia la Internet mediante un modem analógico, con una velocidad máxima de 33,600 kbps, apoyado de un software residente en disco duro del equipo remoto y el cual habilita al cliente del túnel, y en donde además se configurarán las llaves de encripción para la autenticación de la conexión. Este software se conoce como *VPN client* y la terminación del túnel puede ser implantada en router o en Firewall. Para nuestro esquema de WideCom, lo más apropiado será emplear la terminación del canal en el Firewall para que las políticas se apliquen en un solo equipo (el Firewall), y así mismo se asignen los permisos pertinentes para cada usuario.

Puesto que emplearemos a la Internet como el transporte de las conexiones virtuales, no hay necesidad de instalar un servidor de acceso, ya que quien recibirá las llamadas locales será el proveedor local de la Internet, en donde, por acuerdo, existirá un servidor de acceso que validará las conexiones, y la conexión del mismo al site central de WideCom se realizará mediante un enlace dedicado, con un ancho de banda de 256 kbps y con la información encripatada usando L2TP e IPsec. Esto se observa en la figura 4.8.

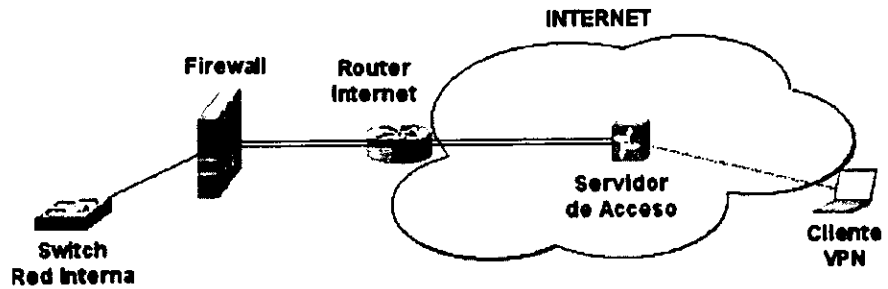


Figura 4.8. Creación de túnel virtual por servidor de acceso dentro del ISP.

Ya que se decidió emplear al Firewall como terminador del túnel, es importante señalar algunos aspectos de encripción que serán empleados por el diseño de la seguridad. La técnica de encripción que se utilizará cae dentro del estándar DES y es un mecanismo que no requiere de permisos especiales de exportación, en el sentido que los Estados Unidos no puede prohibir su venta a asociaciones fuera de sus fronteras; sin embargo, si se quisiera implantar un mecanismo más fuerte de encripción, tal y como lo es 3DES, los permisos se hacen presentes y los trámites serían muy susceptibles de retrasos por tratarse de un mecanismo inventado en los Estados Unidos, y la posibilidad de corromper su algoritmo por países competidores o rivales, pone en duda su venta a asociaciones fuera del país.
El intercambio de llaves que se efectuará entre las partes a comunicar será de la modalidad asimétrica; en la cual, como se mencionó en el capítulo 2, existen dos tipo de llaves, la pública y la privada.

4.4. Selección de hardware

Tomando en cuenta la solución a implementar y brindar con ello la satisfacción del cliente se realizará una selección de equipo , logrando con ello obtener un equilibrio entre los costos y las características técnicas del mejor equipo. A continuación se presentan las tablas comparativas de los diferentes quipos y los resultados de este comparativo, comenzamos con los comparativos de equipo de computo en la tabla 4.8:

(PRECIOS EN USD)	**Dell Latitude LSH 500**	**IBM ThinkPad X20 34U**	**Sony VAIO PCG-SR17K**	**Toshiba Portégé 3480CT**
Precio de la conf. probada (en USD)	$2,448, precio directo	$2,500, precio directo	$2,399, precio directo	$2,300, precio al público
Procesador	Mobile Pentium III/500	Mobile Pentium III/600	Mobile Pentium III/700	Mobile Pentium III/600
Vel. el ahorro de energía (Mhtz)	N/A	500	550	500
Peso del sistema/con adaptador de AC	3.7/4.5 libras	3.5/4.2 libras	2.9/3.6 libras	3.22/3.9 libras
Dimensiones (AAP, en pulgadas)	1x10.7x8.6	1x11x8.9	1x10.5x8.5	0.8x10.3x9.1
Tamaño y tipo de la pantalla	12.1*TFT	12.1*TFT	10.4*TFT	11.3*TFT
Resolución de la pantalla	800x600	1,024x768	1,024x768	1,024x768
Conjunto de chips para gráficos	NeoMagic Magic Media 256"V	ATI Rage Mobility M	S3 Savage IX	S3 Savage IX
Memoria para gráficos	2.5MB en SGRAM	4MB en SDRAM	8MB en SDRAM	8MB en SGRAM
Capacidad del disco duro	20GB	20GB	20GB	12GB
Unidad del disquetes externa	Incluida	Integrada en la base para la expansión, $199USD	$79USD	Incluida
Unidad CD-Room externa	$99	$125	$299	Integrada con la base para la expansión, $399
Unidad CD-RW externa	N/A	$389	$499	N/A
Unidad LS-120 SuperDisk externa Bocinas integradas	$139 1	$225 1	N/A 2	N/A 1
Contactos de línea de entrada línea de salida				
Puertos paralelo/ en serie/ infrarrojo integrados				
Puertos USB integrados	1	2	1	0
Replicador de puertos	$199	$149	N/A	$399
Estación de puertos o base para la expansión (precios en USD)	N/A	$499	N/A	$399

Tabla 4.8. Comparativo de equipo de cómputo (Continua tabla)

Ethernet 10/100 integrada				(a través del replicador de puertos)
Ranura para tarjeta PC	1 Tipo II	1 Tipo II	1 Tipo II	1 Tipo II
Bateria de alta capacidad: duración que se especifica	2 horas ($49)	3.8 horas ($161)	3 horas ($299)	9 horas ($459)
Garantía std en partes	3 años/3 años	3 años/3 años	1 año/ 1año	1 año/ 1año
Cuota por servicio en el sitio	Incluida (3 años)	$49	N/A	$79

Se presenta a continuación en la tabla 4.9 el comparativo para los equipos de manejo de voz y datos:

CONCEPTO	CISCO	MICOM
Tipo	Servidor de acceso remoto Voice Wateway	Multiplexor acceso integrado
Modelo	AS 2610	Marathon 20k PRO
Protocolo	IP, Frame Relay, HDLC, PPP	Frame Relay , Micro Band ATM
Canales por DSO	5 Canales	8 Canales
Señalización R2- MFC	Si	No
Soperte	Son fabricantes de equipo, Soporte 24 hrs en el TAC, refacciones SH,HD	10 centros de servicio, 22 oficinas, refacciones
Equipamiento	2 WIC slots, 1 Network module slot, 1 voice fax slot, 1 pto serial WAN	Voice card
Manejo de ancho de banda dinámico	Si	Si
Compresión	Voz y datos	Voz y datos
Forma de compresión a cuantos kbps	Comprime a 8	Comprime a 8
Maneja TANDEM SWITCHING	Si	No
Se asigna prioridad al tráfico de voz y datos	Si	Si
Número de sitios remotos	60	8
Número total de canales de voz por equipo	60	30
Número de equipos a interconectar	10	6
E1 que maneja	2	2
Número de puertos LAN y tipo	2 LAN, Ethernet 802.3	1 pto por cada tarjeta IRM
Número de puertos seriales	2	6
Administración y monitoreo	Cuenta con agente SNMP para propositos de administración	No cuenta con esta facilidad
Alimentación	127 VAC	127 VAC

Tabla 4.9. Comparativo de equipo de voz y datos.

Utilizando estas tablas se realizará la selección del equipo adecuado para cubrir los requerimientos de nuestro sistema a implementar.

CAPÍTULO 5

Implantación de la Red de Voz y Datos

En este capitulo se plantean las etapas de consideraciones previas a la instalación y la instalación de los equipos tanto de ruteo como los servidores y terminales de trabajo además de la configuración de los diferentes equipos, para lograr con ello una comunicación eficiente y capaz de soportar el tráfico de una gran red.

5.1. Instalación

Previo a la configuración de los equipos es necesario realizar la instalación de los mismos, se describen a continuación la información a considerar antes y después de la instalación.

5.1.1. Preparando la instalación del equipo de ruteo

Para realizar una instalación segura se recomienda seguir los siguientes pasos :

Mantener el área cercana al chasis limpia y libre de polvo durante y después de la instalación. Remueva la cubierta del chasis y coloquela en un lugar seguro.
Ponga las herramientas en un lugar seguro y evite que alguien pueda caer con ellas.
No vista ropa que genere estática y pueda dañar el chasis.
Utilice anteojos de seguridad.

El router puede ser colocado en un escritorio, montado en un rack o en una pared. La localización del soporte del chasis es extremadamente importante para el funcionamiento del equipo . Colocar equipos muy cerca uno de otro , con ventilación inadecuada y un difícil acceso a los paneles de control pueden causar fallas. Es necesario tomar precauciones sobre la buena ventilación del sitio.
Ahora debemos cuidar ciertos puntos en la colocación de los racks que sostendrán los equipos. Cuando se monta un chasis en un rack abierto se debe asegurar que el rack no bloquee las salidas de aire de los equipos, en el caso de instalar un rack cerrado, que será nuestro caso, se debe tomar en cuenta la instalación de un ventilador en la parte alta del mismo, con ello el calor generado será llevado hacia la parte alta del mismo y la dispersará en el medio ambiente.

En cuanto a las consideraciones necesarias para la alimentación de energía se debe contar con una fuente de energía libre de picos y ruido, se debe instalar un regulador de voltaje si es necesario, el router posee un switch para cambiar la operación del equipo de a 110V o 22oV, los equipos incluyen un cable de 1.8 metros para la alimentación eléctrica, se debe instalar en un circuito que maneje 120VAC y 10^{a} para su correcto funcionamiento.

Ahora prepararemos las condiciones para conectar a la red:

Cuando se prepara el equipo se deben tomar en cuenta las limitaciones de distancia y el potencial de interferencia electromagnética.
Tomando en cuenta el estándar IEEE802.3 establecido por el IEEE se necesitan los siguiente materiales:

- Cable sin blindaje 1 a 1 con conectores RJ-45 o cable 100BaseT-2pair categoría 5
- Cable coaxial delgado 10Base2-Ethernet o mejor conocido como Ethernet delgado, se debe tomar en cuenta que la máxima distancia segura es de 186 metros.
- Cable coaxial delgado 10Base5-Ethernet el cual puede ser instalado en un máximo de 500 metros.
- Cable UTP 10BaseT-Ethernet. El máximo segmento de distancia que se puede instalar es de 100 metros.

5.1.2. Instalación del equipo

Podemos montar el equipo en tres diferentes modos:

- Montando el equipo en un escritorio utilizando las cintas adhesivas en la superficie plana.
- Montando el equipo en un rack, donde si solo es un equipo debe colocarse en el fondo del mismo, utilizando los brackets que vienen en el empaque del router.
- Montando el equipo en la pared, colocando lo brackets en los lados del router y atornillandolos a la pared

Ahora debemos conectar la alimentación al router, simplemente introduciendo la clavija en el receptáculo posterior del equipo y colocando la protección para evitar desconexiones. Se recomienda no conectar el otro extremo del cable al contacto si no hasta tener completados los pasos.

Finalmente se realizan las conexiones a la red, se posicionan los hubs y los cables correspondientes.

Después de finalizar la instalación del hardware conectamos el equipo al contacto y ponemos el switch en la posición ON , con esto tenemos listo el equipo para la configuración.

5.1.3. Instalación de Servidores y estaciones de trabajo

Para estos equipos se deben tener consideraciones similares a las de la preparación para la instalación del router como son la limpieza del sitio, las consideraciones eléctricas y las fisicas que deben cumplirse.

A continuación comenzamos con las configuraciones de los equipos.

5.2. Configuración de los Servidores NT

En esta sección describiremos la metodología para dar de alta los Servidores de Dominio de las sucursales de WideCOM, incluyendo la Central en el D.F., para ello tomaremos las siguiente consideraciones: todos y cada uno de los Servidores trabajarán en TCP/IP, las direcciones IP serán fijas, tanto para los equipos de control como para los hosts (PCs, LapTops, Impresoras de Red y otros dispositivos de Red).

La configuración de los Servidores contempla los servicios estándar, necesarios para que las LAN sean funcionales, junto con sus estaciones de trabajo y capaces de compartir recursos tales como: unidades de almacenamiento, impresoras de red, carpetas y las aplicaciones necesarias para el desempeño básico de los empleados de las sucursales.

La configuración incluye las siguientes partes:

- Configuración de las Opciones de Red de Servidores

- Identificación
- Servicios
- Protocolos
- Adaptadores de Red

- Implementando Servicios el Servicio de Información de Internet
- Configuración de un Servidor de Nombres de Dominio
- Configuración de Opciones de Red de Estaciones de Trabajo

Configuración de las Opciones de Red de Servidores

La configuración de la red es fundamental para establecer las reglas de comunicación entre los elementos de la red, por ello tomamos principal cuidado en la configuración de cada uno de sus elementos. A continuación se describen las partes principales de la configuración de red.

Para accesar a las opciones de Red seguimos los siguientes pasos:

1. Pulsamos el mouse sobre la barra de inicio.
2. Vamos a "Configuración o Settings".
3. Seleccionamos "Panel de Control o Control Panel".
4. Pulsamos el mouse sobre el icono de "Red o Network".

A continuación se muestran los pasos a seguir para la configuración de la identificación en un servidor.

Identificación

Las propiedades del Servidor son imprescindibles para las estaciones de trabajo, por ello, se configura un Nombre de Servidor y un Grupo de Trabajo o Dominio. La configuración de Identificación de Servidor se muestra en la figura 5.1.

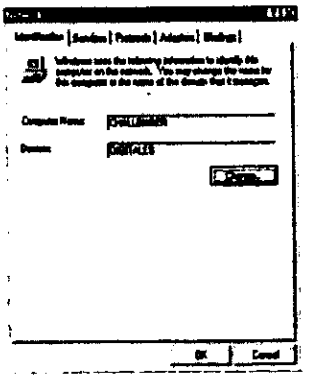


Figura 5.1. Configuración de la Identificación de un Servidor NT.

Ahora se configuran los servicios tales como de impresión, comunicación, control etc.

Servicios

Cada Servidor tiene un uso particular y específico dentro de la Red, esto dependerá del tipo de servicios que tenga instalados e inicializados, para soportar aplicaciones de: comunicación, control, impresión, etc. La ventana de configuración se servicios se muestra en la figura 5.2.

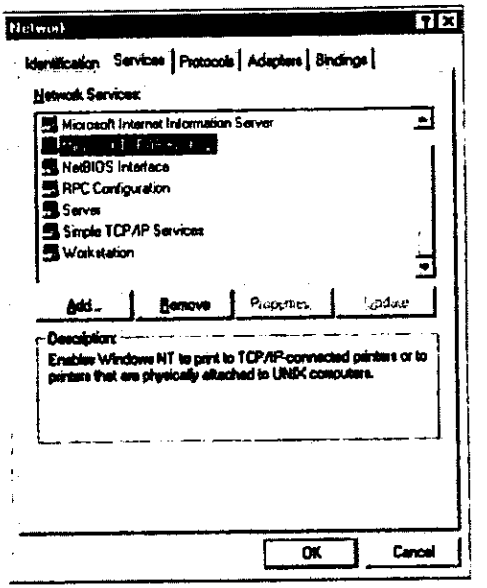


Figura 5.2. Configuración de Servicios de un Servidor NT.

Por ejemplo.

Para agregar los Servicios de Impresión se siguen los siguientes pasos:

1. Pulsamos el botón derecho del mouse sobre el icono "Add" dentro de la opción de Servicios.

2. Seleccionamos el Servicio de Impresión con TCP/IP.

3. Definimos la dirección de los archivos del Servicio pulsando el botón derecho del mouse sobre el icono "Have Disk".

En la figura 5.3 se muestra la ventana de Servicios de Red para agregar los servicios de impresión con TCP/IP.

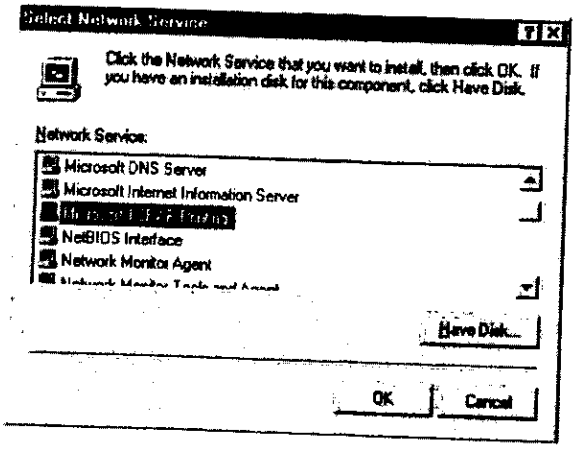


Figura 5.3. Seleccionando un Servicio para un Servidor NT.

Para el uso de determinados archivos de configuración tenemos que recurrir a carpetas de trabajo, a continuación se identifica una de las carpetas de trabajo importantes.

La Carpeta i386 de NT

Todos y cada uno de los archivos de configuración se encuentran en la carpeta i386 del Disco de NT Server. Siempre que se requiera añadir un servicio será necesaria dicha carpeta. Toda vez que se cargue un nuevo servicio a un Servidor NT, éste tendrá que reinicializarse. La figura 5.4. muestra la ventana de solicitud de la carpeta i386 para añadir servicios.

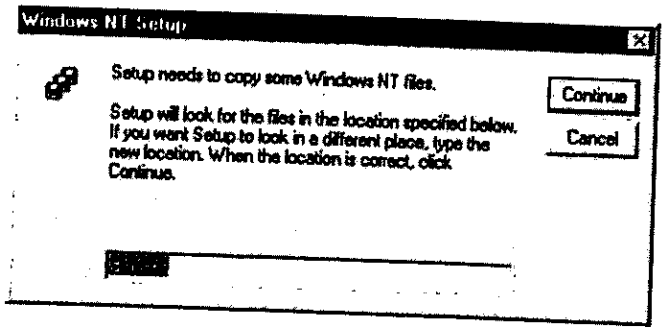


Figura 5.4. Ventana de solicitud de la carpeta i386.

Teniendo en cuenta que los equipos pueden fungir como multitareas presentamos la configuración de un equipos con diferentes tarjetas.

Protocolos

Los Servidores pueden tener instaladas más de una tarjeta de red y también más de un protocolo a la vez en cada una de ellas, para mantenerse comunicado con otros servidores o dispositivos de la Red. En la figura 5.5. se muestran tres protocolos de comunicación y transporte de datos cargados en la configuración de la Red.

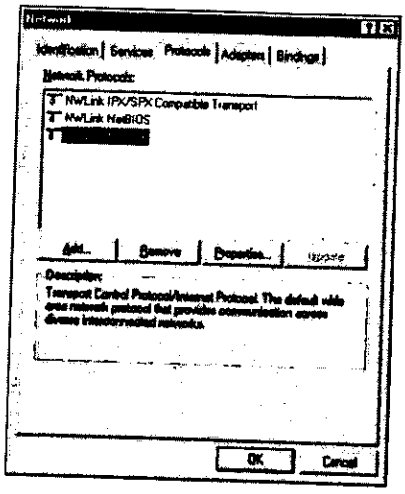


Figura 5.5. Ventana de protocolos de las opciones de Red.

Para agregar un protocolo seguimos los siguientes pasos:

1. Pulsamos la tecla Add, dentro de la ventana de protocolos.
2. Seleccionamos el protocolo.
3. Inmediatamente nos pide la Dirección de la carpeta con los archivos. Podemos seleccionar la opción "Have Disk" para especificar la ruta adecuada.

En la figura 5.6. se muestra la ventana de selección de protocolos de Red para el Servidor NT.

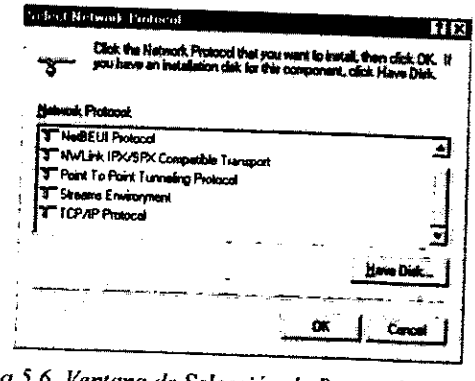


Figura 5.6. Ventana de Selección de Protocolo de Red.

Adaptadores de Red

Los servidores son capaces de soportar más de una tarjeta de Red, y trabajar con diferentes protocolos al mismo tiempo, por ello existe esta opción, donde podemos configurar cada una de las tarjetas. Como se muestra en la figura 5.7

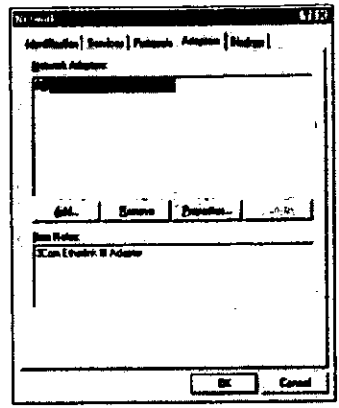


Figura 5.7. Ventana de Configuración de Red.

Después de configurar los adaptadores de red necesitamos configurar los enlaces que se trabajaran en nuestra red.

Enlaces

Las enlaces de Red son conexiones entre tarjetas, protocolos y servicios instalados en el servidor. Podemos usar esta ventana para habilitar o deshabilitar dichas conexiones o definir el orden en como el servidor encontrará la información en la Red. La figura 5.8 muestra la ventana de Red con la opción de configuración de enlaces del Servidor en la Red.

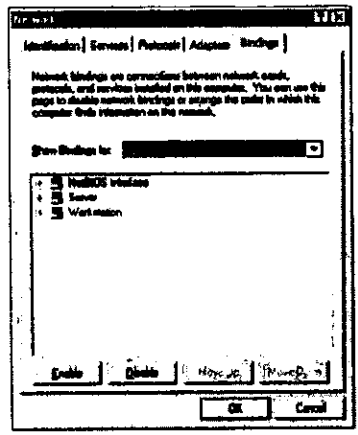


Figura 5.8. Ventana de Red con la opción de configuración de enlaces.

Ahora procedemos a la configuración de un servidor de Internet.

Instalación del IIS *(Internet Information Server, Servidor de Información de Internet)*

Los pasos para llevar a cabo esta configuración son los siguientes:

1. Desde el escritorio, seleccionar "Start/Run".

Se muestra en la figura 5.9 el gráfico correspondiente:

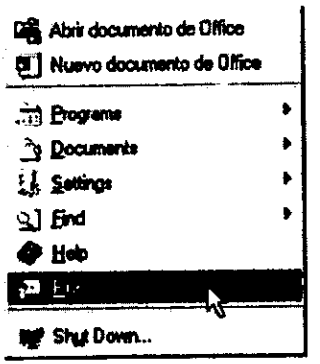


Figura 5.9. Menú de programas de inicio.

2. Desde la caja de selección Run, seleccionar "Browse".

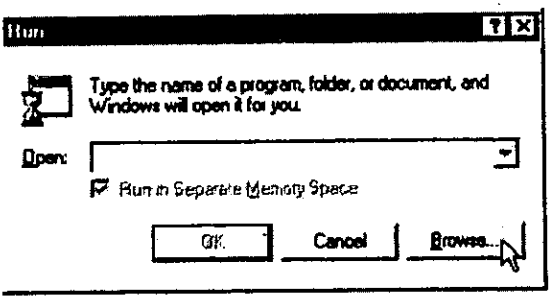


Figura 5.10. Ventana de ejecutar programas..

3. *Buscar en la carpeta "i386" la dirección "i386\Inetsrv\Inetstp.exe".*

4. Después de elegir archivo correcto, seleccionar "Open".

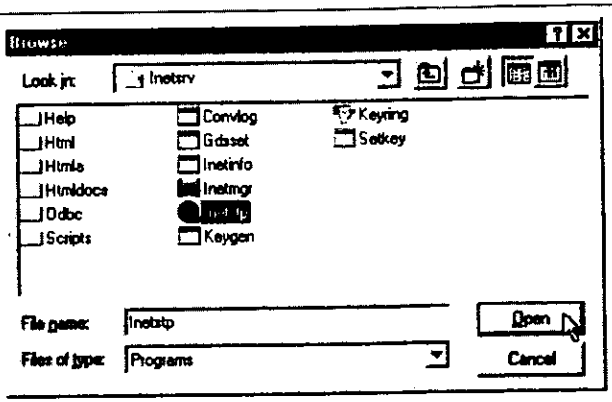


Figura 5.11. Ventana para buscar y seleccionar archivos ejecutables.

5. Aparece la caja de diálogo Run, selecciona "Ok" para continuar.

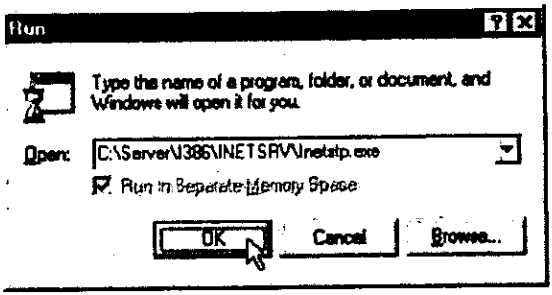


Figura 5.12. Ruta de ubicación del archivo "Inetstp.exe.

6. Se despliega la caja de diálogo del Servidor de Información de Internet de Microsoft, selecciona "Ok".

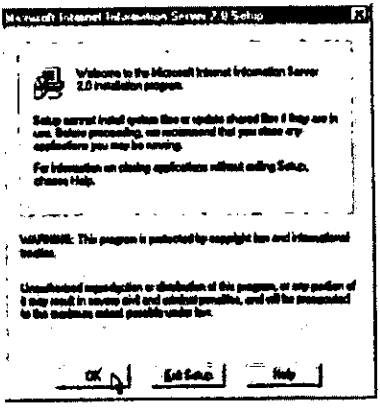


Figura 5.13. Ventana de configuración del IIS.

7. Aparece la caja de configuración del IIS de Microsoft, selecciona "Add/Remove".

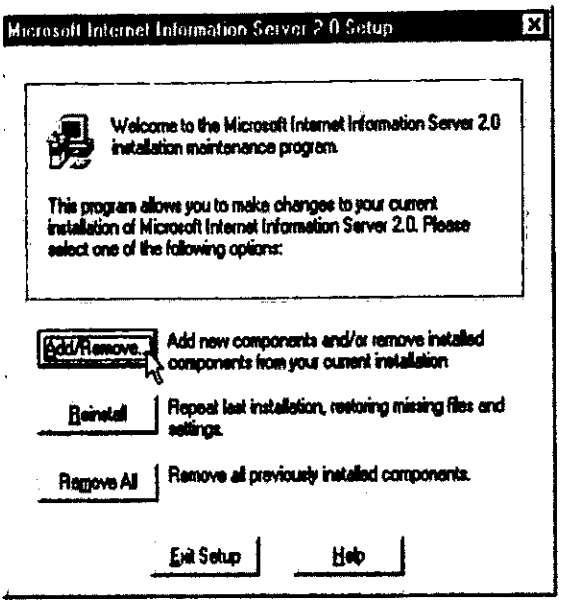
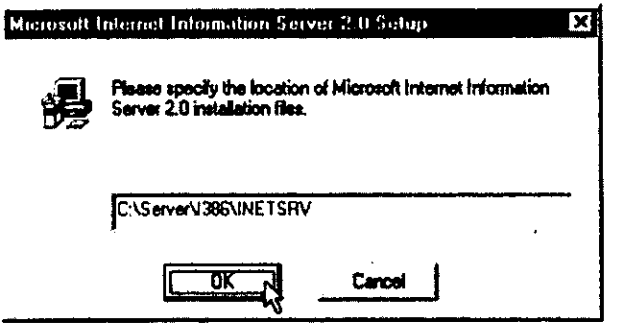


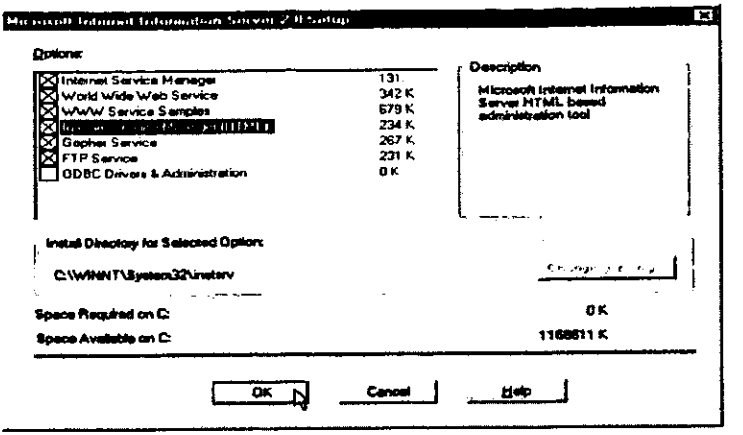
Figura 5.14. Ventana opciones de configuración del IIS.

8. Aparece una ventana para verificar la dirección del IIS, Selecciona "Ok".



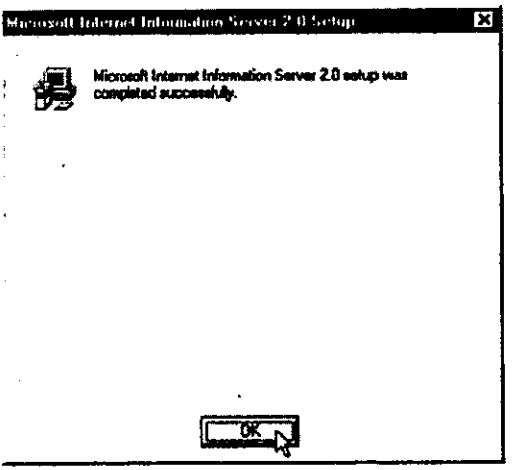
5.15. Ventana de verificación de la ruta del archivo Inetsrv.exe.

9. Revisa que esté seleccionada la caja del Administrador de Servicios de Internet (HTML), selecciona Ok.



5.16. Ventana de selección de Opciones del IIS Server.

10. Aparece la caja de dialogo indicando el fin de la instalación del IIS, selecciona Ok.



5.17. Ventana de fin de instalación del IIS.

11. Fin de la instalación.

Con estos pasos ha quedado finalizada la instalación de un servidor de Internet, a continuación se procede a configurar las terminales de trabajo.

5.3. Configuración de las Opciones de Red para Estaciones de Trabajo

Configurar las opciones de red conlleva las opciones de identificación de la estación de trabajo, grupo de trabajo o dominio, control de acceso, protocolo y otras opciones, que van de acuerdo a las necesidades de control, acceso y comunicación de las empresas.

Dentro del corporativo WideCOMM trabajaremos en un ambiente de Windows NT 4.0, con estaciones de trabajo operando bajo Windows 98 y el protocolo IP.
La configuración de las opciones de red se describen a continuación. Para ello seguiremos los siguientes pasos.

1. En el escritorio de la computadora a configurar y con el puntero del ratón sobre el icono "Entorno de Red", pulsamos el botón derecho .

Aparecerá el menú de opciones de red, seleccionamos el icono "Propiedades". En la figura. 5.18. Se muestra la ventana de opciones de red.

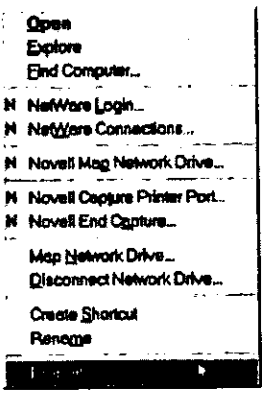


Figura 5.18. Opciones del icono entorno de red.

2. Aparece la ventana de Opciones de Red. Dentro de esta ventana encontramos las opciones de configuración, identificación y control de acceso.

En la opción de configuración configuramos los clientes y tarjetas de red, protocolos, accesos telefónicos, compartimento de carpetas e impresoras.

3. Dentro de la ventana de Identificación, figura 5.19, encontramos la información que identificará a la estación de trabajo o computadora, con datos como: nombre de la computadora, grupo de trabajo y una descripción de más detallada del equipo. En la figura 5.20. Se muestra la ventana de red en su opción de identificación.

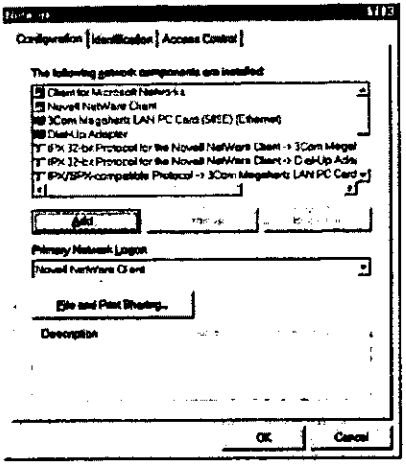


Figura 5.19. Ventana de configuración de opciones de red.

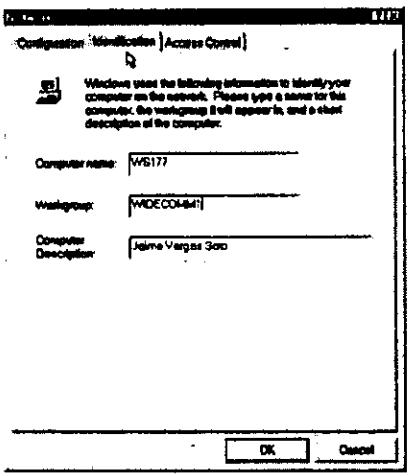


Figura 5.20. Ventana de configuración de identificación de las computadoras de la red.

4. Por último tenemos la opción de configuración del control de acceso, figura 5.21. Ésta nos permitirá controlar la entrada a un grupo de trabajo o dominio por medio de un cliente de red. Lo anterior será por con una ventana que restringe la entrada a la red mediante un nombre de usuario y una clave de acceso.

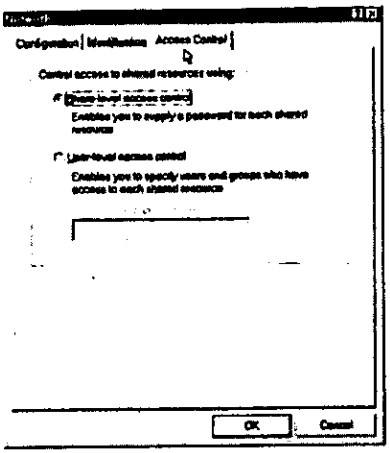


Figura 5.21. Ventana de configuración del control de acceso a la red.

5. Para configurar la dirección IP de las computadoras entramos a la ventana de configuración de red y buscamos "TCP/IP". Con el puntero del ratón sobre esta opción seleccionamos propiedades. En la figura 5.22. se muestra la ventana de configuración del protocolo TCP/IP.

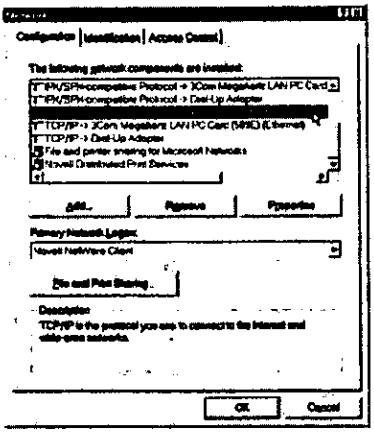


Figura 5.22. Ventana de configuración del protocolo TCP/IP.

6. Dentro de la configuración de la dirección IP encontramos dos opciones de obtener una dirección IP automáticamente o una IP específica; el primer caso se usará si existe un Servidor con servicios de DHCP, es decir, otra computadora que asigne direcciones IP a las estaciones con acceso al dominio o grupo de trabajo que controla. En el segundo caso pondremos una dirección fija y la máscara de subred correspondiente de acuerdo a la red en que trabajará este equipo. Posteriormente bastará con seleccionar Ok para continuar con la

configuración. En la Figura 5.23. Se muestra la configuración de las direcciones IP y de máscara de subred de una computadora.

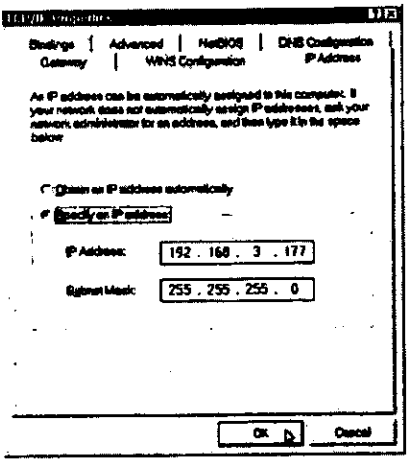


Figura 5.23. Ventana de configuración de la dirección IP de una computadora.

7. Por último, es necesario configurar la puerta de salida o gateway. Esto sólo es necesario si se maneja una computadora para salir de la Intranet de la empresa y accesar al la Internet o a servicios fuera de la red LAN de la que depende la computadora configurada. Si este es el caso, la dirección corresponde a la del servidor que provee tal servicio. La figura 5.24. muestra la ventana de configuración de la puerta de salida de una computadora.

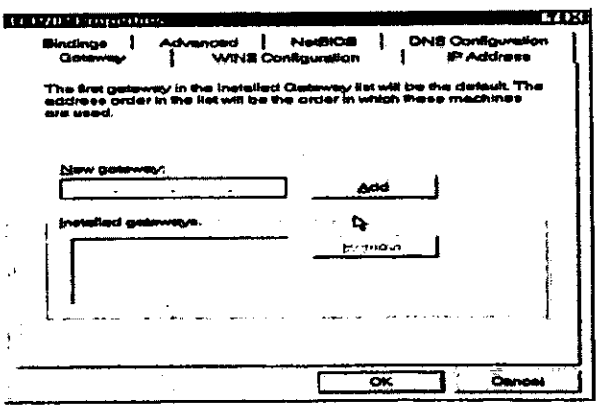


Figura 5.24. Ventana de configuración de la puerta de acceso de una computadora.

8. Otra parte de la configuración es el compartimento de recursos, en este caso, archivos e impresoras, figura 5.25. Para configurar estas opciones, regresamos a las opciones de red y seleccionamos el icono "Compartir archivos e impresoras".

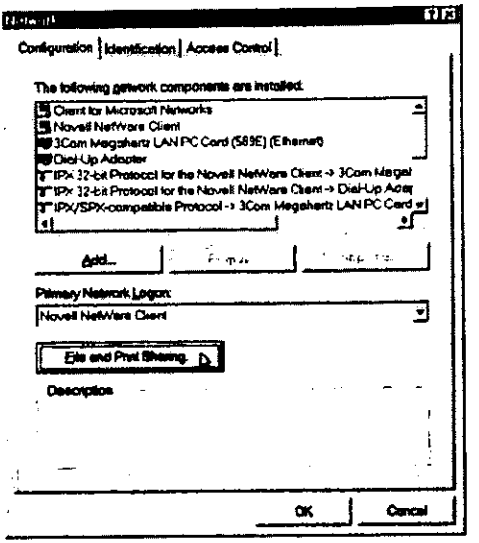


Figura 5.25. Ventana de opciones de red y compartimento de recursos.

9. Aparecerá la ventana de compartimento de archivos e impresoras. Dentro de ella, podemos seleccionar las opciones convenientes en cada caso. Después de lo anterior, sólo es necesario dar ok para terminar. La figura 5.26 muestra la ventana de compartimento de archivos e impresoras.

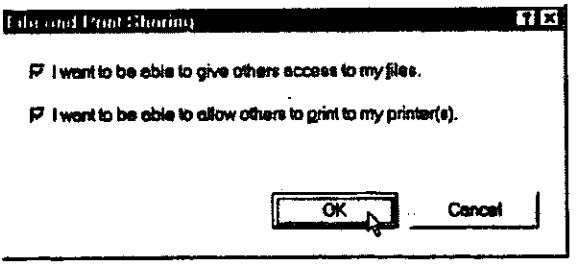


Figura 5.26. Ventana de compartimento de archivos e impresoras entre computadoras.

10. La parte final de la configuración, consiste en la selección del cliente para redes Microsoft, como se muestra en la figura 5.27. Para ello elegimos el cliente y entramos a sus propiedades.

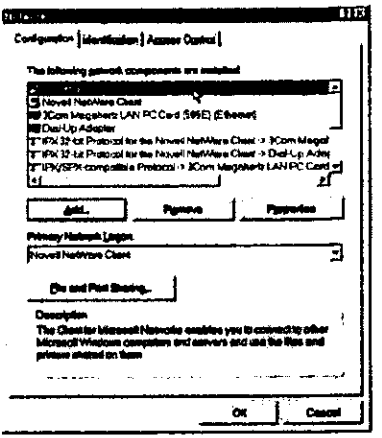


Figura 5.27. Ventana de configuración del cliente de redes Microsoft.

11. En las opciones del cliente encontramos: la validación como cliente de red dentro de un dominio y la validación rápida a la red. En la figura 5.28 mostramos las opciones de validación del cliente de redes Microsoft.

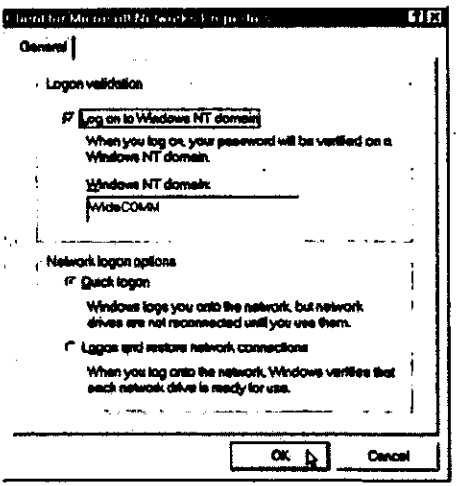


Figura 5.28. Ventana configuración de las opciones del cliente de redes Microsoft.

12. Para concluir la configuración de las opciones de red aceptamos la configuración pulsando ok hasta cerrar la ventana de configuración de red y reiniciar el equipo.

Después de reiniciar la computadora entramos al entorno de red de WideCOMM para verificar el acceso a la red. Lo anterior se muestra en la figura 5.29.

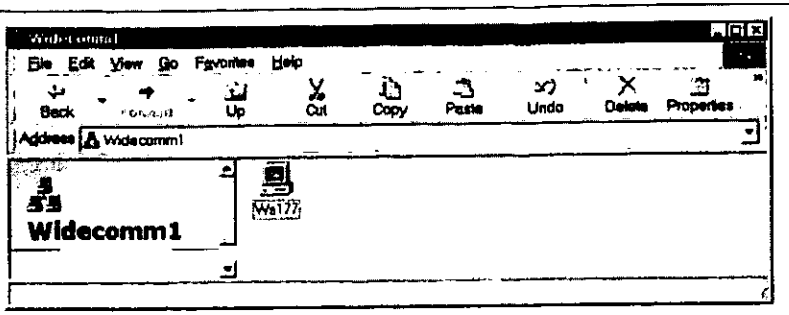


Figura 5.29. Ventana de la Red del corporativo WideCOMM.

Con esto terminamos la configuración de la opciones de red cada una de las estaciones de trabajo.

5.4. Implementación de la WAN

Para la implementación de la red WAN en el corporativo WIDECOM se va a manejar un direccionamiento por medio de IP, el cual nos permitirá enlazar las ciudades de México, Guadalajara, Monterrey, León, Querétaro, Toluca, San Juan del Río y Gómez Palacio. A estas ciudades les denominaremos nodos.

Para paquetes de información de un nodo a otro, las redes de conmutación deben determinar de manera constante la trayectoria correcta (enrutamiento). El descubrimiento de rutas será el proceso a usar para identificar los posibles caminos que pueda tomar la información.

El direccionamiento en IP se compone en dos partes: del número que especifica a la red y él número que especifica al host dentro de la misma red. Para nuestro caso trabajaremos con un direccionamiento de IP de capa B (172.16.10.0). IP trabaja en la capa 3 del modelo OSI, la cual busca las rutas posibles en la red, selecciona la mejor, la aprende y la transmite.

El enrutamiento se puede realizar compilando y enviando tablas de ruteo a los ruteadores que estén conectados. Cada ruteador construye su propia tabla al intercambiar información con los demás. En la red pueden existir muchos ruteadores y cada uno de ellos solamente obtiene información de sus vecinos.

En la figura 5.30 se muestra en forma genérica la distribución de los nodos para la red WAN a utilizar por el corporativo. Como se puede apreciar esta red consta de dos nodos principales: el primero estará ubicado en la ciudad de México, este nodo es una conexión punto multipunto, el segundo estará ubicado en la ciudad de Querétaro, el cual a diferencia del primero solo es un enlace punto a punto. Se cuenta con equipos ruteadores que se encargaran de cumplir que los enlaces se mantengan funcionales y en alta productividad.
El direccionamiento se distribuirá como lo muestra la tabla 5.1 En la conexión entre nodos estaremos trabajando con 30 bits para la máscara de subred, lo cual es más que suficiente para nuestros requerimientos, ya que con esto obtendremos 4 direcciones de

subred para cada nodo; cabe aclarar que sólo dos serán disponibles, debido a que una de ellas estará asignada para broadcast y una para la subred, por lo tanto sólo se tendrán disponibles dos direcciones, que se asignarán para los ruteadores en cada uno de los nodos.

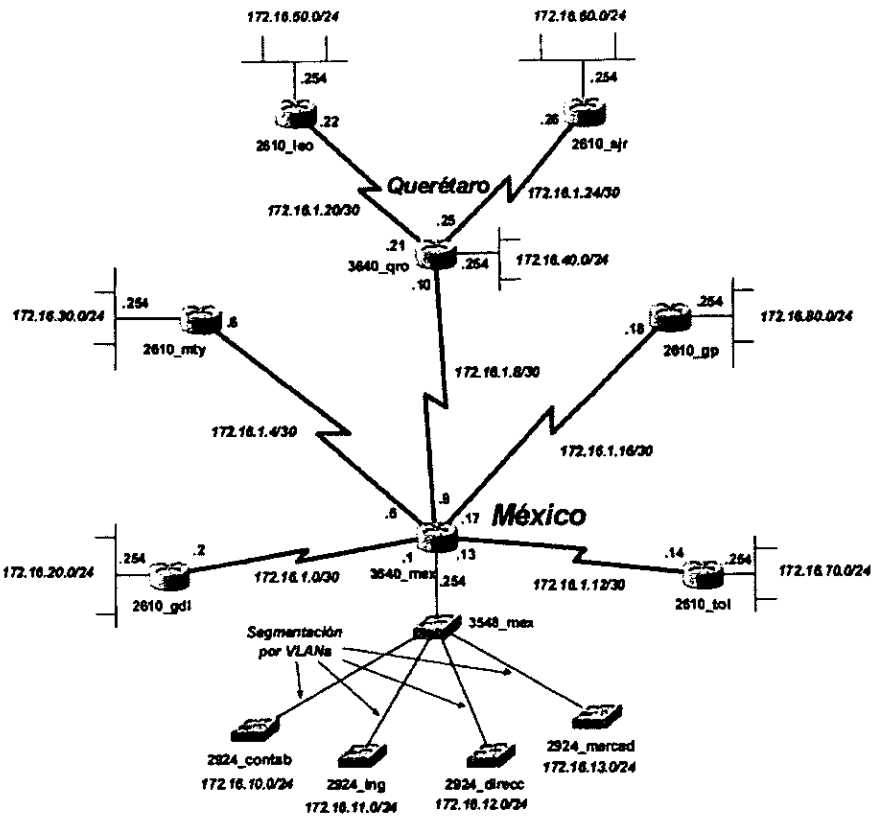


Figura 5.30. Implantación de la red WAN.

Ciudad	Subred	Broadcast
México	172.16.1.0	
Guadalajara	172.16.1.4	172.16.1.3
Monterrey	172.16.1.8	172.16.1.7
Querétaro	172.16.1.12	172.16.1.11
Toluca	172.16.1.16	172.16.1.15
Gómez Palacio	172.16.1.20	172.16.1.19
León	172.16.1.24	172.16.1.23
San Juan del Río	172.16.1.28	172.16.1.27

Tabla 5.1. Asignación de dirección IP para subred y broadcast.

De esta manera se observa que las ciudades de Guadalajara, Monterrey, Querétaro, Toluca y Gómez Palacio estarán enlazadas directamente a la ciudad de México; mientras que san Juan del Río y León tendrán enlace directo sólo con Querétaro, que a su vez será la encargada de enlazar la comunicación de estas dos ciudades al nodo central en México.
En la tabla 5.2 se muestra la asignación de direccionamiento IP para los routers a utilizar en el corporativo de acuerdo a su enlace:

ENLACES	
México 172.16.1.1	Guadalajara 172.16.1.2
México 172.16.1.5	Monterrey 172.16.1.6
México 172.16.1.9	Querétaro 172.16.1.10
México 172.16.1.13	Toluca 172.16.1.14
México 172.16.1.17	Gómez Palacio 172.16.1.18
Querétaro 172.16.1.21	León 172.16.1.22
Querétaro 172.16.1.25	San Juan del Río 172.16.1.26

Tabla 5.2. Asignación dirección IP para routers.

Por otro lado, la distribución en los nodos estará compuesta de la siguiente manera: se asignarán direcciones con máscaras de subred de 24 bits cada una, de esta forma se podrá tener un rango de direcciones para la subred de cada localidad, que va desde la dirección 1 hasta la 254. Por ejemplo, en Guadalajara las direcciones serán desde la 172.16.20.1 hasta la 172.16.20.254; la asignación de manera local de cada uno de los nodos se muestra en la tabla 5.3. Las direcciones con terminaciones de 1 a 10 serán reservadas para la asignación de servidores, y las de terminación 254 serán reservadas para el router dentro de la subred. Con esto se tendrán disponibles para la asignación a laptops y PCs las direcciones comprendidas de la 11 hasta la 253, que cubren perfectamente el requerimiento de direcciones para hosts en cada localidad.

México	172.16.10.0
Guadalajara	172.16.20.0
Monterrey	172.16.30.0
Querétaro	172.16.40.0
Toluca	172.16.50.0
Gómez palacio	172.16.60.0
León	172.16.70.0
San Juan del Río	172.16.80.0

Tabla 5.3. Asignación dirección IP en nodos.

Por último, también se proveerá el servicio de facturación de localidades que no estén dentro de los enlaces mencionados. En esta caso se tendrán las regiones de Puebla, Villahermosa, Veracruz, Reynosa, San Luis Potosí, Ciudad Juárez, Chihuahua y Morelia. Estas localidades tendrán el acceso a nuestra red por medio de un servicio de Internet, que permitirá enviar la documentación necesaria del usuario. Para lograr el enlace se asignarán direcciones IP con máscara de subred también de 24 bits. En la tabla 5.4. se lista el direccionamiento para estas ciudades. Las direcciones se ordenarán de la misma manera que los nodos locales, implicando que para la asignación de servidores se utilizarán las primeras 10 direcciones, con la diferencia de que aquí no existirá un router en la localidad, por ello no existe una dirección reservada para el mismo.

Puebla	172.16.110.0
Villahermosa	172.16.120.0
Veracruz	172.16.130.0
Reynosa	172.16.140.0
San Luis Potosí	172.16.150.0
Cd Juárez	172.16.160.0
Chihuahua	172.16.170.0
Morelia	172.16.180.0

Tabla 5.4. Asignación dirección IP localidades vía Internet.

5.5. Implantación del Plan de Marcación

El presente plan de asignación de cadenas y generación de las rutas de marcado tiene como objetivo establecer las bases para una adecuada administración y uso de la numeración disponible para el proyecto, mediante la asignación eficiente, justa, equitativa y no discriminatoria de los recursos disponibles.

5.5.1. Asignación de cadenas y generación de las rutas de marcado

En la figura 5.31 se muestra la conexión que se realizará para lograr la comunicación entre los diferentes equipos y la PSTN, para iniciar una comunicación exitosa por la red, basada en el plan de marcación diseñado. En esta figura observamos como el usuario que genera la llamada se encuentra conectado al conmutador, digita el CODEC para obtener el servicio de una troncal digital y realizar la conexión por la red.
Para llevar a cabo esta comunicación se tiene que configurar los equipos involucrados en la misma, comenzaremos con el PBX :

Emplearemos herramientas de administración del sistema como los dispositivos de entrada/salida mencionados a continuación:

- Una terminal TTY o VDT como dispositivo de entrada/salida.
- Una impresora compatible con RS232 como dispositivo de salida únicamente.
- Un teléfono SL-1 como dispositivo de entrada únicamente.

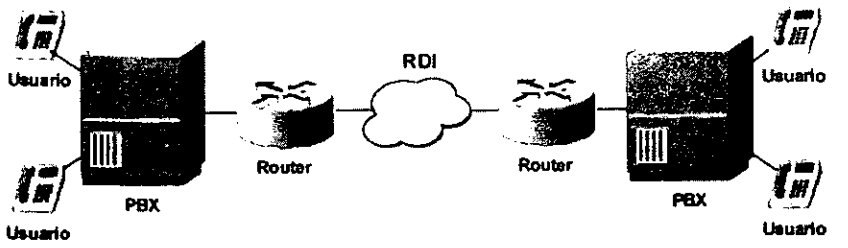


Figura 5.31. Conexión para iniciar el marcado por red.

Los sistemas de entrada o salida pueden operar con terminales teniendo las siguientes características:

- Interfase: RS232C
- Código: ASCII
- Velocidad: 110, 300, 1200, 2400, 4800, y 9600 baud.
- Corriente de Loop: 20 mA

Para accesar al modo de configuración del sistema se requiere un código de acceso , el cual nos permite navegar por las diferentes pantallas, se teclea el código de acceso y ahora ingresaremos a las pantallas de mantenimiento del equipo, donde pulsamos el comando DN que nos lleva al modo de mantenimiento. Dentro de este modo podemos utilizar los programas de administración y mantenimiento que son empleados para definir la configuración del sistema y opciones de función. Estos tipos de programas trabajan en el formato de respuesta por prompt y se usarán para: Habilitar y deshabilitar pruebas de hardware, obtener el estado del hardware y desarrollar pruebas del equipo

A continuación se presenta la configuración del conmutador.

```
OVL000
>LD 20


PT0000
MARP NOT ACTIVATED

REQ  PRT
TYPE DID
TN   7
CUST 0
DATE
PAGE

PROGRAMACION DE LOS 30 PUERTOS PERTENECIENTES A LA RUTA DE TRONCALES
DID = SE PROGRAMAN EN EL LD 14

****************************************
```

```
TN   007 01       PUERTO DEL PBX: 7 = NO. SLOT O TARJETA,     1 = PUERTO
1/30 DE LA TARJETA
TYPE DID                TIPO DE TRONCAL = DID
CUST 0                  GRUPO AL QUE PERTENECE, CUSTOMER = 0, DONDE
PERTENECE TODO EL CORPORATIVO
TRK  DTI2               TRUNK DATA BLOCK = DTI2
SICA 1                  Signaling Category table number
PDCA 1                  PAD table number
PCML A                  Mu-Law or A-law companding law = A-LAW
NCOS 1                  Network Class Of Service
RTMB 6 1                Route Member = Ruta 6 Miembro 1
NITE             Night Service Directory Number (DN)
CLS  UNR MFC CND WTA LPR APN THFD  P10
                              Class of service options =      UNR =
Unrestricted
                                                    MFC =
                                                    CND =
                                                    WTA = Warning tone
Allowed
                                                    LPR = Low Priority
Trunk
                                                    THFD = Centrex
Switchhook Flash Denied
                                                     P10 = Make-break ratio
for dial pulse dialing; primary
                                                              10 pps
(pulses per second)

MFL  0
MFPD NO
TKID             ID de la troncal = DESCRIPCION
DTCR NO
DATE 25 JUN 2001        Fecha de programación.
*****************************************


TN   007 02
TYPE DID
CUST 0
TRK  DTI2
SICA 1
PDCA 1
PCML A
NCOS 0
RTMB 6 2
NITE
CLS  UNR MFC CND WTA LPR APN THFD
     P10
MFL  0
MFPD NO
TKID
DTCR NO
DATE 21 MAY 2000

TN   007 03
TYPE DID
CUST 0
TRK  DTI2
SICA 1
PDCA 1
PCML A
```

```
NCOS 0
RTMB 6 3
NITE
CLS  UNR MFC CND WTA LPR APN THFD
     P10
MFL  0
MFPD NO
TKID
DTCR NO
DATE 11 MAY 2000
*********************************************

PROGRAMACION DE LA RUTA 6 DE TRONCALES DID


REQ  PRT
TYPE RDB
TN
CUST 0
DATE
PAGE


REQ  END
>LD 21

PT1000
**********************
CREACION DE LA RUTA DE TRONCALES DIGITALES = SE PROGRAMA EN EL LD 16
**************************
REQ  PRT
TYPE RDB
CUST 0
ROUT 6
**********************


TYPE RDB                ROUTE DATA BLOCK
CUST 00                 CUSTOMER = 0
DMOD
ROUT 6                  ID DE LA RUTA = 6
TKTP DID                TIPO DE TRONCALES = DID
SAT  NO                 TRUNK ROUTE VIA EARTH ORBITING SATELLITE
TRANSMISSION = NO
RCLS EXT                ROUTE CLASSMARKED AS EXTERNAL
DTRK YES                DIGITAL TRUNK = YES
DGTP DTI2               DIGITAL TRUNK TYPE = DTI 2 MB
DSEL VCE                VOICE ONLY
PTYP DCO                TIPO DE PUERTO EN EL LADO REMOTO = DIGITAL /
C.O. (ANALOGICO)
AUTO NO                 AUTERMINATE = NO
ICOG IAO                INPUT AND OUTPUT CALLS = LLAMADAS SALIENTES Y
ENTRANTES
SRCH RRB                TIPO DE BUSQUEDA DE LAS TRONCALES = ROUND
ROBIN, DE MAYOR A MENOR HASTA COMPLETAR EL CICLO
STEP
ACOD 78                 ACCESS CODE = NUMERO DE ACCESO PARA TOMAR UNA
TRONCAL DE LA RUTA
TARG
OABS
INST
```

```
IDC  NO                  INCOMING DID DIGIT CONVERSION ON THIS ROUTE =
NO, NO REALIZAR NINGUNA CONVERSION DE DIGITOS
DCNO 0 *
NDNO 0
DEXT NO                  DIGIT DISPLAY OPTION = NO
MFC  R2MF          R2 MODIFICADO
MFCI 1
R2MD YES
DIG# 4                   NUMERO DE DIGITOS ESPERADOS = 4
SGL  NO
BSSU NO
MFCO 1
OPP  NORM
SWP  NORM
TIMR MFC 12032
     MFO 0
     ICF 512
     OGF 512
     EOD 13952

     DSI 34944
     NRD 10112
     DDL 70
     ODT 4096
     RGV 640
     FLH 512
     GTO 896
     GTI 896
     TFD 0
SST  5 0
DTD  NO
SCDT NO
2 DT NO
NEDC ETH           NEAR END DISCONNECT CONTROL = EITHER (CUALQUIERA)
FEDC ETH           FAR END DISCONNECT CONTROL = EITHER (CUALQUIERA)
CPDC NO
DLTN YES
HOLD 02 02 40
SEIZ 02 02
SVFL 02 02
OPCB NO
DDO  NO
DRNG NO
CDR  YES           CDR TO OUTPUT FOR CALLS ON TRUNK IN THIS ROUTE =
DESPLIEGUE DE REGISTRO DE LLAMADAS (MONITOREO)


PAGE 002

INC  YES                 CDR PARA LLAMADAS ENTRANTES = YES
TTA  YES
ABAN YES
OAL  YES
AIA  YES
OAN  YES
OPD  YES
NDP  EXC 0
NATL YES
SSL
CFWR NO
IDOP NO
```

```
MUS  YES                    MUSIC ON HOLD = YES
MRT  40                     RUTA DE MUSICA = 40 (SI MARCAMOS EL 7140,
ENTRAMOS A LA RUTA 40 QUE ES DONDE SE CONECTA EL PROGRAMUSIC)
EQAR NO
FRL  0 0
FRL  1 1
FRL  2 2
FRL  3 3
FRL  4 4
FRL  5 5
FRL  6 6
FRL  7 7
PANS YES
TTBL 0
OHTD NO
PLEV 2
OPR  NO
RCAL NO
MCTS NO
ALRM NO
BTT  30
ACKW NO
CNIT NO
CTAT YES
ART  0
OPDL 0
PECL NO
DCTI 0
NADT 0

REQ  END
```

Con estos pasos hemos configurado al conmutador para que cada vez que el usuario digite el número 77 asigne una troncal digital y se encuentre listo para realizar el traslado de la llamada.

Ahora se realizará la configuración básica del router para que la llamada sea procesada correctamente, al igual que en la configuración anterior se trata de dar una breve explicación de los comandos:

En las siguientes líneas se hace el llamado para configurar el router:

```
2610_pruebas#config t
2610_pruebas#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
2610_pruebas(config)#dial-p          * Aquí comenzamos a configurar los dial peers.
2610_pruebas(config)#dial-peer vo
2610_pruebas(config)#dial-peer voice ?
  <1-2147483647>  Voice dial-peer tag

2610_pruebas(config)#dial-peer voice ?
  <1-2147483647>  Voice dial-peer tag

2610_pruebas(config)#dial-peer voice 10 ?
  pots  Telephony
```

```
 voatm  Voice over ATM              * en esta sección se configura el modo de VoIP
 vofr   Voice over Frame Relay
 voip   Voice over IP

2610_pruebas(config)#dial-peer voice 10 voip ?
 <cr>

2610_pruebas(config)#dial-peer voice 10 voip
2610_pruebas(config-dial-pee)#des
2610_pruebas(config-dial-pee)#destination-pattern +7... *Patrón de destino
2610_pruebas(config-dial-pee)#destination-pattern +7...
2610_pruebas(config-dial-pee)#se
2610_pruebas(config-dial-pee)#ses
2610_pruebas(config-dial-pee)#session ?
 protocol   The session protocol to be used in getting to this peer
 target     The session target for this peer
 transport  The transport layer protocol used for this peer

2610_pruebas(config-dial-pee)#session tra□ □□ □arget ?
 WORD  A string specifying the session target

2610_pruebas(config-dial-pee)#session target ipv4:?
WORD

2610_pruebas(config-dial-pee)#session target ipv4:172.16.3.158 ? * Dirección IP
 <cr>

2610_pruebas(config-dial-pee)#session target ipv4:172.16.3.158
2610_pruebas(config-dial-pee)#
2610_pruebas(config-dial-pee)#
2610_pruebas(config-dial-pee)#exitr
                  ^
% Invalid input detected at '^' marker.

2610_pruebas(config-dial-pee)#□exit
2610_pruebas(config)#
2610_pruebas(config)#
2610_pruebas(config)#dial-□
2610_pruebas(config)#dial-p
2610_pruebas(config)#dial-peer vo
2610_pruebas(config)#dial-peer voice □ □□ □□ □□ □□ □
2610_pruebas(config)#dial-peer voice □ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□
□□ □□
2610_pruebas(config)#dial-□
2610_pruebas(config)#dial-?
dial-control-mib  dial-peer

2610_pruebas(config)#dial-p
2610_pruebas(config)#dial-peer vo
2610_pruebas(config)#dial-peer voice 11 ?
```

```
 pots  Telephony
 voatm  Voice over ATM
 vofr  Voice over Frame Relay
 voip  Voice over IP

2610_pruebas(config)#dial-peer voice 11 pots
2610_pruebas(config-dial-pee)#des
2610_pruebas(config-dial-pee)#destination-pattern +778*
2610_pruebas(config-dial-pee)#op□ □□ □p?
permission port preference prefix progress_ind

2610_pruebas(config-dial-pee)#po
2610_pruebas(config-dial-pee)#port ?
  <1-1>  Voice interface slot #

2610_pruebas(config-dial-pee)#port 1?
/

2610_pruebas(config-dial-pee)#port 1/?
  <0-1>  Voice interface SubUnit #

2610_pruebas(config-dial-pee)#port 1/0?
/

2610_pruebas(config-dial-pee)#port 1/0/?
  <0-1>  Voice interface port # within vic

2610_pruebas(config-dial-pee)#port 1/0/0 ?
  <cr>

2610_pruebas(config-dial-pee)#port 1/0/0
2610_pruebas(config-dial-pee)#
2610_pruebas(config-dial-pee)#^Z
2610_pruebas#
2610_pruebas#
2610_pruebas#
00:29:10: %SYS-5-CONFIG_I: Configured from console by console
2610_pruebas#
2610_pruebas#sh ru
% Ambiguous command:  "sh ru"
2610_pruebas#sh run
Building configuration...

Current configuration : 1103 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname 2610_pruebas
!
logging rate-limit console 10 except errors
enable secret 5 $1$.Mhf$CCDselTRxkCCaNdg6B.H5.
enable password delta1
!
memory-size iomem 10
ip subnet-zero
no ip routing
!
!
no ip finger
!
no ip dhcp-client network-discovery
 --More-- □□□□□□□□□      □□□□□□□□□call rsvp-sync
interface Ethernet0/0
 ip address 172.16.11.1 255.255.255.252
 no ip route-cache
 half-duplex
!interface Serial0/0
 no ip address
 no ip route-cache
 shutdown
 no fair-queue
!
interface Serial0/1
 no ip address
 no ip route-cache

2610_pruebas(config)#rouet□
2610_pruebas(config)#router ?              * Asiganción del protocolo de ruteo.
  bgp     Border Gateway Protocol (BGP)
  egp     Exterior Gateway Protocol (EGP)
  eigrp   Enhanced Interior Gateway Routing Protocol (EIGRP)
  igrp    Interior Gateway Routing Protocol (IGRP)
  isis    ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile  Mobile routes
  odr     On Demand stub Routes
  ospf    Open Shortest Path First (OSPF)
  rip     Routing Information Protocol (RIP)
  static  Static routes

2610_pruebas(config)#router eigrp ?
  <1-65535>  Autonomous system number

2610_pruebas(config)#router eigrp 100 ?
  <cr>
```

```
2610_pruebas(config)#router eigrp 100
IP routing not enabled
2610_pruebas(config)#net
2610_pruebas(config)#netbios ne?
netbios

2610_pruebas(config)#neipr routin
2610_pruebas(config)#ip routing
2610_pruebas(config)#
2610_pruebas(config)#ip routing router eigrp 100
2610_pruebas(config-router)#?
Router configuration commands:
 auto-summary       Enable automatic network number summarization
 default            Set a command to its defaults
 default-information  Control distribution of default information
 default-metric     Set metric of redistributed routes
 distance           Define an administrative distance
 distribute-list    Filter networks in routing updates
 eigrp              EIGRP specific commands
 exit               Exit from routing protocol configuration mode
 help               Description of the interactive help system
 maximum-paths      Forward packets over multiple paths
 metric             Modify IGRP routing metrics and parameters
 neighbor           Specify a neighbor router
 network            Enable routing on an IP network
 no                 Negate a command or set its defaults
 offset-list        Add or subtract offset from IGRP or RIP metrics
 passive-interface  Suppress routing updates on an interface
 redistribute       Redistribute information from another routing protocol
 timers             Adjust routing timers
 traffic-share      How to compute traffic share over alternate paths
 variance           Control load balancing variance

2610_pruebas(config-router)#□□□net
2610_pruebas(config-router)#network ?
 A.B.C.D  Network number

2610_pruebas(config-router)#network 172.16.0.0 ?
 A.B.C.D  EIGRP wild card bits
 <cr>

2610_pruebas(config-router)#network  172.16.0.0 □  □□  □□  □□  □□  □.11.0
255.25.2□ □□ □5.255.0□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□
□□ □□ □□ □□ □0.0 ?
 A.B.C.D  EIGRP wild card bits
 <cr>
00:33:15: %SYS-5-CONFIG_I: Configured from console by console
```

Con esta configuración básica funcionará el equipo, que en conjunto con el PBX, nos mandará las llamadas a las tablas deseadas. De esta manera se configurarán las

direcciones IP que serán los puntos importantes en nuestra red, además de los dial peers para que el equipo sepa que acción tomar cuando reciba determinada marcación.

5.6. Estrategia de seguridad

La estrategia de seguridad está compuesta por dos aspectos: por un lado, la configuración que se cargará a las barreras de seguridad (Firewalls), que traducirá las direcciones de la red corporativa para su acceso a la Internet, al igual que las traducciones de entrada para dar servicios de Web, FTP y DNS dentro de la sección denominada como "publ". Por otro lado, la configuración de los accesos por marcación, que van desde la configuración necesaria en los modems remotos de las sucursales sin enlace dedicado, hasta la implantación necesaria en el router que recibirá las peticiones de un servidor de acceso de un proveedor de Internet (ISP).

5.6.1. Configuración de Firewalls

La parte correspondiente a los firewalls constará de los apartados que se encargarán de la traducción dinámica de direcciones de red, que viajan hacia la internet por medio de una emulación de una dirección homologada, tomando un puerto diferente para cada petición, esto es válido para las conexiones de salida; mientras que para las conexiones entrantes, los mapeos se hacen de forma estática para que las direcciones privadas que mantiene la conectividad local siempre sean observadas desde la Internet, con las mismas direcciones homologadas, que serán provistas por el proveedor de dicho servicio. La figura 5.32 muestra el esquema con el que se colocarán los servicios de Web, transferencia de archivos y resolución de direcciones.

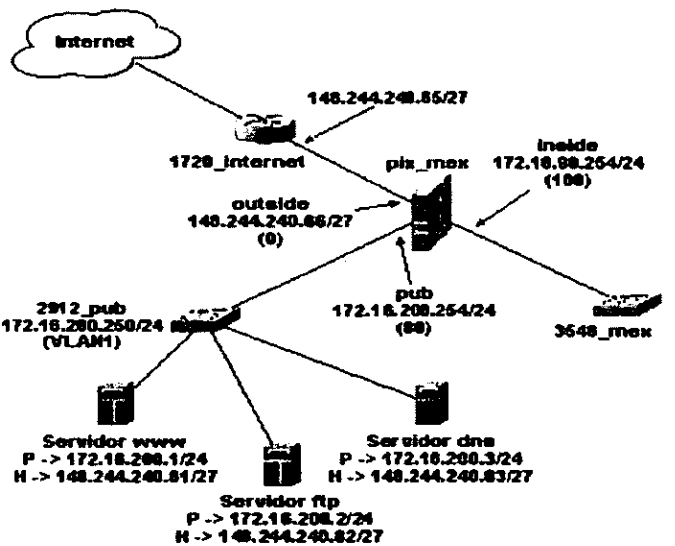


Figura 5.32. Implantación de servidores públicos en WideCOM.

De la figura podemos observar que los servidores aportan servicios de red muy específicos, por lo que la configuración dentro del Firewall es relativamente directa y sencilla, tal y como se muestra a continuación, que despliega la configuración parcial de este equipo que se encarga de mapear y proveer los servicios de cada servidor por dirección homologada.

```
Pix_mex# wr term
Building configuration...
: Saved
:
PIX Version 5.1(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security80
nameif ethernet2 pub security15
nameif ethernet3 stateful security20
enable password c7ElluQ7oBqyTNrT encrypted
passwd do0Af3zKM5NNK7qi encrypted
hostname pix_mex
!
!Esta sección establece las políticas de seguridad que se definieron
!en la parte de diseño y que solo permiten el flujo hacia los puertos
!ahí especificados; estos son: www -> WEB, domain -> DNS y ftp -> FTP
access-list acl_out permit tcp any host 148.244.240.81 eq www
access-list acl_out permit udp any host 148.244.240.83 eq domain
access-list acl_out permit tcp any host 148.244.240.82 eq ftp
ip address outside 148.244.184.66 255.255.255.224
ip address inside 172.16.90.254 255.255.255.0
ip address pub 172.16.200.254 255.255.255.0
ip address stateful 192.168.254.1 255.255.255.0
global (outside) 1 148.244.240.41
nat (inside) 1 172.16.90.0 255.255.255.0 0 0
nat (pub) 1 172.16.200.0 255.255.255.0 0 0
!
!Esta sección se encarga de asignar las direcciones estáticas entre
!los perímetros antes definidos. Al mismo tiempo, la máscara de red
!se escoge como 255.255.255.255 para garantizar que la asignación
!desde la Internet sea ùnica y hacia un solo Host interno.
static (pub,outside) 148.244.240.81 172.16.200.1 netmask
      255.255.255.255 0 0
static (pub,outside) 148.244.240.82 172.16.200.2 netmask
      255.255.255.255 0 0
static (pub,outside) 148.244.240.83 172.16.200.3 netmask
      255.255.255.255 0 0
!
!Estas línea enlaza las políticas al puerto de salida
!del Firewall
access-group acl_pub in interface pub
!
!Finalmente, las siguientes líneas establecen la dirección del flujo
!de datos en forma de simples rutas estáticas que dirigen hacia fuera
!o hacia adentro el transporte de paquetes
route outside 0.0.0.0 0.0.0.0 148.244.240.65 1
route inside 172.16.10.0 255.255.255.0 172.16.100.254 1
route inside 172.16.11.0 255.255.255.0 172.16.100.254 1
route inside 172.16.12.0 255.255.255.0 172.16.100.254 1
route inside 172.16.13.0 255.255.255.0 172.16.100.254 1
route inside 172.16.20.0 255.255.255.0 172.16.100.254 1
route inside 172.16.30.0 255.255.255.0 172.16.100.254 1
route inside 172.16.40.0 255.255.255.0 172.16.100.254 1
```

```
route inside 172.16.50.0 255.255.255.0 172.16.100.254 1
route inside 172.16.60.0 255.255.255.0 172.16.100.254 1
route inside 172.16.70.0 255.255.255.0 172.16.100.254 1
route inside 172.16.80.0 255.255.255.0 172.16.100.254 1
```

El resto de la configuración típica de un firewall está orientada a establecer parámetros de monitoreo y presentación de datos que permiten hacer la depuración de fallas más simple y rápida.

Lo último que falta por definir es la configuración que debe poseer tanto el servidor de acceso del ISP como el router que recibirá y terminará los túneles virtuales.

5.6.2. Configuración de Túneles Virtuales

La parte de encripción de datos estará implantada mediante la autentificación de las conexiones desde la Internet con direcciones homologadas determinadas y convenidas entre WideCOM y el *ISP (Internet Service Provider, Proveedor de Servicios de Internet.)*

Esta idea se representa en la figura 5.33 junto con la conexión de los servidores de facturación. Puesto que se decidió que los enlaces virtuales serían a través de redes públicas, sólo las sucursales que carecerán de enlaces dedicados mantendrán una conexión de carácter temporal hacia las oficinas centrales de la Ciudad de México.

Esta conexión virtual se apoyará en la asignación de direcciones IP dentro de un equipo que posee el proveedor de Internet, y que estará configurado para atender las peticiones de llamadas locales que iniciarán los modems remotos. Este mecanismo se representa en la figura 5.34 En ella, la única función del equipo conocido como servidor de acceso, asignará unas direcciones IP especiales siempre y cuando el usuario se valide con el formato: username@mkos.name.

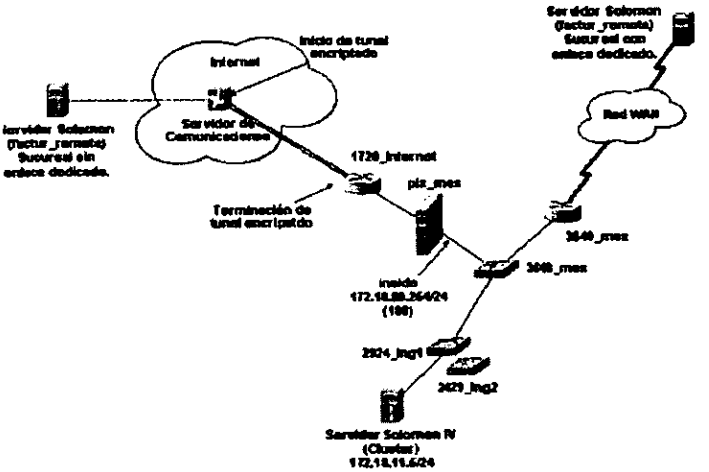


Figura 5.33. Implementación de túneles virtuales .

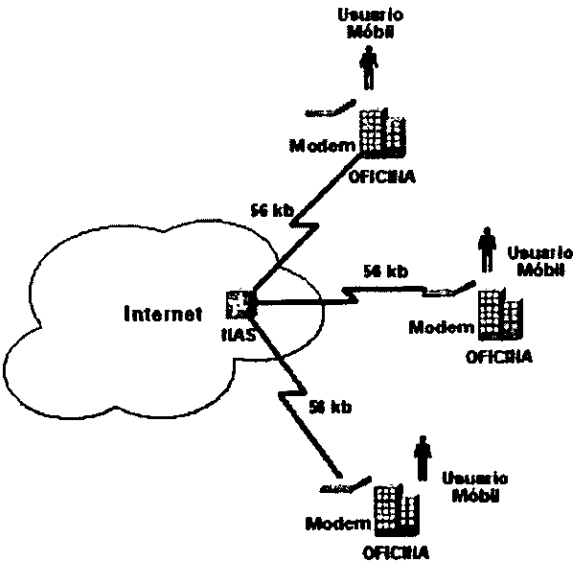


Figura 5.34. Conexión múltiple de usuarios remotos a un servidor de acceso.

A continuación, se muestran fragmentos de la configuración del servidor de acceso que reparte las direcciones y que se encuentra dentro de las instalaciones del proveedor nacional de Internet.

```
Hostname isp-nas
!
aaa new-model
aaa authentication login default enable
aaa authentication login console none
aaa authentication ppp default tacacs+ local
aaa authorization exec default none
aaa accounting exec default start-stop tacacs+
!
enable secret 5 $1$2Ezj$2ygSgy
enable password escape
!
ip domain-name isp1.net
!
!Habilita el servicio de VPNs en el servidor de acceso
vpdn enable
vpdn source-ip 201.1.1.1
!
!El grupo1 (group1) establece la conexión hacia el router de Internet
!ubicado en México, además de definir el uso del protocolo L2TP
!
vpdn-group 1
      request dialin l2tp ip 207.1.1.1 domain mkos.com
      local name isp1
!
crypto isakmp policy 10
      authentication rsa-encr
```

```
      group 2
      lifetime 240
!
!Esta sección define la política de traducción usada por IPsec;
!Además, puesto que se está usando L2TP, se debe correr Ipsec
!en el transporte en lugar de habilitar el tuneleo normal.
crypto ipsec transform-set auth_cisco_dial ah-sha-hmac esp-des esp-
sha-hmac
      mode transport
!
crypto ca identity vpnnetwork
      certificate 44fc6c531fc34446927e4ee307a806b20
!Certificate is múltiple lines of hex digits
quit
      certificate ca 3051df7169beee31b821dfe4b3a338e5f
!Certificate is múltiple lines of hex digits
quit
!
!Crypto map to encryp traffic destined to Denver home gw for mkos.com
!
crypto map VPDN_MKOS local-address Loopback0
      crypto map VPDN_MKOS 1000 ipsec-isakmp
      set peer 207.1.1.1
      set transform-set auth_mkos_dial
      match address VPDN_mkos_tunnel
!
interface Loopback0
      ip address 201.1.1.1 255.255.255.252
      no ip directed-broadcast
      crypto map VPDN_MKOS
!
!Por último, se define la lista de acceso para determinar
!el tráfico que debe aplicarse a IPsec, con el nombre VPDN_mkos_tunel
ip access-list extended VPDN_mkos_tunel
      permit ip host 201.1.1.1 host 207.1.1.1
!
```

Esta configuración, aunque está fragmentada, muestra la forma en que se abre el túnel y se encripta con la combinación de L2TP y IPsec, la cual es una forma típica de implementar seguridad en tráfico público. Sin embargo, una de las notas importantes que se verificarán en el capítulo siguiente, es la alta sensibilidad al retraso que sufren estas conexiones, puesto que el protocolo de seguridad está pensado para evitar intrusiones en el tránsito y cuando existen retrasos en la respuesta a las peticiones de conexión, el algoritmo termina la sesión y el intercambio de llaves deben iniciarse de nuevo desde el principio.

Con esto hemos configurado los equipos que intervendrán en nuestra red seguiremos, con las pruebas a los mismos.

CAPÍTULO 6

Análisis del desempeño de la red

El análisis de desempeño de la red de voz y datos se basa en mediciones que se realizaron en la misma red, tomando como base solo dos nodos: las oficinas centrales en México y el punto remoto de Querétaro. La selección de este enlace se basa en la incidencia de comunicaciones con esta plaza, además del intercambio continuo de datos y archivos. Este enlace permite usar ambas puntos remotos como entidades aisladas y extender las pruebas a cualquier nodo de la red de WideCOMM, con la consideración de los canales tanto de voz como de datos que aplica a cada caso.

El desempeño de los equipos se evaluará al seleccionar un conjunto de parámetros que permiten diferenciar el comportamiento de la red bajo ciertas circunstancias de uso. Tales parámetros serán descritos en tres secciones que sentarán las bases del análisis, al igual que se presentarán resultados de las pruebas realizadas y que de alguna forma corroborarán el desempeño de la red.

6.1. Red de estudio

La red de WideCOMM consta de un nodo central y varios nodos remotos en una topología de estrella, lo que permite la compartición de recursos y de mensajes, por medio de enlaces dedicados que poseen diferentes anchos de banda para cada sucursal remota, en función de las necesidades proyectadas en cada una de las mismas. A través de la red es posible la transferencia de datos, intercambio de correos electrónicos, acceso a Internet y otras aplicaciones como la facturación electrónica.

El ancho de banda está determinado por la necesidad de transferir grandes cantidades de información sin que se presenten retrasos considerables, estas transferencias son esporádicas, por lo que el requerimiento completo del ancho de banda no es constante.

De cualquier forma, la implantación de la red de voz no representa un problema para el envío de datos; ya que, por lo general, los paquetes de voz son pequeños y se colocan fácilmente dentro de los datos serializados sin que los procesos de facturación se vean afectados. De hecho, la intención de este estudio es probar la factibilidad del envío de voz sobre la red de datos usando el protocolo de Internet VoIP.

El siguiente escenario muestra la red de estudio que se tomó para realizar las pruebas (México-Querétaro). Este segmento transporta hasta 4 canales de voz simultáneos, además del tráfico de datos de uso diario, todo sobre un enlace dedicado de 128 kb. El análisis hacia los demás nodos comienza de la escalación que se tomó como base para sustentar el número de canales de voz en cada enlace, de forma que el análisis para cuatro canales de voz podrá extenderse hacia los demás nodos en la proporción adecuada. El esquema de la figura 6.1, muestra este escenario para el análisis que se llevó a cabo, se observa el enlace a 128 kb que une a los routers de México y Querétaro, mostrándose también la interfaz de comunicaciones de cada uno. No obstante que en este esquema sólo se representan dos nodos, la justificación de su elección radica en un análisis de la ocupación del medio y en donde, después de una clasificación de sucursales, México y Querétaro resultaron con el tráfico de datos más alto (archivos, correo e Internet).

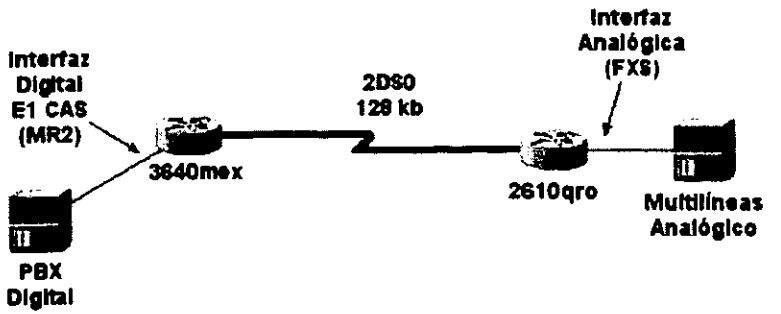


Figura 6.1. Red de estudio para el análisis de desempeño.

6.2. Metodología

Para hacer el análisis de desempeño de redes y/o aplicaciones, independiente de su tipo, hay tres aproximaciones básicas, que son: modelado teórico, mediciones y simulaciones; la elección de una u otra depende en buena medida de los recursos disponibles, las restricciones operativas y el estado de la red o aplicación en estudio. Para este estudio se tuvieron en cuenta las mediciones, que serán enunciadas en su respectivo momento.

6.2.1. Ocupación del canal debido al tráfico de datos

Para determinar la ocupación del enlace WAN se tomaron mediciones en 5 oficinas de diferentes tamaños (basados en la cantidad de transacciones promedio realizadas en un día), en el lapso de una semana, de las 07:00 a las 17:00, usando un software de gestión de redes. Las mediciones se realizaron con intervalos de 5 segundos, ya que en los ensayos de prueba y error fue el mejor compromiso encontrado entre cantidad de datos *versus* tráfico SNMP (*Simple Network Management Protocol, Protocolo de Manejo de Red Simple)* , que introduce una tasa de bit no deseada que puede alterar la medición. Las oficinas se seleccionaron de tal manera que fuesen representativas dentro del universo muestral, buscando tener al menos dos por tipo (A,B,C), según el número de transacciones diarias realizadas en promedio. La clasificación de estas se presentan en la tabla 6.1 .

Tipo A	Tipo B	Tipo C
México	Guadalajara	San Juan de Río
Querétaro	Monterrey	León
		Gómez Palacio

Tabla 6.1. Clasificación de Oficinas por número de transacciones.

En la tabla 6.2 se presentan las mediciones de ocupación del canal en las oficinas objeto del estudio en forma de percentiles

0%	1.016	1.176	1.36	1	992
5%	1.584	1.776	2.256	1.72	1.068
10%	1.672	1.904	2.408	1.872	1.712
15%	1.744	2.016	2.552	2.024	1.824
20%	1.824	2.136	2.688	2.184	1.936
25%	1.904	2.272	2.832	2.384	2.072
30%	2	2.432	3.008	2.64	2.248
35%	2.128	2.624	3.216	2.952	2.48
40%	2.288	2.896	3.52	3.344	2.832

Tabla 6.2. Ocupación del enlace WAN (64kbps) en porcentaje (Continúa tabla)

45%	2.536	3.248	3.856	3.678	3.24
50%	2.976	3.696	4.28	4.4	3.688
55%	3.456	4.312	4.952	5.432	4.8
60%	4.504	5.56	6.528	7.224	8.136
65%	7.608	7.92	8.536	8.952	8.992
70%	8.92	9.176	9.368	9.328	90288
75%	9.112	9.512	9.832	9.8	9.768
80%	9.376	10.032	10.28	10.552	10.792
85%	9.92	10.869	11.072	11.656	14.136
90%	11.112	12.448	12.976	14.824	26.96
95%	16.32	16.808	18.24	20.096	34.536
100%	mayor	mayor	Mayor	Mayor	Mayor

Tabla 6.2. Ocupación del enlace WAN (64kbps) en porcentaje.

De la tabla 6.2 se puede observar que todas las oficinas medidas tienen un comportamiento similar en términos de la función de distribución de probabilidad FDP de la tasa 1. Es importante resaltar que las mediciones se hicieron en oficinas de Ciudad de México, por ser la de mayor número de transacciones promedio, para tener holgura en los resultados obtenidos de tasa de bit, y esta función sólo presenta pequeñas diferencias según el tipo de oficina. Un fenómeno interesante que vale la pena resaltar es la naturaleza bimodal generalizada de la función de densidad de probabilidad de tasa de bit en los enlaces WAN de todas las oficinas, independiente de la hora del día, esta independencia significa que no importa demasiado el rango de horas en la que se realicen las mediciones de tasa de bit, ni la duración de la misma, ya que los resultados siempre son similares.

Además se puede concluir que la utilización de los enlaces es baja, con lo que no parece fuera de lugar el pensar en cursar voz a través de estos. Además, es posible concluir que los fenómenos de más baja ocupación del enlace son más probables que cualquier otro, y que los picos de probabilidad de ocupación están similarmente espaciados (máximo modo 1 entre 1518 y 3036 bps con probabilidad entre 0.25 y 0.35 y máximo modo 2 entre 9108 y 10626 bps con probabilidad entre 0.04 y 0.08).

6.2.2. Ocupación del canal debido a la voz

Para determinar la ocupación del canal de 64 kbps de una oficina típica por una llamada de voz usando los diferentes CODEC's implementados, se siguió una metodología que varia con respecto a la de las transacciones, debido a dos puntos:

- La corta duración de las llamadas de voz con respecto a un día de operación normal de una oficina.

- La necesidad de determinar los puertos TCP para dar prioridades en los enrutadores a este tipo de tráfico

Por estos dos puntos se tomó la decisión de usar un analizador de protocolos para hacer la captura de todos los paquetes de voz, y filtrarlos (ya que solo interesan los paquetes de voz) y así determinar la tasa de bit de la aplicación usando una macro de MS Excel. Para las pruebas se utilizó una conversación estándar de 5 minutos de duración, con los mismos interlocutores y en el ambiente controlado que se aprecia en la figura 6.2. se interrumpió el enlace WAN para colocar el analizador de protocolos.

Figura 6.2. Ambiente de prueba de Cisco.

Los CODEC's probados se listan en la tabla 6.3.

Solución	CODEC's Medidos
CISCO	G..723 5.3 kbps
	G.723 6.3 kbps
	G.729
	G.726 16 kbps
	G726 24 kbps
	G711 a-law
Ericsson	GSM
Nortel Networks	G.729[a]

Tabla 6.3. CODEC's probados.

En la figura 6.3 se presenta el histograma de frecuencias de utilización de tasa de bit para los CODEC's que mayor compresión realizan a la voz; éstos interesan especialmente ya que su promedio de tasa de bit es apreciablemente menor a los otros 5 CODEC's probados. (G.729-a = 32.072 kbps, GSM = 43..746 kbps, G.711=96.079 kbps, G.726-24 = 40.765 kbps, G.726-16=26.329 kbps, *G.729 – 14.964* kbps, *G.723-6.3 =11.969* kbps *y G.723-5.3 - 10.275* kbps), haciéndolos más atractivos de implementar; por lo menos en cuanto a consumo de recursos faltando todavía la valoración subjetiva de las pruebas de calidad de voz entregada.

En la figura 6.3 se puede observar claramente que la dispersión de tasa de bit en el enlace de prueba es muy pequeña, y que ésta se concentra en los tres casos por debajo de los 21,000 bps, con lo que es posible pensar que cualquiera de estas llamadas de voz puede ser cursada en uno de los enlaces actuales.

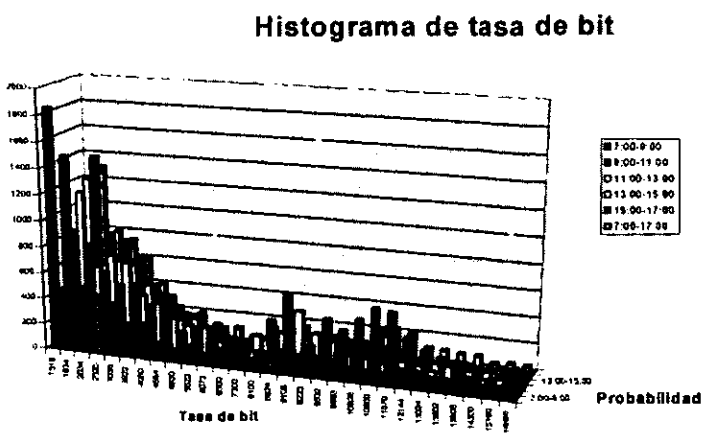


Figura 6.3. Histograma de tasa de bit de los CODEC's G.729, G.723 6.3 y G.723 5.3

6.2.3. Tasa de bits conjunta (voz + datos)

A simple vista es posible creer que con la ocupación media obtenida de las mediciones de tasa de bit, tanto de oficinas como de llamadas telefónicas (CODEC's G.723 5.3, G.723 6.3 y G.729), es posible cursar voz, pero todavía no existe una completa certeza. Por esta razón, con los datos medidos de voz y tomando a la oficina de México como tipo, se realizó una superposición de variables aleatorias, para tener una primera aproximación de lo que sería la tasa de bit de voz y datos en un enlace; los resultados se presentan en la tabla 6.4.

Perc	Mex G.723 R24	Mex G.726 R16	Mex G.729	Mex G723 6.3	Mex G726 5.3
0%	11,463	13,135	14,783	10,583	10,519
5%	39,951	24,023	19,015	16,487	16,127
10%	36,007	27,271	20,423	17,719	16,759
15%	36,535	28,007	21,239	18,247	17,111
20%	37,095	28,743	21,783	18,743	17,591
25%	37,847	29,319	22,375	19,127	17,991
30%	41,847	30,263	22,935	19,647	18,931
35%	44,631	32,823	23,351	20,071	18,599
40%	47,127	33,927	23,903	20,599	19,319
45%	51,847	35,367	24,527	21,239	19,463
50%	54,551	36,559	24,887	21,735	19,895

Tabla 6.4. Suma histogramas tasa de bit de datos + VoIP para la oficina de México (Continúa tabla).

55%	55,799	38,151	25,319	22,119	20,295
60%	56,919	38,919	25,623	22,631	20,583
65%	58,743	40,183	25,991	23,271	21,079
70%	59,447	40,951	26,423	23,671	21,399
75%	60,295	41,862	26,775	23,927	21,719
80%	61,111	42,759	26,167	24,279	22,135
85%	61,895	44,103	27,605	24,679	22,615
90%	62,439	45,643	28,447	25,127	23,127
95%	63,527	46,651	29,207	25,895	23,751
100%	67,134	49,463	30,655	27,479	27,175

Tabla 6.4. Suma histogramas tasa de bit de datos + VoIP para la oficina de México

De los resultados de la tabla 6.4 se confirma la posibilidad de cursar una llamada por los enlaces WAN de las oficinas sucursales, pero llama la atención que con una sola llamada de voz, la utilización del canal sea tan alta; ya que se planea instalar dos teléfonos por oficina, además se debe tener en cuenta que este método es meramente indicativo y que no tiene en cuenta aspectos como el retardo y el tamaño de los buffers. También es importante resaltar que esta superposición no presenta toda la información necesaria para determinar la utilización de un enlace con más de dos oficinas y mucho menos para ciudades como Toluca y Gómez Palacio, cuyo enlace de acceso a México es de 64 kbps. Es en este punto en donde las mediciones de tasa de bit dejan de ser útiles, para dar paso a la simulación, en donde los fenómenos de retardo, utilización efectiva del canal y tamaño de los buffers pueden ser estudiados con detalle.

6.3. Pruebas Subjetivas de calidad de voz

Ya que una mínima utilización de la tasa de bit disponible en los enlaces WAN para una aplicación de telefonía sobre IP no garantiza que una llamada de voz tenga una calidad satisfactoria, paralelamente a las pruebas objetivas, se han llevado a cabo pruebas subjetivas que miden la calidad de voz de sistemas telefónicos, independientemente de su naturaleza.

La ITU-T ha desarrollado las recomendaciones P.800 y P.50 cuyo tema son pruebas subjetivas para medir la calidad de voz de sistemas telefónicos, estas recomendaciones se tomarán en cuenta para este estudio. Dentro de estas pruebas subjetivas se han escogido tres, las cuales son: conversación, esfuerzo de escucha y detectabilidad de respuesta cuantificada.

Conversación

En esta prueba se escogen varios grupos de parejas y se hace que la conversación sea calificada por cada una, con lo cual se podrán realizar las pruebas estadísticas.

Esfuerzo de Escucha

Esta prueba busca establecer el esfuerzo necesario para que el significado de las frases sea comprendido por las mismas personas antes seleccionadas.

Detectabilidad de Respuesta Cuantificada

En ocasiones es necesario investigar el ruido, desvanecimiento y otras perturbaciones mediante la respuesta de los participantes de la prueba.

Ya que en la prueba las mediciones se realizan en dos escenarios: el primero de ellos con la red en las mejores condiciones de retardo y pérdida de paquetes, el segundo con una red congestionada; se congestionó el ambiente controlado utilizando una transferencia de archivos a través FTP, protocolo reconocido por su amplia capacidad de utilización recursos.

Para efectos prácticos, los resultados de los CODEC´s G.723 5.3, G.723 6.3 y G.729 fueron agrupados bajo el titulo Cisco 1 y los CODEC´s G.726 16, G.726 24 y G.711.7 bajo el título Cisco 2. Los resultados se aprecian en la tabla 6.5.

En la tabla 6.5 se observa el fuerte impacto que tiene la congestión del enlace en todas las implementaciones de VoIP, independientemente del proveedor utilizado; y aunque se aprecian pequeñas diferencias en la calidad de voz percibida, ya que podemos notar que el equipo con la mejor calidad de voz es Cisco con los CODEC´s del grupo Cisco 1, es evidente que los protocolos de reserva de recursos todavía no proveen una buena calidad de voz en condiciones de alto tráfico.

	Conversación		Esfuerzo escucha		Ruta Cuantificada	
	Limpia	Congestionada	Limpia	Congestionada	Limpia	Congestionada
CISCO 1	4	3.4	3.7	3.4	4.6	2.8
CISCO2	3.8	3.3	3.6	3.3	4.5	2.6
ERICSSON	3.7	3.3	3.7	3.3	4.5	2.5
NORTEL	3.7	3.4	3.6	3.2	4.6	2.4
PBX	4		4		4	

Tabla 6.5. Pruebas subjetivas.

En las pruebas subjetivas se tuvo un especial cuidado en 3 factores básicos:

- Tamaño promedio del buffer
- Utilización promedio del canal/Retardo promedio

Basándonos en estos factores presentamos los resultados obtenidos, figuras 6.4, 6.5, 6.7 y 6.7. Las figuras 6.6 y 6.7 presenta el crecimiento pronunciado de los buffers en el caso de 4 y 5 sucursales respectivamente, cuando se realizan entre 0 y 4 llamadas.

En las figuras 6.4 y 6.5 se observa la gran diferencia que existe en ambos escenarios ya que para 4 llamadas telefónicas, el aumento del tamaño del buffer es muy importante: crece en proporciones de 1024%, 4617% y 4610% para los CODEC's G.723-5.3, G723-6.3 y G.729, respectivamente.

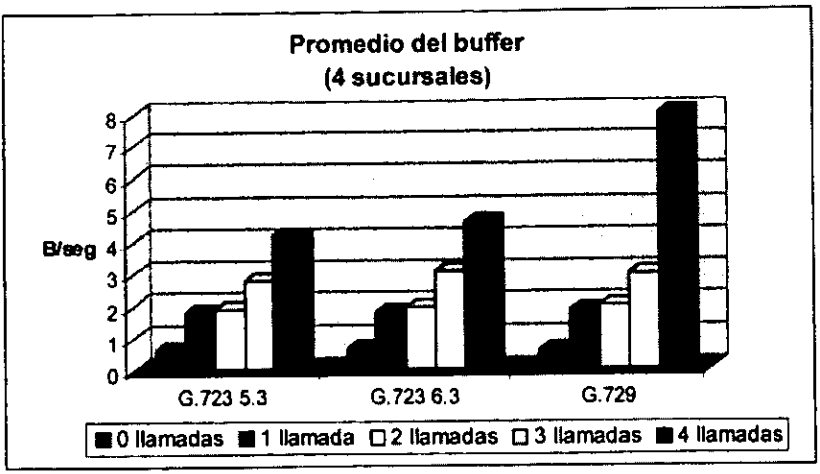


Figura 6.4. Tamaño promedio del buffer del enrutador concentrador de Querétaro.

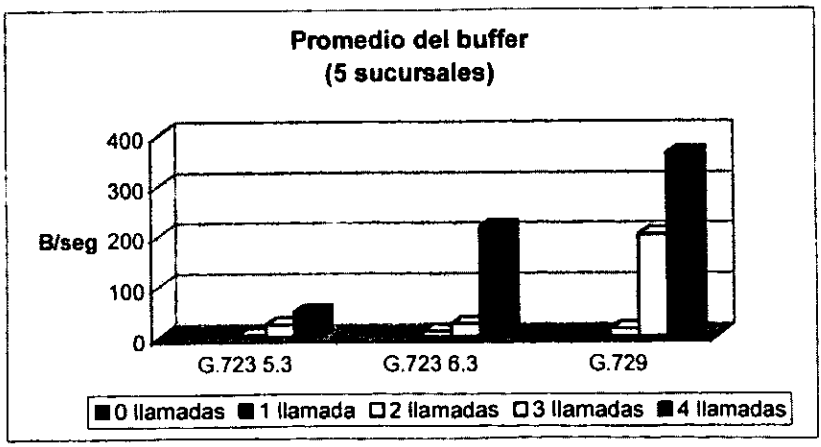


Figura 6.5. Tamaño promedio del buffer del enrutador concentrador de México.

En la figura 6.6 se observa la utilización promedio del enlace WAN de la ciudad de México, esta figura presenta el aumento escalonado de la utilización del enlace, y su misión es determinar el "peso" de una llamada de voz en términos de tasa de bit, este peso en promedio es de cerca de 8 kbps, y empieza a disminuir a medida que se acerca al nivel de saturación del enlace.

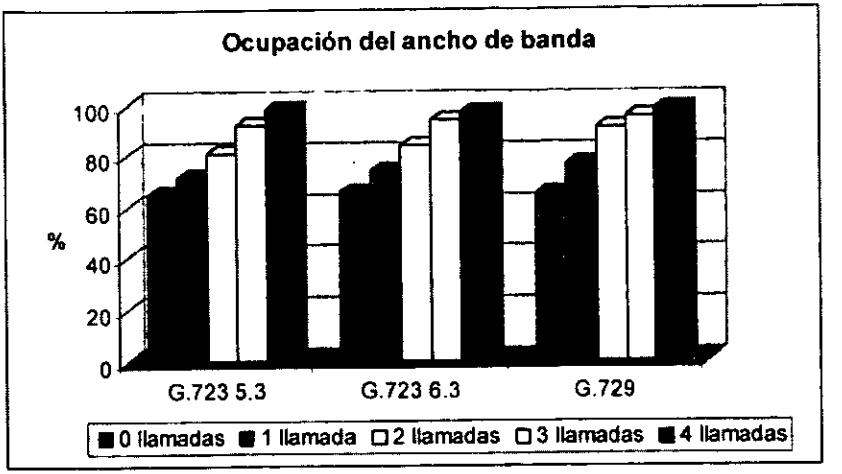


Figura 6.6. Utilización promedio del canal de 64kbps En México.

En la figura 6.7 mostramos un resultado que es preocupante, es el de retardo promedio en el enlace, y su desmedido aumento al pasar de tres llamadas a cuatro, aumentado porcentualmente en 612%, 1331% y 1375% para los CODEC's G.723-5.3, G.723-6.3 y G.729 respectivamente.

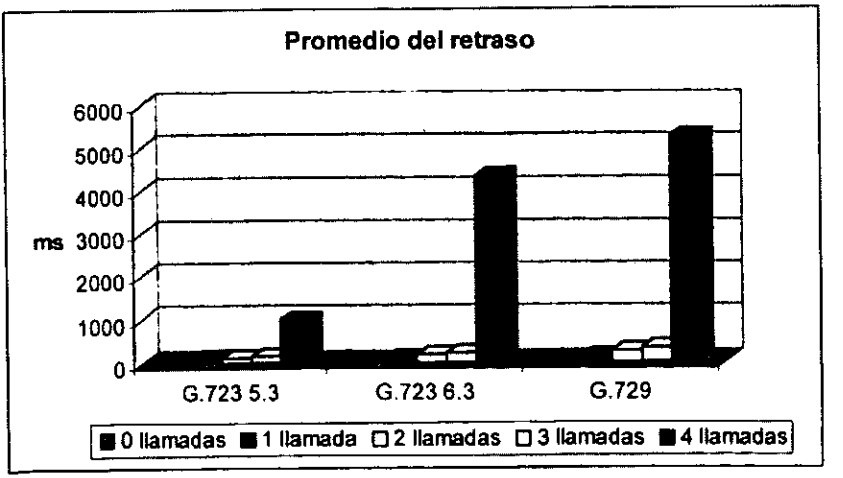


Figura 6.7. Retardo promedio del canal de 64 kbps en México

Este resultado evidencia el problema más grande de VoIP, y es que un canal sigue admitiendo llamadas independiente de las condiciones de congestión del mismo, desmejorando las condiciones de servicio para las llamadas ya establecidas.

6.4. Conclusiones

Un resultado significativo obtenido a partir de este estudio es que no existen mecanismos de bloqueo de llamadas en VoIP, tal como existen en la telefonía convencional. Estos mecanismos probaron ser útiles cuando en las simulaciones, una sola llamada adicional deterioró por completo la calidad de la conexión representada en tamaño del buffer y retardo promedio. El que este mecanismo no esté presente significa que el desempeño de un enlace y de la red completa se ve comprometido cada vez que alguien levanta un teléfono.

Este mecanismo de bloqueo de llamadas debería estar asociado a variables que no impliquen envío de paquetes a través del enlace como por ejemplo el tamaño del buffer. A través de las pruebas subjetivas se demostró que los protocolos de reserva de recursos, todavía están en sus etapas iniciales, ya que si bien la calidad de voz que se evidenció cuando las condiciones de la red eran las mejores (tráfico moderado), eran comparables a una PBX normal. Cuando estas condiciones cambiaron (alto tráfico) la calidad percibida por el jurado de todos los sistemas telefónicos probados se decremento sustancialmente.

También es evidente que no existen grandes diferencias en cuento a calidad de voz en uno y otro proveedor, en cambio lo que si los diferencia son los dispositivos utilizados para empaquetar voz en datagramas IP, ya que cada uno utiliza su fortaleza para hacerlo (Nortel en sus plantas telefónicas, Cisco con sus enrutadores y Ericsson diseñó un equipo especialmente para esa labor, que en últimas es la tendencia para grandes compañías telefónicas).

El que todavía no exista una tendencia por parte de los proveedores acerca del tipo de equipos que se utilizarán en este tipo de soluciones, hace que, en el afán de salir al mercado, muchas de las soluciones adolezcan de facilidades que en los sistemas telefónicos convencionales se han implementado hace ya bastante tiempo (llamadas en espera, conferencia, tarificación, etc.). Y que además presenten implementaciones complicadas y que funcionalmente tengan deficiencias.

Un aspecto que llamó mucho la atención es el gran tamaño que puede llegar a tener el encabezado IP con respecto al tamaño total del paquete IP. Recordemos que con los CODEC's G.729, y G.723 5.3 el tamaño de los paquetes es de 26 bytes y que además el tamaño mínimo de un encabezado IP es de 20 bytes, lo que deja solo 6 bytes de carga útil. Esta diferencia es de 3.33 : 1 lo que resulta absurdo. Valdría la pena consultar con los proveedores si existen planes de comprimir el encabezado IP para que esta diferencia sea menos notoria; claro que cualquier esfuerzo en esta dirección estaría directamente relacionado con un aumento en la capacidad de procesamiento.

El que los tiempos de llegadas entre paquetes hayan podido ajustarse bien a una FDP exponencial, y que además resulten no correlacionados, no es un resultado ni mucho

menos inesperado, lo que si de alguna manera es nuevo es que los tiempos entre llegadas de CODEC's con tasas de bit tan disímiles como G.711 y G.729, guarden semejanzas tan cercanas y que lo único que los diferencie claramente en cuanto a tráfico inyectado en la red sea el tamaño de los paquetes (166 y 26 bytes respectivamente).

Hemos aprendido con estas pruebas a valorar las bondades y entender los problema generados por estas nuevas tecnologías, a continuación se presentan las conclusiones del proyecto.

CAPÍTULO 7

Resultados y conclusiones

En este capítulo presentamos los logros más relevantes de la red corporativa de multiservicios. La presentación de los resultados estará sustentada en la operación propia de la red.

7.1. Facturación electrónica

Partiendo de la idea inicial de proveer los servicios de facturación en línea para la totalidad de las sucursales que componen el consorcio de WideCOM, el análisis de los tiempos de respuesta para tráfico de tasa conjunta (voz y datos) no se vieron degradados por la presencia del tráfico sensible al retraso, lo que representó un manejo especial del mismo, incluso no impactó en las aplicaciones de datos como son correo electrónico, transferencia de archivos y mensajes de control *SNMP* propios del monitoreo.

En términos generales, podemos afirmar que la estimación de los anchos de banda para cada sucursal proyectada fue adecuada, conforme los requerimientos demandaron servicios de datos y de voz en las oficinas. De manera similar, el uso de un protocolo de ruteo híbrido, tal y como lo es EIGRP, ofrece ventajas que ahorran parte del canal al difundir las tablas de ruteo de toda la red mediante mensajes Multicast, en vez de mensajes Broadcast, los cuales llegan a todos los equipos dentro del mismo dominio sin que procesen la información.

A nivel local, las redes de todas las sucursales se integraron dentro de una jerarquía estructurada, que les permitió tener una gestión más compacta y sencilla, asignando las direcciones de red en una base secuencial que identifica cada región (nodo) de forma única. Cabe mencionar que la segmentación en las oficinas centrales en México mejoró notablemente el tráfico local, puesto que los datos de facturación (incluyendo los datos foráneos), que son los datos más pesados, viajan de forma independiente de los demás segmentos configurados en México, sin consumir recursos de anchos de banda y procesamiento en los equipos de comunicaciones.

El equipo Cisco seleccionado cumplió con las expectativas de desempeño que de el se esperaban, tal y como lo demuestran las gráficas del capítulo 6 (uso de buffers, encolamientos, etc.), en donde la capacidad de procesamiento de los equipos empleados no se degradó de forma significativa, incluso con los procesos que demandaron las tarjetas de voz (analógicas y digitales.)

El último aspecto a cubrir, en los resultados referentes a la red de datos está relacionado con la elección que se hizo a favor de los enlaces dedicados sobre Frame Relay y ATM. En la práctica se descubrió que los enlaces dedicados, aunque representaron un gasto mayor (tanto en instalación como en renta), presentaron una mayor flexibilidad en la configuración, al igual que en la variedad de encapsulados WAN que pueden soportar.

7.2. Servicios de voz por red interna

El punto más atractivo de los multiservicios es sin duda la implementación de la voz; por todos los retos que presenta en el sentido de ser el único tipo de tráfico que sería sensible a sufrir retraso y que, por lo mismo, es la representación más tangible del estado de la red. La implantación de esta red permitió incrementar los ahorros obtenidos, al reemplazar en más de un 80% la cantidad de llamadas por larga distancia a alguno de los nodos pertenecientes a la red.
Por la naturaleza de la topología de la red, todas las llamadas provenientes de los sitios remotos, pero con destino diferente a la Ciudad de México, deben pasar por el sitio central (México), lo que permitirá a futuro colocar un tarificador de llamadas en un solo

sitio y obtener estadísticas más detalladas con respecto al volumen de llamadas, distribución de las mismas, etc.

Algunos otros servicios, que derivaron de la red de voz, permiten aprovechar las características digitales que poseen los equipos multilíneas típicos de las sucursales, tales como DISA, conferencia, transferencia, etc.

Como resultado de las gráficas del capítulo 6 se observó que un canal típico de enlace WAN (64 kbps) no es suficiente para soportar 4 llamadas de voz de forma simultánea, sin que ésta afecte la calidad de servicio entregada. Sin embargo, a últimas fechas se han desarrollado mecanismos que permiten prever si existirán recursos suficientes (ancho de banda, buffers, etc) antes de iniciar una llamada. Estos mecanismos se conocen con el nombre de *VAD(Voice Absence Deleting, Borrado en Ausencia de Voz).*

7.3. Servicios de seguridad

El aspecto que concierne a la seguridad de redes merece un tratamiento especial, por el tipo subjetivo de evaluación a que está sujeto. Para analizar los resultados, los servicios de seguridad estuvieron ubicados en tres nichos principales: creación de túneles virtuales, acceso a la Internet y servicios de web.

La parte más importante, la creación de túneles, observó retrasos en el intercambio de las llaves de encripción (tal y como se observa en el histograma de ocupación del canal de datos), no obstante que el tráfico de los datos útiles de facturación en los enlaces dedicados fueron encriptados de forma más ligera a su llegada al router central en la Ciudad de México. De hecho, se pudo observar que el uso de un enlace conmutado presentó más retrasos por la naturaleza saturada y de baja calidad en las líneas de cobre que son características de la PSTN. En este sentido, una forma común de probar la seguridad de una red es por medio de barridos de direcciones IP con la intención de probar, primero la existencia de un host en particular, y después determinar los servicios que están corriendo en dicho host esto es, el número de puertos en capa 4 que se encuentran activos en el momento de la prueba.

En general, los equipos que realizan este tipo de barridos operan de forma similar, por un lado; por otro, la práctica común ha consistido en emplear dispositivos pertenecientes al mismo proveedor de la solución de seguridad, lo que plantea cierta subjetividad acerca del resultado obtenido el cual consta de una lista de: vulnerabilidades potenciales, vulnerabilidades confirmadas y vulnerabilidades reparadas (estas últimas como resultado de un segundo barrido.)

Debido a la subjetividad mencionada, el punto a resaltar estriba en el proceso de encriptación con el que viajan los datos en cualquier tipo de enlace, además de la autenticación entre el que recibe y el que envía la información que anteceden al proceso de encripción. Cabe mencionar que en el caso remoto de una intrusión en el medio de transmisión dedicado, lo que observaría un tercero sería tráfico cifrado e ininteligible, que usualmente frustra al intruso; lo que nos da una idea más clara de la ventaja que aportan los protocolos IPsec y L2TP.

Los servicios de la Internet se controlaron de forma centralizada mediante la implementación de un PIX Firewall; ya que todos los accesos hacia la red de redes deben autorizarse y filtrarse a través de este dispositivo, haciendo un uso más eficiente del ancho de banda hacia la Internet, y garantizando de esta manera el acceso de los túneles virtuales de que hacen uso las sucursales que carecen de enlace dedicado. Asi mismo, la implementación del sitio web de WideCOM dentro de uno de los perímetros creados por el PIX goza de una seguridad robusta por los mecanismos de protección que están diseñados específicamente para proteger de ataques y formas de intrusión no autorizadas.

7.4. Conclusiones generales

Este proyecto es exitoso e incrementa la productividad del personal y de la empresa en general, que reduce considerablemente gastos por envío de valijas, llamadas de larga distancia, transporte, viáticos, y demás gastos en que se incurría al atender las diferentes plazas de WideCOMM.

Debemos decir que este proyecto cumple con su propósito, porque incrementó la cultura y el conocimiento de nosotros como estudiantes y futuros ingenieros de la Universidad Nacional Autónoma de México y su Facultad de Ingeniería, fomentando de esta manera el uso extensivo de los conocimientos adquiridos en las diferentes asignaturas cursadas en las aulas, además con esto crea en nosotros nuevas expectativas de desarrollo para desempeñarnos como ingenieros y profesionales al servicio de las empresas nacionales.

En este tiempo en el mercado aparecen nuevas herramientas, productos para apoyar cada una de las etapas de la ingeniería electrónica y comunicaciones, por lo que el uso adecuado de estas modificará el desarrollo de los sistemas de comunicación y logrará mejorar la calidad de los servicios, lo que nos impulsa a seguir adquiriendo conocimiento y alcanzar un nivel superior día con día.

Digno de mencionarse es el grado de conocimiento adquirido y conjuntado en el seminario; así como las herramientas y la metodología aprendida y aplicada en esta tesis, que será elemento básico y fundamental para poder enfrentarnos al mundo del trabajo profesional.

APENDICE A

Configuración de equipos

A continuación se describe la configuración de los equipos de comunicaciones para el proyecto de tesis propuesto.

```
! ******************************************************************
! 3640isp.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.5 Build 8
!   Lunes, 10 de Septiembre de 2001, 09:22:47 p.m.
!
! Hostname: 3640isp
! Model: 3640
! ******************************************************************
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname 3640isp
!
enable password cisco
username cteCDJ password 7 123456
username cteCHI password 7 123456
username cteMOR password 7 123456
username ctePUE password 7 132456
username cteREY password 7 132456
username cteSLP password 7 123456
username cteVER password 7 123456
username cteVHA password 7 132456
username cteZAC password 7 123456
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
! Internet Key Exchange (IKE)
!
crypto isakmp enable
crypto isakmp identity address
!
crypto isakmp policy 1
 encryption des
 hash md5
 authentication pre-share
 group 1
 lifetime 86400
crypto isakmp key widecomm address 148.244.240.65
!
! IPSec
!
crypto ipsec transform-set cm-transformset-1 ah-md5-hmac esp-des esp-md5-hmac
crypto map cm-cryptomap local-address Serial 1/0
!
crypto map cm-cryptomap 1 ipsec-isakmp
 match address 100
 set peer 148.244.240.65
 set transform-set cm-transformset-1
 set security-association lifetime seconds 3600
 set security-association lifetime kilobytes 4608000
!
controller E1 0/0
!
interface Dialer 1
 desceigrption connected to Dial-inPCs(modem)_4
 ip unnumbered FastEthernet 0/0
 ip tcp header-compression passive
```

```
 encapsulation ppp
 dialer in-band
 dialer-group 1
 ppp authentication chap
 no cdp enable
 peer default ip address pool 3640isp-Group-1
!
interface Dialer 2
 desceigrption connected to Dial-inPCs(modem)
 ip unnumbered FastEthernet 0/0
 ip tcp header-compression passive
 encapsulation ppp
 dialer in-band
 dialer-group 1
 ppp authentication chap
 no cdp enable
 peer default ip address pool 3640isp-Group-2
!
interface Dialer 3
 desceigrption connected to Dial-inPCs(modem)_1
 ip unnumbered FastEthernet 0/0
 ip tcp header-compression passive
 encapsulation ppp
 dialer in-band
 dialer-group 1
 ppp authentication chap
 no cdp enable
 peer default ip address pool 3640isp-Group-3
!
interface Dialer 4
 desceigrption connected to Dial-inPCs(modem)_2
 ip unnumbered FastEthernet 0/0
 ip tcp header-compression passive
 encapsulation ppp
 dialer in-band
 dialer-group 1
 ppp authentication chap
 no cdp enable
 peer default ip address pool 3640isp-Group-4
!
interface Dialer 5
 desceigrption connected to Dial-inPCs(modem)_8
 ip unnumbered FastEthernet 0/0
 ip tcp header-compression passive
 encapsulation ppp
 dialer in-band
 dialer-group 1
 ppp authentication chap
 no cdp enable
 peer default ip address pool 3640isp-Group-5
!
interface Dialer 6
 desceigrption connected to Dial-inPCs(modem)_3
 ip unnumbered FastEthernet 0/0
 ip tcp header-compression passive
 encapsulation ppp
 dialer in-band
 dialer-group 1
 ppp authentication chap
 no cdp enable
 peer default ip address pool 3640isp-Group-6
!
interface Dialer 7
 desceigrption connected to Dial-inPCs(modem)_5
 ip unnumbered FastEthernet 0/0
 ip tcp header-compression passive
 encapsulation ppp
 dialer in-band
 dialer-group 1
 ppp authentication chap
 no cdp enable
```

```
 peer default ip address pool 3640isp-Group-7
!
interface FastEthernet 0/0
 no desceigrption
 no ip address
 shutdown
!
interface Serial 1/0
 no shutdown
 desceigrption connected to Internet
 crypto map cm-cryptomap
 ip address 148.243.240.67 255.255.255.240
 encapsulation hdlc
!
interface Serial 1/1
 physical-layer async
 no shutdown
 desceigrption connected to Dial-inPCs(modem)_4
 ip unnumbered FastEthernet 0/0
 async mode dedicated
 dialer rotary-group 1
!
interface Serial 1/2
 physical-layer async
 no shutdown
 desceigrption connected to Dial-inPCs(modem)
 ip unnumbered FastEthernet 0/0
 async mode dedicated
 dialer rotary-group 2
!
interface Serial 1/3
 physical-layer async
 no shutdown
 desceigrption connected to Dial-inPCs(modem)_1
 ip unnumbered FastEthernet 0/0
 async mode dedicated
 dialer rotary-group 3
!
interface Serial 1/4
 physical-layer async
 no shutdown
 desceigrption connected to Dial-inPCs(modem)_2
 ip unnumbered FastEthernet 0/0
 async mode dedicated
 dialer rotary-group 4
!
interface Serial 1/5
 physical-layer async
 no shutdown
 desceigrption connected to Dial-inPCs(modem)_8
 ip unnumbered FastEthernet 0/0
 async mode dedicated
 dialer rotary-group 5
!
interface Serial 1/6
 physical-layer async
 no shutdown
 desceigrption connected to Dial-inPCs(modem)_3
 ip unnumbered FastEthernet 0/0
 async mode dedicated
 dialer rotary-group 6
!
interface Serial 1/7
 physical-layer async
 no shutdown
 desceigrption connected to Dial-inPCs(modem)_5
 ip unnumbered FastEthernet 0/0
 async mode dedicated
 dialer rotary-group 7
!
router eigrp
```

```
 passive-interface Serial 1/0
 no auto-summary
!
!
ip local pool 3640isp-Group-1 172.16.100.1 172.16.100.1
ip local pool 3640isp-Group-2 172.16.100.1 172.16.100.1
ip local pool 3640isp-Group-3 172.16.100.1 172.16.100.1
ip local pool 3640isp-Group-4 172.16.100.1 172.16.100.1
ip local pool 3640isp-Group-5 172.16.100.1 172.16.100.1
ip local pool 3640isp-Group-6 172.16.100.1 172.16.100.1
ip local pool 3640isp-Group-7 172.16.100.1 172.16.100.1
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Serial 1/0
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
!
line 18
 exec
 autoselect ppp
 autoselect during-login
 login local
 modem InOut
 transport input all
 stopbits 1
 speed 38400
 flowcontrol hardware
!
line 19
 exec
 autoselect ppp
 autoselect during-login
 login local
 modem InOut
 transport input all
 stopbits 1
 speed 38400
 flowcontrol hardware
!
line 20
 exec
 autoselect ppp
 autoselect during-login
 login local
 modem InOut
 transport input all
 stopbits 1
 speed 38400
 flowcontrol hardware
!
line 21
 exec
 autoselect ppp
 autoselect during-login
 login local
 modem InOut
 transport input all
 stopbits 1
```

```
 speed 38400
 flowcontrol hardware
!
line 22
 exec
 autoselect ppp
 autoselect during-login
 login local
 modem InOut
 transport input all
 stopbits 1
 speed 38400
 flowcontrol hardware
!
line 23
 exec
 autoselect ppp
 autoselect during-login
 login local
 modem InOut
 transport input all
 stopbits 1
 speed 38400
 flowcontrol hardware
!
line 24
 exec
 autoselect ppp
 autoselect during-login
 login local
 modem InOut
 transport input all
 stopbits 1
 speed 38400
 flowcontrol hardware
!
end

! ************************************************************************
! 1720internet.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.5 Build 8
!   Lunes, 10 de Septiembre de 2001, 09:25:37 p.m.
!
! Hostname: 1720internet
! Model: 1720
! ************************************************************************
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname 1720internet
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
! Internet Key Exchange (IKE)
!
crypto isakmp enable
crypto isakmp identity address
!
crypto isakmp policy 1
 encryption des
 hash md5
```

```
 authentication pre-share
 group 1
 lifetime 86400
crypto isakmp key widecomm address 148.243.240.67
!
! IPSec
!
crypto ipsec transform-set cm-transformset-1 ah-md5-hmac esp-des esp-md5-hmac
crypto map cm-cryptomap local-address Serial 0
!
crypto map cm-cryptomap 1 ipsec-isakmp
 match address 100
 set peer 148.243.240.67
 set transform-set cm-transformset-1
 set security-association lifetime seconds 3600
 set security-association lifetime kilobytes 4608000
!
interface FastEthernet 0
 no desceigrption
 no ip address
 shutdown
!
interface Serial 0
 no shutdown
 desceigrption connected to Internet
 crypto map cm-cryptomap
 ip address 148.244.240.65 255.255.255.240
 encapsulation hdlc
!
router eigrp

 passive-interface Serial 0
 no auto-summary
!
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Serial 0
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
!
end

! ************************************************************************
! 2610gdl.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.5 Build 8
!   Lunes, 10 de Septiembre de 2001, 09:26:07 p.m.
!
! Hostname: 2610gdl
! Model: 2610
! ************************************************************************
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname 2610gdl
```

```
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Ethernet 0/0
 no shutdown
 desceigrption connected to Red Local de Gudalajara
 ip address 172.16.20.254 255.255.255.0
 keepalive 10
!
interface Serial 0/0
 no shutdown
 desceigrption connected to 3640mex
 bandwidth 128
 ip address 172.16.1.2 255.255.255.252
 encapsulation ppp
 ip rtp header-compression
 ip rtp reserve 16384 100 48
!
voice-port 1/0/0
 no shutdown
 desceigrption connected to tel_gdl_001 (71-001)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/0/1
 no shutdown
 desceigrption connected to tel_gdl_002 (71-002)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/0
 no shutdown
 desceigrption connected to tel_gdl_003 (71-003)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/1
 no shutdown
 desceigrption connected to fax_gdl_004 (71-004)
 comfort-noise
 cptone MX
 signal loopstart
!
dial-peer voice 1 pots
 port 1/0/0
 destination-pattern 71001
!
dial-peer voice 2 pots
 port 1/0/1
 destination-pattern 71002
!
dial-peer voice 3 pots
 port 1/1/0
 destination-pattern 71003
!
dial-peer voice 4 pots
 port 1/1/1
 destination-pattern 71004
!
dial-peer voice 10 voip
 codec g729r8
 ip precedence 5
```

```
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72001
!
dial-peer voice 11 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72002
!
dial-peer voice 12 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72003
!
dial-peer voice 13 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72004
!
dial-peer voice 14 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73001
!
dial-peer voice 15 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73002
!
dial-peer voice 16 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73003
!
dial-peer voice 17 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73004
!
dial-peer voice 18 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74001
!
dial-peer voice 19 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74002
!
dial-peer voice 20 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
```

```
 vad
 destination-pattern 74003
!
dial-peer voice 21 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74004
!
dial-peer voice 22 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75001
!
dial-peer voice 23 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75002
!
dial-peer voice 24 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75003
!
dial-peer voice 25 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75004
!
dial-peer voice 26 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76001
!
dial-peer voice 27 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76002
!
dial-peer voice 28 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76003
!
dial-peer voice 29 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76004
!
dial-peer voice 30 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
```

```
 destination-pattern 77001
!
dial-peer voice 31 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77002
!
dial-peer voice 32 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77003
!
dial-peer voice 33 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77004
!
dial-peer voice 34 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78001
!
dial-peer voice 35 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78002
!
dial-peer voice 36 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78003
!
dial-peer voice 37 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78004
!
! VoIP phone number-to-extension database
!
num-exp 1... 71...
num-exp 2... 72...
num-exp 3... 73...
num-exp 4... 74...
num-exp 5... 75...
num-exp 6... 76...
num-exp 7... 77...
num-exp 8... 78...
!
router eigrp

 network 172.16.0.0
 no auto-summary
!
!
ip classless
no ip http server
snmp-server community public RO
```

```
no snmp-server location
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
!
end

! ************************************************************************
! 2610mty.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.5 Build 8
!   Lunes, 10 de Septiembre de 2001, 09:26:22 p.m.
!
! Hostname: 2610mty
! Model: 2610
! ************************************************************************
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname 2610mty
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Ethernet 0/0
 no shutdown
 desceigrption connected to Red Local de Monterrey
 ip address 172.16.30.254 255.255.255.0
 keepalive 10
!
interface Serial 0/0
 no shutdown
 desceigrption connected to 3640mex
 bandwidth 196
 ip address 172.16.1.6 255.255.255.252
 encapsulation ppp
 ip rtp header-compression
 ip rtp reserve 16384 100 48
!
interface Serial 0/1
 no desceigrption
 no ip address
 shutdown
!
voice-port 1/0/0
 no shutdown
 desceigrption connected to tel_mty_001 (72-001)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/0/1
 no shutdown
 desceigrption connected to tel_mty_002 (72-002)
 comfort-noise
 cptone MX
```

```
 signal loopstart
!
voice-port 1/1/0
 no shutdown
 desceigrption connected to tel_mty_003 (72-003)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/1
 no shutdown
 desceigrption connected to fax_mty_004 (72-004)
 comfort-noise
 cptone MX
 signal loopstart
!
dial-peer voice 1 pots
 port 1/0/0
 destination-pattern 72001
!
dial-peer voice 2 pots
 port 1/0/1
 destination-pattern 72002
!
dial-peer voice 3 pots
 port 1/1/0
 destination-pattern 72003
!
dial-peer voice 4 pots
 port 1/1/1
 destination-pattern 72004
!
dial-peer voice 9 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71001
!
dial-peer voice 10 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71002
!
dial-peer voice 11 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71003
!
dial-peer voice 12 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71004
!
dial-peer voice 13 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73001
!
dial-peer voice 14 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
```

```
 vad
 destination-pattern 73002
!
dial-peer voice 15 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73003
!
dial-peer voice 16 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73004
!
dial-peer voice 17 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74001
!
dial-peer voice 18 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74002
!
dial-peer voice 19 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74003
!
dial-peer voice 20 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74004
!
dial-peer voice 21 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75001
!
dial-peer voice 22 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75002
!
dial-peer voice 23 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75003
!
dial-peer voice 24 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
```

```
 destination-pattern 75004
!
dial-peer voice 25 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76001
!
dial-peer voice 26 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76002
!
dial-peer voice 27 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76003
!
dial-peer voice 28 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76004
!
dial-peer voice 29 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77001
!
dial-peer voice 30 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77002
!
dial-peer voice 31 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77003
!
dial-peer voice 32 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77004
!
dial-peer voice 33 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78001
!
dial-peer voice 34 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78002
```

```
!
dial-peer voice 35 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78003
!
dial-peer voice 36 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78004
!
! VoIP phone number-to-extension database
!
num-exp 1... 71...
num-exp 2... 72...
num-exp 3... 73...
num-exp 4... 74...
num-exp 5... 75...
num-exp 6... 76...
num-exp 7... 77...
num-exp 8... 78...
!
router eigrp

 network 172.16.0.0
 no auto-summary
!
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
!
end

! ************************************************************************
! 2610leo.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.5 Build 8
!   Lunes, 10 de Septiembre de 2001, 09:26:33 p.m.
!
! Hostname: 2610leo
! Model: 2610
! ************************************************************************
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname 2610leo
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
```

```
no ip domain-lookup
ip routing
!
interface Ethernet 0/0
 no shutdown
 desceigrption connected to Red Local de León
 ip address 172.16.50.254 255.255.255.0
 keepalive 10
!
interface Serial 0/0
 no shutdown
 desceigrption connected to 2610qro
 bandwidth 64
 ip address 172.16.1.26 255.255.255.252
 encapsulation ppp
 ip rtp header-compression
 ip rtp reserve 16384 100 24
!
interface Serial 0/1
 no desceigrption
 no ip address
 shutdown
!
voice-port 1/0/0
 no shutdown
 desceigrption connected to tel_leo_001 (76-001)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/0/1
 no shutdown
 desceigrption connected to tel_leo_002 (76-002)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/0
 no shutdown
 desceigrption connected to tel_leo_003 (76-003)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/1
 no shutdown
 desceigrption connected to fax_leo_004 (76-004)
 comfort-noise
 cptone MX
 signal loopstart
!
dial-peer voice 1 pots
 port 1/0/0
 destination-pattern 76001
!
dial-peer voice 2 pots
 port 1/0/1
 destination-pattern 76002
!
dial-peer voice 3 pots
 port 1/1/0
 destination-pattern 76003
!
dial-peer voice 4 pots
 port 1/1/1
 destination-pattern 76004
!
dial-peer voice 5 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
```

```
 vad
 destination-pattern 73001
!
dial-peer voice 6 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73002
!
dial-peer voice 7 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73003
!
dial-peer voice 8 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73004
!
dial-peer voice 9 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71001
!
dial-peer voice 10 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71002
!
dial-peer voice 11 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71003
!
dial-peer voice 12 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71004
!
dial-peer voice 13 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72001
!
dial-peer voice 14 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72002
!
dial-peer voice 15 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
```

```
 destination-pattern 72003
!
dial-peer voice 16 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72004
!
dial-peer voice 17 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74001
!
dial-peer voice 18 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74002
!
dial-peer voice 19 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74003
!
dial-peer voice 20 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74004
!
dial-peer voice 21 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75001
!
dial-peer voice 22 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75002
!
dial-peer voice 23 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75003
!
dial-peer voice 24 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75004
!
dial-peer voice 25 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77001
```

```
!
dial-peer voice 26 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77002
!
dial-peer voice 27 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77003
!
dial-peer voice 28 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77004
!
dial-peer voice 29 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78001
!
dial-peer voice 30 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78002
!
dial-peer voice 31 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78003
!
dial-peer voice 32 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78004
!
! VoIP phone number-to-extension database
!
num-exp 1... 71...
num-exp 2... 72...
num-exp 3... 73...
num-exp 4... 74...
num-exp 5... 75...
num-exp 6... 76...
num-exp 7... 77...
num-exp 8... 78...
!
router eigrp

 network 172.16.0.0
 no auto-summary
!
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
```

```
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
!
end

! ************************************************************************
! 2610qro.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.5 Build 8
!   Lunes, 10 de Septiembre de 2001, 09:26:46 p.m.
!
! Hostname: 2610qro
! Model: 2610
! ************************************************************************
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname 2610qro
!
enable password cisco
username cisco password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Ethernet 0/0
 no shutdown
 desceigrption connected to Red Local de Querétaro
 ip address 172.16.40.254 255.255.255.0
 keepalive 10
!
interface Serial 0/0
 no shutdown
 desceigrption connected to 3640mex
 bandwidth 256
 ip address 172.16.1.10 255.255.255.252
 encapsulation ppp
 ip rtp header-compression
 ip rtp reserve 16384 100 48
!
interface Serial 0/1
 no shutdown
 desceigrption connected to 2610sjr
 bandwidth 64
 ip address 172.16.1.21 255.255.255.252
 encapsulation ppp
 ip rtp header-compression
 ip rtp reserve 16384 100 24
!
interface Serial 0/2
 no shutdown
 desceigrption connected to 2610leo
 bandwidth 64
 ip address 172.16.1.25 255.255.255.252
 encapsulation ppp
 ip rtp header-compression
 ip rtp reserve 16384 100 24
```

```
!
voice-port 1/0/0
 no shutdown
 desceigrption connected to tel_qro_001 (73-001)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/0/1
 no shutdown
 desceigrption connected to tel_qro_002 (73-002)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/0
 no shutdown
 desceigrption connected to tel_qro_003 (73-003)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/1
 no shutdown
 desceigrption connected to fax_qro_004 (73-004)
 comfort-noise
 cptone MX
 signal loopstart
!
dial-peer voice 1 pots
 port 1/0/0
 destination-pattern 73001
!
dial-peer voice 2 pots
 port 1/0/1
 destination-pattern 73002
!
dial-peer voice 3 pots
 port 1/1/0
 destination-pattern 73003
!
dial-peer voice 4 pots
 port 1/1/1
 destination-pattern 73004
!
dial-peer voice 5 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71001
!
dial-peer voice 6 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71002
!
dial-peer voice 7 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71003
!
dial-peer voice 8 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
```

```
 destination-pattern 71004
!
dial-peer voice 9 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72001
!
dial-peer voice 10 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72002
!
dial-peer voice 11 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72003
!
dial-peer voice 12 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72004
!
dial-peer voice 13 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74001
!
dial-peer voice 14 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74002
!
dial-peer voice 15 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74003
!
dial-peer voice 16 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74004
!
dial-peer voice 17 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75001
!
dial-peer voice 18 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75002
```

```
!
dial-peer voice 19 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75003
!
dial-peer voice 20 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75004
!
dial-peer voice 21 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76001
!
dial-peer voice 22 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76002
!
dial-peer voice 23 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76003
!
dial-peer voice 24 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76004
!
dial-peer voice 25 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77001
!
dial-peer voice 26 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77002
!
dial-peer voice 27 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77003
!
dial-peer voice 28 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77004
!
```

```
dial-peer voice 29 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78001
!
dial-peer voice 30 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78002
!
dial-peer voice 31 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78003
!
dial-peer voice 32 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78004
!
! VoIP phone number-to-extension database
!
num-exp 1... 71...
num-exp 2... 72...
num-exp 3... 73...
num-exp 4... 74...
num-exp 5... 75...
num-exp 6... 76...
num-exp 7... 77...
num-exp 8... 78...
!
router eigrp

 network 172.16.0.0
 no auto-summary
!
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
!
end

! ************************************************************************
! 2610sjr.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.5 Build 8
!   Lunes, 10 de Septiembre de 2001, 09:27:12 p.m.
!
! Hostname: 2610sjr
! Model: 2610
! ************************************************************************
!
```

```
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname 2610sjr
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Ethernet 0/0
 no shutdown
 desceigrption connected to Red Local de San JUan del Rio
 ip address 172.16.60.254 255.255.255.0
 keepalive 10
!
interface Serial 0/0
 no shutdown
 desceigrption connected to 2610qro
 bandwidth 64
 ip address 172.16.1.22 255.255.255.252
 encapsulation ppp
 ip rtp header-compression
 ip rtp reserve 16384 100 24
!
interface Serial 0/1
 no desceigrption
 no ip address
 shutdown
!
voice-port 1/0/0
 no shutdown
 desceigrption connected to tel_sjr_001 (77-001)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/0/1
 no shutdown
 desceigrption connected to tel_sjr_002 (77-002)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/0
 no shutdown
 desceigrption connected to tel_sjr_003 (77-003)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/1
 no shutdown
 desceigrption connected to fax_sjr_004 (77-004)
 comfort-noise
 cptone MX
 signal loopstart
!
dial-peer voice 1 pots
 port 1/0/0
 destination-pattern 77001
!
dial-peer voice 2 pots
 port 1/0/1
 destination-pattern 77002
```

```
!
dial-peer voice 3 pots
 port 1/1/0
 destination-pattern 77003
!
dial-peer voice 4 pots
 port 1/1/1
 destination-pattern 77004
!
dial-peer voice 5 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73001
!
dial-peer voice 6 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73002
!
dial-peer voice 7 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73003
!
dial-peer voice 8 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73004
!
dial-peer voice 9 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71001
!
dial-peer voice 10 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71002
!
dial-peer voice 11 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71003
!
dial-peer voice 12 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71004
!
dial-peer voice 13 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72001
```

```
!
dial-peer voice 14 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72002
!
dial-peer voice 15 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72003
!
dial-peer voice 16 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72004
!
dial-peer voice 17 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74001
!
dial-peer voice 18 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74002
!
dial-peer voice 19 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74003
!
dial-peer voice 20 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74004
!
dial-peer voice 21 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75001
!
dial-peer voice 22 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75002
!
dial-peer voice 23 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75003
!
```

```
dial-peer voice 24 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75004
!
dial-peer voice 25 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76001
!
dial-peer voice 26 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76002
!
dial-peer voice 27 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76003
!
dial-peer voice 28 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76004
!
dial-peer voice 29 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78001
!
dial-peer voice 30 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78002
!
dial-peer voice 31 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78003
!
dial-peer voice 32 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78004
!
! VoIP phone number-to-extension database
!
num-exp 1... 71...
num-exp 2... 72...
num-exp 3... 73...
num-exp 4... 74...
num-exp 5... 75...
num-exp 6... 76...
```

```
num-exp 7... 77...
num-exp 8... 78...
!
router eigrp

 network 172.16.0.0
 no auto-summary
!
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
!
end

! ************************************************************************
! 2610gp.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.5 Build 8
!   Lunes, 10 de Septiembre de 2001, 09:27:21 p.m.
!
! Hostname: 2610gp
! Model: 2610
! ************************************************************************
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname 2610gp
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Ethernet 0/0
 no shutdown
 desceigrption connected to Red Local de Gómez Palacio
 ip address 172.16.80.254 255.255.255.0
 keepalive 10
!
interface Serial 0/0
 no shutdown
 desceigrption connected to 3640mex
 bandwidth 128
 ip address 172.16.1.14 255.255.255.252
 encapsulation ppp
 ip rtp header-compression
 ip rtp reserve 16384 100 48
!
interface Serial 0/1
 no desceigrption
 no ip address
 shutdown
!
```

```
voice-port 1/0/0
 no shutdown
 desceigrption connected to tel_gp_001 (74-001)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/0/1
 no shutdown
 desceigrption connected to tel_gp_002 (74-002)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/0
 no shutdown
 desceigrption connected to tel_gp_003 (74-003)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/1
 no shutdown
 desceigrption connected to fax_gp_004 (74-004)
 comfort-noise
 cptone MX
 signal loopstart
!
dial-peer voice 1 pots
 port 1/0/0
 destination-pattern 74001
!
dial-peer voice 2 pots
 port 1/0/1
 destination-pattern 74002
!
dial-peer voice 3 pots
 port 1/1/0
 destination-pattern 74003
!
dial-peer voice 4 pots
 port 1/1/1
 destination-pattern 74004
!
dial-peer voice 5 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73001
!
dial-peer voice 6 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73002
!
dial-peer voice 7 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73003
!
dial-peer voice 8 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73004
```

```
!
dial-peer voice 9 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71001
!
dial-peer voice 10 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71002
!
dial-peer voice 11 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71003
!
dial-peer voice 12 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71004
!
dial-peer voice 13 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72001
!
dial-peer voice 14 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72002
!
dial-peer voice 15 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72003
!
dial-peer voice 16 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72004
!
dial-peer voice 17 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75001
!
dial-peer voice 18 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75002
!
```

```
dial-peer voice 19 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75003
!
dial-peer voice 20 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.70.254
 vad
 destination-pattern 75004
!
dial-peer voice 21 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76001
!
dial-peer voice 22 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76002
!
dial-peer voice 23 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76003
!
dial-peer voice 24 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76004
!
dial-peer voice 25 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77001
!
dial-peer voice 26 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77002
!
dial-peer voice 27 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77003
!
dial-peer voice 28 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77004
!
dial-peer voice 29 voip
```

```
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78001
!
dial-peer voice 30 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78002
!
dial-peer voice 31 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78003
!
dial-peer voice 32 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78004
!
! VoIP phone number-to-extension database
!
num-exp 1... 71...
num-exp 2... 72...
num-exp 3... 73...
num-exp 4... 74...
num-exp 5... 75...
num-exp 6... 76...
num-exp 7... 77...
num-exp 8... 78...
!
router eigrp

 network 172.16.0.0
 no auto-summary
!
!
ip classless
no ip http server
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
!
end

! ************************************************************************
! 2610tol.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.5 Build 8
!   Lunes, 10 de Septiembre de 2001, 09:27:30 p.m.
!
! Hostname: 2610tol
! Model: 2610
! ************************************************************************
!
service timestamps debug uptime
```

```
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname 2610tol
!
enable password cisco
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Ethernet 0/0
 no shutdown
 desceigrption connected to Red Local de Toluca
 ip address 172.16.70.254 255.255.255.0
 keepalive 10
!
interface Serial 0/0
 no shutdown
 desceigrption connected to 3640mex
 bandwidth 128
 ip address 172.16.1.18 255.255.255.252
 encapsulation ppp
 ip rtp header-compression
 ip rtp reserve 16384 100 48
!
interface Serial 0/1
 no desceigrption
 no ip address
 shutdown
!
voice-port 1/0/0
 no shutdown
 desceigrption connected to tel_tol_001 (75-001)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/0/1
 no shutdown
 desceigrption connected to tel_tol_002 (75-002)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/0
 no shutdown
 desceigrption connected to tel_tol_003 (75-003)
 comfort-noise
 cptone MX
 signal loopstart
!
voice-port 1/1/1
 no shutdown
 desceigrption connected to fax_tol_004 (75-004)
 comfort-noise
 cptone MX
 signal loopstart
!
dial-peer voice 1 pots
 port 1/0/0
 destination-pattern 75001
!
dial-peer voice 2 pots
 port 1/0/1
 destination-pattern 75002
!
```

```
dial-peer voice 3 pots
 port 1/1/0
 destination-pattern 75003
!
dial-peer voice 4 pots
 port 1/1/1
 destination-pattern 75004
!
dial-peer voice 5 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73001
!
dial-peer voice 6 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73002
!
dial-peer voice 7 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73003
!
dial-peer voice 8 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.40.254
 vad
 destination-pattern 73004
!
dial-peer voice 9 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71001
!
dial-peer voice 10 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71002
!
dial-peer voice 11 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71003
!
dial-peer voice 12 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.20.254
 vad
 destination-pattern 71004
!
dial-peer voice 13 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72001
!
```

```
dial-peer voice 14 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72002
!
dial-peer voice 15 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72003
!
dial-peer voice 16 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.30.254
 vad
 destination-pattern 72004
!
dial-peer voice 17 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74001
!
dial-peer voice 18 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74002
!
dial-peer voice 19 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74003
!
dial-peer voice 20 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.80.254
 vad
 destination-pattern 74004
!
dial-peer voice 21 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76001
!
dial-peer voice 22 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76002
!
dial-peer voice 23 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76003
!
dial-peer voice 24 voip
```

```
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.50.254
 vad
 destination-pattern 76004
!
dial-peer voice 25 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77001
!
dial-peer voice 26 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77002
!
dial-peer voice 27 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77003
!
dial-peer voice 28 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.60.254
 vad
 destination-pattern 77004
!
dial-peer voice 29 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78001
!
dial-peer voice 30 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78002
!
dial-peer voice 31 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78003
!
dial-peer voice 32 voip
 codec g729r8
 ip precedence 5
 session target ipv4:172.16.10.254
 vad
 destination-pattern 78004
!
! VoIP phone number-to-extension database
!
num-exp 1... 71...
num-exp 2... 72...
num-exp 3... 73...
num-exp 4... 74...
num-exp 5... 75...
num-exp 6... 76...
num-exp 7... 77...
```

APÉNDICE B

Acrónimos

ADSL (Asynchronous Digital Suscriber Line, Línea de Abonado Digital en modo Asíncrono)
AM (Amplitud Modulada)
ANSI (American National Standards Institute, Instituto de Estandares Nacional Americano)
ARCNET (Attached Resource Computer Network, Red de Computadoras de Recursos Conectados)
ARP (Access Request Point, Punto de Petición de Acceso)
ARPANET (Advanced Research Projects Administration Network, Red Avanzada de Administración de Proyectos)
ASCII
ASIC
ASK (Amplitud Shift Keying, Codificación por Cambio en Amplitud)
ASP (Active Server Pages, Páginas de Servidor Activo)
ASPs (Application Service Providers, Proveedores de Servicios de Aplicación)
ATM (Asyncronus Transfer Mode, Modo de Transferencia Asíncrona)
AUI (Attachment Unit Interface, Unidad Interface de Adjuntado)
BASE (Banda Base)
BIA (Burn In Address)
BOOT (Bootstrap Protocol, Protocolo de Arranque)
BRI (Basic Rate Interface; Interface Basica de Velocidad)
BROAD (Banda Ancha)
BROWSER (Buscador)
CAD (Converter Analog Digital, Convertidor Analogo-Digital)
CAS (Channel Associated Signaling, Señalización por Canal Asociado)
CCITT (Consultative Committe on International Telephony and Telegraphy, Comité de Consulta Internacional en Telegrafía y Telefonía)
CET (Cisco Encryption Technology, Tecnología de Encripción de Cisco)
CFE (Comisión Federal de Electricidad)
CIR (Comitted Information Rate, Tasa de Intercambio de información Comprometida.)
CO (Central Office, Oficina Central)
CODEC (COdificador DECodificador)
COT's (Central Office Trunks, Troncales de Oficina Central)
CPE (Customer Premises Equipment, Equipo en las Instalaciones del Cliente)
CSMA/CD (Carrier Sense Multiple Access with Collision Detection, Acceso Múltiple por Sensado de Portadora con Detección de Colisiones).
CTI (Computer-Telephony Integration, Integración Servidora Teléfono)
CHAP (Challenge Handshake Authentication Protocol, Protocolo de Autentificación de Intercambio de Saludo)
DARPA (Defense Advanced Research Projects Agency, Agencia de Desarrollo Avanzado de Proyectos de la Defensa)
DCE (Data Communications Equipment, Equipo de Comunicación de Datos)
DES (Data Encrypted Standar, Estándar de Encripción de Datos)
DES (Data Encryption Standard,Estándar de Encriptado)
DID (Direct Inward Dial, Números Directos)
DISA (Direct Inward System Access, Sistema de Acceso Entrante Directo)
DISA (Direct Inward System Access, Sistema de Acceso Entrante Directo)
DNS (Domain Name Server, Servidor de Dominio de Nombre)
DNS (Domain Name Service, Servicio de Nombre de Dominios)

DOD (Department Of Defense, Departamento de la Defensa)
DSP (Digital Signal Processor, Procesadores Digitales de Señal)
DTE (Data Terminal Equipment, Equipo Terminal de Datos)
DTMF (Dual Tone Multifrequency, Tonos Duales de Multifrecuencia)
EDI (Electronic Data Interchange, Intercambio Electrónico de Datos)
EEPROMs (Electrically Ereasable Programable Memory, Memoria Programable y Borrable Electricamente)
EIA (Electronic Industries Alliance, Alianza de Industrias Electronicas)
EIGRP (Enhanced Interior Gateway Routing Protocol,Protocolo de Ruteo Interno de Puerta de Acceso)
E-mail (Electronic Mail, Correo Electrónico)
FDDI (Fibre Distributed Data Interface, Interface de Distribución de Datos por Fibra)
FI (Facultad de Ingeniería)
FIPS (Federal Information Process System, Sistema Federal de Transporte de Información)
Firewall (Pared de Fuego)
FM (Frecuencia Modulada)
FPS (Firewall Proxy Server , Servidor Apoderado del Proxi)
FSK (Frequency Shift Keying, Codificación por Cambio en la Frecuencia)
FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos)
FXO (Foreing Exchange Office, Oficina de conmutación Foranea)
FXS (Foreing Exchange Station, Estación de Conmutación Foranea)
GRE (Generic Routing Encapsulation, Encapsulamiento de Ruteo Generico)
GS (Ground Start, Arranque por Detección de Tierra)
HTML (Hypertext Mark-Up Language, Lenguaje de Marcado de Hipertexto)
IBM (Industries for Business Machines, Equipos para Industrias de Negocio)
ICMP (Internet Control Message Protocol, Protocolo de Control de Mensajes de Internet)
IEEE (Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos)
IETF (Internet Engineering Task Force, Fuerza de Tareas de Ingeniería para la Internet)
IGMP (Internet Group Management Protocol, Protocolo de Administración de Grupo de Internet)
IIS (Internet information Server, Servicio de Servidor de Información de Internet)
IKE (Internet Key Exchange, Intercambio de Claves de Internet)
IP (Internet Protocol, Protocolo de Internet)
IPSec (Internet Protocol Security, Seguridad de Protocolo de Internet)
IPX (Internetworking Packet Exchange, Intercambio de Paquetes Interredes)
ISA (Industrial Standard Application,
ISDN (Integrated Services Digital Network, Red Digital de Servicios Integrados)
ISO (Internacional Standard Organization, Organización Internacional de Estandarización)
ISP (Internet Service Provider. Proveedor de Servicios de Internet)
IT (Information Technologies, Tecnologías de Información)
ITU-T (Internacional Telecominications Union, Union Internacional de Telecomunicaciones)
ITU-T (International Telecommunications Union, Unión Internacional de Telecomunicaiones)
IWU (InterWorking Unit, Unidad InterRedes)
L2TP (Level 2 Tunel Protocol, Protocolo de Túnel de Nivel 2)
LAN (Local Area Network, Red de Área Local)
LCP (Link Control Protocol, Protocolo de Control de Enlace)

LS (Loop Start, Arranque por detección Cierre de Circuito)
MAC (Medium Access Control, Control de Acceso al Medio)
MD2 (Message Digest 2, Resumen de Mensaje 2)
MD4 (Message Digest 2, Resumen de Mensaje 4)
MD5 (Message Digest 2, Resumen de Mensaje 5)
MILNET (Military Net, Red militar)
MODEM (MOdulador-DEModulador)
MR2 (Modified R2, R2 Modificado)
MSAU (Multiple Stations Access Unit, Unidades de Acceso a Múltiples Estaciones)
NAS (Network Access Server, Servidor de Acceso de Red)
NAT (Network Address Translator,Traductor de Direcciones de Red)
NCO (Netware Core Protocol, Protocolo de Red Core)
NICs (Network Interface Cards, Tarjetas de Interfaz de Red)
NIST (National Institute of Standars and Technology, Instituto Nacional de Estandares y Tecnologia)
NSA (National Security Agency, Agencia de Seguridad Nacional)
NTP (Network Time Protocol, Protocolo deTiempo de Red)
OSI (Open System Interconection, Interconexión de Sistema Abierto)
PAM (Pulse Amplitud Modulation, Modulación por Amplitud de Pulso)
PAT (Port Address Translation, Traducción de Dirección por Puerto)
PBX (Private Branch eXchange, Conmutador de voz Privado)
PC (Personal Computer, Computadora Personal)
PCM (Pulse Code Modulation, Modulación por Código de Pulso)
POP3 (Post Office Protocol,Protocolo Posterior de Oficina)
POTS (Plain Old Telephone Network, Red Telefónica de Marcación Antigua)
PPP (Point-to-Point Protocol, Protocolo Punto a Punto)
PPTP (Point-to-Point Tunneling Protocol, Protocolo de tunelización Punto a Punto)
PRI (Primary Rate Interface, Interface Primaria de Velocidad)
PSK (Pulse Shift Keying,Codificación por Cambio de Pulso)
PSTN (Public Switching Telephony Network, Red Telefónica Pública Conmutada)
PyMEs (Pequeñas y Medianas Empresas)
QoS (Quality of Service, Calidad de Servicio)
RADIUS (Remote Address Dial In User Service, Servicio de Usuario de Dirección Remota por Marcación)
RAM (Random Access Memory, Memoria de Acceso Aleatorio)
RARP (Reverse Address Resolution Protocol, Protocolo de Resolución por Dirección Inversa)
RAS (Registration, Admision and Status , Registro Adminitration and Status)
RDSI (Red Digital de Servicios Integrados)
RDSI-BA (Red Digital de Servicios Integrados. Banda-Ancha)
RDSI-BE (Red Digital de Servicios Integrados. Banda-Estrecha)
RFCs (Request For Comment, Solicitud de Comentarios)
RIP (Router Information Protocol, Protocolo de Información de Ruteo)
Round Robin (Toma Circular Secuencial)
RTCP (Real Time Control Protocol, Protocolo de Control en Tiempo Real)
RTP (Real Time Protocol, Protocolo en Tiempo Real)
SAP (Service Advertising protocol, Protocolo de Servicio de Advertencia)

SCAN (System Control Antivirus Network, Sistema de Control de Antivirus en la Red)
SDLC (Synchronous Data Link Control, Control de Enlace de Datos Síncrono)
SHA (Secure Hash Algorithm, Algoritmo de Seguridad por Confrontamiento)
SHF (Super High Frecuency, Super Alta Frecuencia)
SLIP (Serial Line IP Protocol, Protocolo de Internet por Línea Serial)
SMDS (Switched Multi-Megabit Data Service, Servicio Conmutado de Datos Multi-megabit)
SMTP (Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo)
SNA (System Network Architecture, Arquitectura de Sistema de Red)
SNR (Signal to Noise Ratio, Tasa de Señal-Ruido)
SPX (Sequential Packet Exchange, Intercambio de Paquetes Secuencialmente)
SSH (Non-Secure Shell,Concha no segura)
SSL (Secure Socket Layer,Eqtiquetado de Seguridad)
STP (Shielded Twisted Pair, Par Trenzado Blindado)
STP (Spanning Tree Protocol, Protocolo de Expansión de Árbol)
TA (Terminal Adapters, Adaptadores de Terminal)
TACACS+ (Terminal Access Controller Access Control System Plus, Sistema de Control de Acceso por Controlador de Acceso Terminal Plus)
TCP (Transmition Control Protocol , Protocolo de Control de Transmisión)
TELMEX (Teléfonos de México)
TIA (Telecommunications Industry Association, Asociación de la Industria de Telecomunicaciones)
UART (Universal Asynchronous Receiver Transmitter, Transmisor- Receptor Universal Asíncrono)
UDP (User Datagram Protocol, Protocolo estructura de Datos de Usuario)
UNAM (Universidad Nacional Autónoma de México)
UPS (Uniterrumplible Power Systems, Sistemas de Energía sin Interrupción)
URLs (Universal Resource Location, Ubicación Universal de Recurso)
UTP (Unshielded Twisted Pair, Par Trenzado Sin Blindaje)
VAD (Voice Absence Deleting, Borrado en Ausencia de Voz)
VDT (Video Data Termial, Terminal de video de datos)
VF (Voice Frequencies, Frecuencias de Voz)
VLANs (Virtual Local Area Network, Redes de Área Local Virtual)
VPDN (Virtual Private Dial-Up Network, Red de Marcación Privada Virtual)
VPN (Virtual Private Network, Red Privada Virtual)
WAN (Wide Area Network, Redes de Área Amplia)
WWW (World Wide Web, Red Amplia Mundial)

APÉNDICE C

Especificaciones del Equipo

A continuación se presentan las especificaciones técnicas de los equipos de comunicaciones

Equipos de acceso:

Cisco 1720

Technical Specifications
Physical Interfaces/Ports
• One 10/100BaseTX Fast Ethernet port (RJ-45)
– Automatic speed detection
– Automatic duplex negotiation
• Two WAN interface card slots
– Supports any combination of up to two WAN
interface cards as shown in Table 1: WIC-1T, WIC-2T,
WIC-1DSU-56K4, WIC-1DSU-T1, WIC-1B-S/T,
WIC-1B-U, WIC-2A/S, WIC-1ADSL, WIC-1ENET
• Synchronous serial interfaces on serial WAN interface
cards
– Interface speed: up to 2.0 Mbps (T1/E1)
– Synchronous serial protocols: PPP, High-Level Data
Link Control (HDLC), Link Access Procedure, Balanced (LAPB), IBM SNA
– Synchronous serial WAN services: Frame Relay, X.25,
SMDS
– Synchronous serial interfaces supported on the
WIC-1T, WIC-2T, and WIC-2A/S cards: V.35, EIA/
TIA-232, EIA/TIA-449, X.21, EIA-530
• Asynchronous serial interfaces on serial WAN interface
cards
– Interface speed: up to 115.2 kbps
– Asynchronous serial protocols: PPP, Serial Line
Internet Protocol (SLIP)
– Asynchronous interface: EIA/TIA-232
• ADSL WAN interface card
– Supports ATMadaptation layer 5 (AAL5) services and
applications
– Interoperates with Alcatel DSL access multiplexer
(DSLAM) with Alcatel chipset and Cisco 6130/6260
DSLAM with Globespan chipset
– Complies with ANSI T1.413 issue 2 and ITU 992.1
(G.DMT)
• ISDN WAN interface cards
– ISDN dialup and ISDN DSL (IDSL) at 64 and
128 kbps
– Encapsulation over IDSL Frame Relay and PPP
• One auxiliary (AUX) port
– RJ-45 jack with EIA/TIA-232 interface (plug compatible with Cisco 2500 series AUX port)
– Asynchronous serial data terminal equipment (DTE)
with full modem controls Carrier Detect (CD), data
sheet ready (DSR), Request To Send (RTS), Clear To
Send (CTS)
– Asynchronous serial data rates up to 115.2 kbps
• One console port
– RJ-45 jack with EIA/TIA-232 interface (plug compatible with Cisco 1000/1600/2500/2600 series
console ports)
– Asynchronous serial DTE
– Transmit/receive rates up to 115.2 kbps (default
9600 bps, not a network data port)
– No hardware handshaking such as RTS/CTS
• One internal expansion slot for support of hardware-assisted
services such as encryption (up to T1/E1)
Processor
• Motorola MPC860T PowerQUICC at 48 MHz
DRAM and Flash Memory
• Run from RAM architecture
• DRAM
– Onboard (fixed/default): 32 MB
– One DIMM slot
– Maximum DRAM: 48 MB
• Flash
– Type: onboard (socketed) mini-Flash card
– Default: 8 MB
– Available sizes: 16 MB
– Maximum Flash: 16 MB
– Support dual Flash bank
Dimensions
• Width: 11.2 in.(28.4 cm)

• Height: 3.1 in. (7.85 cm)
• Depth: 8.7 in. (22.1 cm)
• Weight (minimum): 2.6 lb (1.18 kg)
• Weight (maximum): 2.9 lb (1.32 kg)
Power
• Locking connector on power socket
• AC input voltage: 100 to 240 VAC
• Frequency: 47 to 64 Hz
• AC input current: 0.5 amps
• Power dissipation: 20W (maximum)
Environmental
• Operating temperature: 32 to 104 F (0 to 40 C)
• Nonoperating temperature: –4 to 149 F (–20 to 65 C)
• Relative humidity: 10 to 85% noncondensing
operating; 5 to 95% noncondensing, nonoperating
Safety
• UL 1950
• CSA 22.2—No. 950
• EN60950
• EN41003
• AUSTEL TS001
• AS/NZS 3260
• ETSI 300-047
• BS 6301 (power supply)
EMI
• AS/NRZ 3548 Class A
• Class B
• FCC Part 15 Class B
• EN60555-2 Class B
• EN55022 Class B
• VCCI Class II
• CISPR-22 Class B
Immunity
• 55082-1 Generic Immunity Specification Part 1:
Residential and Light Industry
• IEC 1000-4-2 (EN61000-4-2)
• IEC 1000-4-3 (ENV50140)
• IEC 1000-4-4 (EN61000-4-4)
• IEC 1000-4-5 (EN61000-4-5)
• IEC 1000-4-6 (ENV50141)
• IEC 1000-4-11
• IEC 1000-3-2
Network Homologation
• Europe: CTR2, CTR3
• Canada: CS-03
• Unites States: FCC Part 68
• Japan: Jate NTT
• Australia/New Zealand: TS013/TS-031
• Hong Kong: CR22

Cisco 2610

The Cisco 2600 Series provides unparalleled flexibility

and port density options for branch offices. The following
table highlights a few of the Cisco 2600 configuration
possibilities:

Simultaneous Voice Calls (digital/analog) 60/4
T1/E1 Connections (including ATM) 8
Integrated Modems 16
ISDN PRI (B channels) 64
ISDN BRI 10
Asynchronous Serial 37
Synchronous Serial 12

• Main Processor: 80 MHz RISC (Cisco 265x); 50 MHz
RISC (Cisco 262x); 40 MHz RISC (Cisco 261x)
• Flash Memory: 8 to 16MB (Cisco 261x); 8 to 32MB
(Cisco 262x 1 and Cisco 265x only)
• System Memory (DRAM): 32 to 64MB (Cisco 261x
and Cisco 262x); 32 to 128MB (Cisco 265x only,
uses SDRAM)
• WAN Interface Card Slots: 2
• Network Module Slot: 1
• AIM Slot: 1
• Console/Aux Speed: 115.2 Kbps (maximum)
• Width: 17.5 in. (44.5 cm)
• Height: 1.69 in. (4.3 cm)
• Depth: 11.8 in. (30 cm)
• Weight (min): 8.85 lb (4.02 kg)
• Weight (max): 10.25 lb (4.66 kg)
• Power Dissipation: 72W (maximum)
• AC Input Voltage: 100 to 240 VAC
• Frequency: 47 to 64 Hz
• AC Input Current: 1.5 amps
• DC Input Voltage: -38V to -60V (UL label)
• DC Input Current: 2 amps
• Operating Temperature: 32 to 104 F (0 to 40 C)
• Non-operating Temperature: -13 to 158 F(-25 to 70 C)

• Relative Humidity: 5 to 95% non-condensing
• Noise Level (min): 38-dbA
• Noise Level (max): 42-dbA
The Cisco 2600 Series conforms to a number of safety,

EMI, immunity, and network homologation standards.
Details can be obtained through your Cisco reseller or
account manager.

Equipo principal (core:)

Cisco 3640

Processor Type 100-MHz IDT R4700
Flash Memory 4 MB, upgradable to 32 MB
System Memory 32 MB DRAM, upgradable to 128 MB DRAM
Network Module Slots Four slots
Power AC, DC, Redundant Power Option
Dimensions 17.5-in. width x 3.44-in. height x 15.75-in. depth
Performance 50-70 kpps
Console and Auxiliary Ports (up to 115.2 kbps)
Yes
Rack and Wall Mounting Yes
Dual Type II PC Card Slots Yes

Power Requirements
Regulatory Compliance
The Cisco 3600 series conforms to a number of different
safety, EMI, immunity and network homologation
standards. Details of the regulatory specifications are
included at
http://www.cisco.com/public/Support_root.shtml
For More Information, Contact:
U.S. and Canada: 800 GO CISCO (462-4726)

Europe: 32 2 778 4242
Australia: 61 2 9935 4107
Other: 408 526-7209
Or contact your local Cisco office
World Wide Web URL: http://www.cisco.com

Width 17.5 in (44.5 cm)
Height 3.44 in (8.7 cm)
Depth 15.75 in (40.0 cm)
Weight (minimum) 18 lb (8.18 kg)
Weight (maximum) 23 lb (10.5 kg)

Output, Watts 140W Max
AC Input Voltage 100 to 240 VAC
Frequency 47 to 64 Hz
AC Input Current 2 Amps
DC Input Voltage -38V to -75V
DC Input Current 5 Amps

Operating Temperature 32 to 104 F
(0 to 40 C)
Nonoperating Temperature
-13 to 158 F
(-25 to 70 C)

Relative Humidity 5 to 95%
Noise Level (Maximum) 45 dbA

Interfaces:

NM2V

NM-2V Two voice/fax interface card slot network module
Cisco IOS Requirement 11.3(1)T or later for Cisco 3600
11.3(4)T or later for Cisco 2600
Cisco Part Number 800-02491-01
FCC Specifications FCC Class B device
Spare NM-2V=
MTBF 755,717 hours
Requires at Least One VIC (maximum of two) VIC-2FXS 800-02493-01
VIC-2DID 800-06487-01
VIC-2E/M 800-02497-01

VIC-2FXO-M1 800-05298-01
VIC-2FXO-M2 800-05920-01
VIC-2FXO 800-02495-01
VIC-2FXO-M3 800-04581-01
VIC-2FXO-EU 800-03639-01
VIC-2BRI-S/T-TE 800-03803-1
VIC-2BRI-NT/TE

FXS

VIC-2FXS Two-port FXS voice/fax interface card
Interface Type Foreign exchange station
Cisco IOS Requirement 11.3(1)T or later for Cisco 3600
11.3(4)T or later for Cisco 2600
Cisco Part Number 800-02493-01
Compliance FCC Class B device, CE
Safety Conformance UL1950
Spare VIC-2FXS=
Address Signaling Formats In-band DTMF
Out-of-band pulse (10/20 pps)
Signaling Formats Loop start, ground start
Ringing Tone Configurable for different country requirements
Ringing Voltage <45 Vrms at 5 REN at 25 Hz (configurable frequency)
Ringing Frequencies 20 Hz, 50 Hz
Physical Connector RJ-11
Number of Connectors/Ports Two
MTBF 2,248,909 hours

E1/T1 troncal digital

Voice Feature Support
- Private line automatic ring-down (PLAR)
- Local Voice Busy-Out (LVBO)
- Connection trunk
- PBX tie-line replacement
- Answer-address, incoming-called-number on dial-peers
- Echo cancellation (up to 32 ms configurable)
- Silence suppression, voice activity detection (VAD)
- Comfort noise generation
- Hunt groups across cards
- Integrated add/drop multiplexer (drop and insert)
- LED indicators for voice processing resources and port status

Telephony Interface Signaling Support
- T1 and E1 PRI Q.931 user side and network side (NET5)
- T1 and E1 CAS
- T1 and E1 PRI QSIG
- E1 MelCAS
- E1 R2 CAS
- T1 and E1 Transparent CCS (with Multi-D channel)
- E&M (wink, immediate, delay), FXO/FXS loop-start and ground-start signaling
- Inbound signaling (such as DTMF, MF support)

Cisco IOS and Platform Support
- Fully supported via IOS CLI including device configuration, monitoring, link status, security, Layer 2 and 3 protocol configuration and management, and call history
- MPLS support
- Supported on all Cisco 3600 and 2600 series routers

Standards Support
- H.323 version 1 and 2 feature support
- H.323 CODEC-negotiation
- H.323 gateway RAS support (version 1 / version 2)
- Supports ITU Standard Compression Algorithms (G.729, G.723.1, G.729a/b, G.711, G.728, G.726)

Country Support
• World-wide country support
Traditional Circuit Switched PBX Support
• Qualified PBX interoperability for Lucent Definity series, Nortel Meridian, and ROLM/Siemens HICOM, NEC NEAX 2400, Toshiba Strada DK424, Mitel 2000SX, Ericsson, Nortel SL-1 (other PBXs continue to be certified)

Network Management Support
• SNMP protocol compliant
• Manageable via a MIB browser
• CiscoView interface for configuration
• ConfigMaker
• Cisco Voice Manager (CVM) supported, version 2.0
• NetSys supported

Seriales:

Dimensions (H x W x D)
1.55 x 7.10 x 7.2 1.55 x 7.10 x 7.2 1.55 x 7.10 x 7.2 1.55 x 7.10 x 7.2 1.55 x 7.10 x 7.2
Weight 2 lbs. Max 2 lbs. Max 2 lbs. Max 2 lbs. Max 2 lbs. Max
Environmental Conditions
Op. temp. 32–104 F (0–40 C), Non. Op temp -13–158 F (-2– 70 C) Op. temp. 32–104 F (0–40 C), Non. Op temp -13–158 F (-2– 70 C) Op. temp. 32–104 F (0–40 C), Non. Op temp -13–158 F (-2– 70 C) Op. temp. 32–104 F (0–40 C), Non. Op temp -13–158 F (-2– 70 C)
Relative Humidity 5-95% 5-95% 5-95% 5-95% 5-95%
EMI Class B EMI Class B EMI Class B EMI Class B EMI

Equipos de distribución:

Catalyst 2912/24 XL

Technical Specifications
• Performance
– 3.2 Gbps switching fabric
– 3.0 million-pps forwarding rate for 64-byte packets
– 1.6 Gbps maximum forwarding bandwidth
– 4-MB shared-memory architecture shared by all ports
– Packet forwarding rate for 64-byte packets:
– 14,880 pps to 10-Mbps ports
– 148,800 pps to 100BaseT ports
– 8-MB DRAM and 4 MB Flash memory
– 2048 MAC addresses
• Management
– SNMP Management Information Base (MIB) II, SNMP MIB extensions, Bridging MIB (RFC 1493)
• Standards
– IEEE 802.3x full duplex on 10BaseT and 100BaseT ports
– IEEE 802.1D Spanning-Tree Protocol
– IEEE 802.3u 100BaseTX and 100BaseFX specification
– IEEE 802.3 10BaseT specification
• Connectors and Cabling
– 10Base-T ports: RJ-45 connectors; two-pair category 3, 4, or 5 unshielded twisted-pair (UTP) cabling
– 100Base-TX ports: RJ-45 connectors; two-pair Category 5 UTP cabling
– 100Base-FX ports: SC connector, 50/125- and 62.5/125-micron multimode, fiber-optic cabling (Catalyst2924C XL)
– Management console port: RJ-45 connector
• Indicators
– Per-port status LEDs—link integrity, disabled, activity, speed, and full-duplex indications
– System status LEDs—system, RPS, and bandwidth utilization indications
• Dimensions and Weight (H x W x D)
– 1.73 x 17.5 x 9.79 in. (4.4 x 44.5 x 24.8 cm)
– 1 rack unit (RU) high
– 7 lb. (3.2 kg)
• Environmental Conditions and Power Requirements
– Operating temperature: 32 to 122 F (0 to 50 C)
– Storage temperature: –4 to 149 F (–20 to 65 C)
– Operating relative humidity: 10 to 85% noncondensing
– Operating altitude: Up to 10,000 ft. (3000 m)
– Power consumption: 70W maximum; 239 BTU per hour

– AC input voltage/frequency: 100 to 120/200 to 240 VAC (autoranging) 50 to 60 Hz
– MTBF 180,995 hours
• Safety Certifications
– UL 1950
– CSA 22.2 No. 950
– EN 60950
– IEC 950
– AS/NZS 3260, TS001
– CE
• Electromagnetic Emissions Certifications
– FCC Part 15 Class A
– EN 55022B Class A (CISPR 22 Class A)
– VCCI Class A
– AS/NZS 3548 Class A
– BCIQ
– CE Marking
• Warranty
– Lifetime limited warranty
• Ordering Information

Model Numbers
– WS-C2912-XL-EN (12-port, Enterprise Edition)
– WS-C2924-XL-EN (24-port, Enterprise Edition)
– WS-C2924-XL-EN-5P (24-port, Enterprise Edition,
Five-Pack)
– WS-C2924C-XL-EN (22 TX + 2 FX-port, Enterprise
Edition)
– WS-C2924C-XL-EN-5P (22 TX + 2 FX-port, Enterprise Edition, Five-Pack)
For more information on Cisco products, contact:
U.S. and Canada: 800 553-NETS (6387)
Europe: 32 2 778 4242
Australia: 612 9935 4107
Other: 408 526-7209
World Wide Web URL: http://www.cisco.com

Catalyst 3512/24 XL

Performance
• 10.8-Gbps switching fabric
• 4.8 Mpps wire-speed forwarding rate for 64-byte packets (Catalyst 3512 XL), 6.5 million pps wire-speed forwarding rate for 64-byte packets (Catalyst 3524 XL), 8.0 Mpps forwarding rate for 64-byte packets (Catalyst 3548 XL)
• 5.4-Gbps maximum forwarding bandwidth
• 4 MB memory architecture shared by all ports
• 8 MB DRAM (Catalyst 3512 XL and 3524 XL) and
4 MB Flash memory
• 16 MB DRAM (Catalyst 3548 XL) and 4 MB Flash memory
• 8192 MAC addresses
Management
• SNMP Management Information Base (MIB) II, SNMP
MIB extensions, Bridging MIB (RFC 1493)
Connectors and Cabling
• 10Base-T ports: RJ-45 connectors; two-pair Category 3,
4, or 5 unshielded twisted-pair (UTP) cabling
• 100Base-TX ports: RJ-45 connectors; two-pair
Category 5 UTP cabling
• 1000BASE-T GBIC ports: RJ-45 connectors; two-pair
Category 5 UTP cabling
• 1000Base-SX,-LX/LH and -ZX GBIC ports: SC fiber connectors, single mode or multimode fiber
• GigaStack GBIC ports: copper-based Cisco GigaStack
cabling
• Management console port: RJ-45 connector, RS-232
serial cabling
Indicators
• Per-port status LEDs—link integrity, disabled, activity,
speed, and full-duplex indications
• System status LEDs—system, RPS, and bandwidth
utilization indications
Dimensions and Weight (H x W x D)
• 1.75 x 17.5 x 11.8 in. (4.4 x 44.5 x 30 cm) (Catalyst 3512 XL and 3524 XL)
• 1.75 x 17.5 x 15.3 in. (4.4 x 44.5 x 39 cm) (Catalyst 3548 XL)
• One rack-unit (RU) high
• 10.25 lb (4.6 kg) (Catalyst 3512 XL and 3524 XL)
• 11 lb (5.01 kg) (Catalyst 3548 XL)
Environmental Conditions and Power Requirements
• Operating temperature: 32 to 113 F (0 to 45 C)
• Storage temperature: –13 to 158 F (–25 to 70 C)
• Operating relative humidity: 10 to 85% noncondensing
• Operating altitude: Up to 10,000 ft (3000 m)

• Power consumption: 70W maximum (Catalyst 3512 XL and 3524 XL); 100W maximum (Catalyst 3548 XL); 239 BTU per hour (Catalyst 3512 XL and 3524 XL); 600 BTU per hour (Catalyst 3548 XL)
• AC input voltage/frequency: 100 to 120/200 to 240 VAC (autoranging) 50 to 60 Hz
• MTBF 150,000 hours (Catalyst 3512 and 3524 XL)
• MTBF 135,000 hours (Catalyst 3548 XL)

Safety Certifications

• UL 1950
• CSA 22.2 No. 950
• EN 60950
• IEC 950
• AS/NZS 3260, TS001
• CE Marking
• TUV

Electromagnetic Emissions Certifications

• FCC Part 15 Class A
• EN 55022b Class A (CISPR 22 Class A)
• VCCI Class A
• AS/NZS 3548 Class A
• BCIQ
• CE Marking

Warranty

• Lifetime limited warranty

Ordering Information

Model Numbers

• WS-C3512-XL-EN (12-port 10/100 + two-port 1000Base-X, Enterprise Edition)
• WS-C3524-XL-EN (24-port 10/100 + two-port 1000Base-X, Enterprise Edition)
• WS-C3548-XL-EN (48-port 10/100 +two port 1000Base-X, Enterprise Edition)

For More Information on Cisco Products, Contact:

• US and Canada: 800 553-NETS (6387)
• Europe: 32 2 778 4242
• Australia: 612 9935 4107
• Other: 408 526-7209
• World Wide Web URL: http://www.cisco.com

Equipo de seguridad:

PIX 515

*Fail-over requires special Cisco cable
Random Access Memory 32 MB
Flash Memory 16 MB
Console Port RJ-45
Boot/Update Device TFTP
Failover Port* Disabled DB-25 EIA/TIA-232
Physical Dimensions
Height 1.72 in.
Width 16.82 in.
Depth 11.8 in.
Weight 11 lb.
Power Requirements
Autoswitching 100–240 VAC
Frequency 50–60 Hz
Current 1.5–0.75 amps
Operating Environment
Operating Temperature –5 to +45°C (–25 to 113°F)
Nonoperational Temperature –25 to +70°C
Operational Humidity 95% relative humidity (RH)
Operational Altitude 3000m (9843 feet), 25°C (77°F)
Nonoperational Altitude 4570m (15,000 feet), 25°C (77°F)
Operational Shock 1.88 m/sec (74 in./sec) 1/2 sine input
Nonoperational Shock 60G 11 ms 1/2 sine input
Operational Vibration 0.41 Grms2 (5–500 Hz) random input
Nonoperational Vibration 0.41 Grms2 (5–500 Hz) random input
Heat Dissipation (worst case with full power usage) 160.37 BTU/hr
EMI CE, VCCI class II, FCC, BCIQ, Austel CE, VCCI
Safety Agencies UL, C-UL, TUV, IEC 950
UL-1950 Standard 3rd edition
TUV EN 60950 2nd edition, Am.1-4
IEC-950/VDE-0805 EN-60-950 Standard Yes
Bellcore No

PIX Firewall 515-R PIX Firewall 515-UR

APÉNDICE D

SDH
Synchronous Digital Hierarchy

SDH es una alternativa de evolución de las redes de transporte, que nace debido al acelerado crecimiento de las actuales redes de transmisión, demanda de nuevos servicios y aparición de nuevos operadores de red, satisface las exigencias de flexibilidad y calidad que requiere un mercado que esta continuamente en cambio. Además de esto, SDH beneficia también a las empresas operadoras en cuanto a la optimización de su rentabilidad, reducción de costos de operación y mantenimiento y facilidad de supervisión.

Ofrece características como:

- Nuevas topologías de red especialmente en la parte de acceso.

- Acceso directo a afluentes de baja velocidad sin tener que demultiplexar toda la señal que viene a alta velocidad, como ocurre con la PDH actual.

- Facilidad de multiplexación y demultiplexación.

- Mejor capacidad de operación, administración y mantenimiento.

- Adopción de canales auxiliares estandarizados.

- Estandarización de interfaces.

- Fácil crecimiento hacia velocidades mayores, en la medida que lo requiera la red.

- Implementación de sistemas con estructura flexible que pueden ser utilizados para construir nuevas redes (incluyendo LAN, MAN, ISDN).
La SDH nace como una solución a la PDH, por esto haremos una breve descripción de esta ultima antes de entrar en materia.

JERARQUÍA DIGITAL PLESIOCRONA (PDH, Plesiocronous Digital Hierarqui).

El CCITT es el encargado de establecer las recomendaciones necesarias para cualquier tecnología de telecomunicaciones. Actualmente existen en el mundo dos PDH's definidas por el CCITT que son: la Europea basada en la velocidad primaria de 2048 Kbits/s. y la Americana (utilizada en U.S.A y Japón) basada en la velocidad primaria de 1544 Kbits/s, ambas obtenidas por la multiplexación síncrona de trenes básicos de 64Kbits/s (32 y 24 canales respectivamente). Cada una de estas jerarquías exige en cuanto a sincronización una correcta temporización en ambos extremos para demultiplexar adecuadamente las señales.

DESVENTAJAS DE LA PDH:

-La estructura de trama de las centrales hecha por entrelazamiento de octetos a 64 Kbits/s. es síncrona, por tanto el empleo de la justificación para adoptar temporización se vuelve innecesario.

- El entrelazamiento de bits hace que canales a 64 Kbits/s. pertenecientes a un tramo de trafico solo se puedan bifurcar hasta que se demultiplexa a nivel de multiplex primario.

- Los canales de n 64Kbits/s que no se puedan incluir bajo el multiplex primario no se pueden tramitar de ninguna otra forma por la red.

- La información de mantenimiento no esta asociada a vías completas de trafico, sino a enlaces individuales, por lo cual el procedimiento de mantenimiento para una vía completa es complicado.

SINCRONIZACIÓN.

En todo sistema de transmisión digital, la sincronización debe garantizarse en tres niveles diferentes; para transmisión de datos estos niveles son bit, carácter y mensaje. Para transmisión PCM (Modulación de Pulsos Codificados) los niveles son: bit, intervalo de tiempo y trama.

Para transmisión de datos existen 2 técnicas de enfrentar la sincronización : Transmisión asíncrona: Cuando los datos viajan por el canal sin una velocidad fija, es decir que el tiempo que transcurre desde la transmisión de un dato, hasta la transmisión del próximo dato es variable.

Transmisión síncrona: En este caso los datos son transmitidos a una velocidad fija de bits, por una línea que mantiene viva aun cuando no se esté enviando información. En los sistemas PCM la transmisión es siempre síncrona pues el receptor deriva su propia temporización de la señal entrante, mientras los alineamientos de intervalo y de trama se obtienen utilizando un formato predeterminado.

En general se puede decir que muchas de las ventajas de una red digital de telecomunicaciones , son solo factibles en una arquitectura de red síncrona. Sin embargo es difícil que todas las temporizaciones de la red tengan la misma frecuencia instantánea.

DESCRIPCIÓN DE LA SDH.

La existencia de diversas jerarquías digitales (la Europea y la Americana), hacen que cuando el trafico sobrepasa las fronteras nacionales, haya necesidad de efectuar conversiones generalmente costosas para llevar la señal a otro país. Esto y las desventajas de la PDH actual que nombramos anteriormente forzaron a crear una jerarquía digital que proporcionara un estándar mundial unificado que a su vez ayude a que la administración de la red sea mas efectiva y económica. Además satisface las demandas de nuevos servicios y mas capacidad de transmisión, por parte de los usuarios. Aparte de ser un estándar mundial y ofrecer un método de múltiplex ación síncrona, SDH involucra un concepto muy importante : el de red estratificada en capas (tema que trataremos mas adelante), por ahora estudiaremos la SDH en su estructura básica.

ESTRUCTURA BÁSICA DE SDH

SDH trabaja con una estructura básica según lo define la CCITT. Esta estructura es llamada trama básica, la cual tiene una duración de 125 microsegundos, y corresponde a una matriz de 9 filas y 270 columnas, cuyos elementos son octetos de 8 bits; por lo tanto la trama tendrá:

y como su duración es de 125 microsegundos, o sea que se repite 8000 veces por segundo, su velocidad binaria será:

19940*8000 = 155520 Kbits/seg

Esta trama básica recibe el nombre de STM_1 " Modulo de Transporte Síncrono de Nivel 1" (STM_1 = Synchronous Transport Module 1).

En la trama se distinguen tres áreas:

1. Tara de Sección (Section OverHeat).
2. Punteros de AU (AU pointer).
3. Carga Útil (Pail Load).

CONTENEDOR VIRTUAL (VC).

Para que un tributario pueda entrar a formar parte de la carga útil de un STM_1! previamente debe ser " empacado adecuadamente, para ello se procesa con el fin de convertirlo en un contenedor virtual (VC: Virtual Container). Este VC es una señal síncrona en frecuencia con el STM_1 y ocupara un determinado lugar entre la sección de carga útil de la trama.

VELOCIDADES BINARIAS EN SDH.

Las velocidades de bit para los niveles mas altos de las jerarquías SDH van de acuerdo al nivel N del Modulo de Transporte Síncrono (STM). Según la recomendación g.707 del CCITT estas velocidades son:

Nivel	Señal	Velocidad	Velocidad Real
1	STM_1	155.520 x 1	1555.520 Mbits/s
4	STM_4	155.520 x 4	622.080 Mbits/s
16	STM_16	155.520 x 16	2.488.320 Mbits/s

A diferencia de la jerarquía digital plesiocrona, aquí la velocidad del STM_N se obtiene multiplicando la velocidad del modulo básico STM_1, por N, donde N es un entero.

TÉCNICA DE PUNTEROS.

En la red síncrona todos los nodos y multiplexores SDH están controlados por un reloj muy estable. Sin embargo pueden surgir perdidas de sincronismo en alguna parte de la red o puede ser necesario efectuar algún ajuste en los puntos donde el trafico traspasa las fronteras nacionales. Esta tarea de ajustar el sincronismo, se realiza mediante los punteros. Estos indican la posición en que comienza una carga útil. Como cada octeto de una trama STM, tiene un numero que lo

identifica, el puntero indica uno de tale s números, y es donde se encontrara el primer octeto de la carga útil asociada a dicho puntero. De esta forma la carga útil puede por así decirlo "flotar" en una trama STM, pues siempre su posición estará indicada por el puntero.

SDH: RED ESTRUCTURADA EN CAPAS

Una red basada en SDH proporciona los medios para transportar los contenedores entre diversos puntos, para cargar y descargar contenedores de los STM_1 y para transferir contenedores de un medio De transporte a otro (STM_N) .Estas acciones determinan las funciones básicas que se deben realizar en una red SDH. En los puntos de acceso a la red se ensamblan los v/c adecuados a la señal a transmitir, una vez conformado el vc debe ser transportado a través de la red, durante el viaje del vc por la red SDH puede presentarse el caso en que un v/c o varios deben ser descargados del STM_1 o también casos en que deban ser cargados en los STM_1. En su recorrido por la red, el vc pasara por diferentes rutas y con diferentes velocidades .

EQUIPOS PARA SDH

Los equipos necesarios en una red SDH son los siguientes:

•Multiplexor Terminal.
•Multiplexor Add-Drop.
•Multiplexor Cross-Connet.

La función del multiplexor terminal es combinar las funciones de interfaz, ensamblado y desensamblado de los diversos paquetes.

El cross-connect realiza el enrutamiento del trafico entre nodos de la red y se puede clasificar de acuerdo al tipo de vc que intercambie y al nivel jerárquico de las señales. Se pueden clasificar en 3 tipos: los que realizan intercambio a nivel VC-4 o a nivel superior, los que realizan intercambio a nivel del v/c de orden inferior y los que son combinaciones de los anteriores.

GESTIÓN SDH.

La SDH es la primera tecnología que incluye dentro de las normas que la soportan, algunas dedicadas a especificar las facilidades de gestión bajo las directrices de la TMN (*telecomunication management network*). La TMN se concibe como una red superpuesta a la red de telecomunicaciones, que interactúa con ella a través de interfaces normalizadas en ciertos puntos y obtiene información que le permite monitorear y controlar su operación. Su objetivo es dar soporte par a gestión a los operadores de la red.

A continuación se muestra una organización de las normas del CCITT sobre SDH:

•ESTÁNDARES SDH G.707-G.708-G.709 •ARQUITECTURA DE RED: G.803 (Arq. Redes) G.804 •EQUIPOS G.781,G.782,G.783(mux) G.987 (INTER.OPTICAS) G.958 (SIST.DE

LINEA) G.SDX 1,2,3(Cross-connet) Reg.750(Arq.sistemas radio) •GESTIÓN DE RED DE RED M.3010 G.803(arq.redes) G.773(Int.Q) G.804 G.774(Modelo inform)

RED DE GESTIÓN SDH

Los aspectos de gestión de la red SDH, se tratan básicamente en la REC G de la UIT. En el modelo de organización de gestión se distinguen 2 componentes principales:

- Sistemas de operaciones o dispositivos de mediación SO/DM.
- Elementos de red ER.

La diferencia entre estos dos componentes radica en el tipo de función que soportan. Los SO/MO realizan funciones del sistema de operaciones: procesar la información, controlar las funciones de gestión dentro de las cuales hay funciones básicas, funciones de red y funciones de servicio. Realizan funciones de mediación que garantizan la comunicación entre el SO y el ER como control de las comunicaciones, conversión de protocolos, manejo de datos, transferencia de primitivas. Los ER realizan funciones de elemento de red sustentando los servicios de transporte de red basados en SDH, como multicanalizacion, regeneración, transconexion. Se comunican con el SO a fin de ser supervisados y controlados.

- Universidad del Valle
- Escuela de Electricidad y Electrónica
- Cátedra De Comunicaciones
- Curso Redes de Comunicación

Bibliografía

1. Minoli, Daniel;Minoli, Ema, *"Delivering Voice over IP Networks"*, Wiley Computer Publishing 1998
2. Thomsen, Guy; Jani, Yashvant; *"Internet telephony: going like crazy"*, IEEE Spectrum Magazine Mayo 2000.
3. Higginbottom, Gary N. *"Performance Evaluation of Communication Networks"*,. Artech House Inc, 1998
4. *"Internet Protocol Data Communication Service – IP Packet Transfer and Availability Performance Parameters"*, Draft New ITU-T Recommendation I.380.
5. Raman, Lakshmi; *"OSI Systems and Network Management"*. IEEE Communications Magazine, Marzo de 1998.
6. Stallings, William; *"Comunicaciones y Redes de Computadores"*. Prentice Hall 1997.
7. Divakara, Udupa; *"TMN : Telecommunications Management Network. McGraw-Hill"*, 1999
8. *"Internet Protocol Data Communication Service – IP Packet Transfer and Availability Performance Parameters"*, Draft New ITU-T Recommendation I.380.
9. Wyatt, Allén; *"Aprendiendo Windows NT Server 4.0"*; Prentice Hall, 1998
10. Comer, Douglas E.; *"Redes globales de información con Internet y TCP/IP"*; Prentice Hall, 3ª. Edición, 1998
11. Currid, Cerril C.; Gillet, Craig A.; *"Domine Novell Netware"*; Macrobit, 1991
12. Stoltz, Kevin; *"Todo acerca de... Redes Computación"*;Prentice Hall, 1995
13. Lowe, Doug; *"Redes para Dummies"*; Grupo Editorial Norma, 2ª Edición, 1997
14. Comer, Douglas E.; *"Redes de computadoras, Internet e Interresdes"*; Prentice Hall, 1997
15. Peterson, L.; Dacie, B.; *"Computer Networks: A Systems Aproach"*; Morgan Kaufmann Publishers, inc; 1996