UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
"CAMPUS ARAGÓN"

"PROPUESTA DE CONECTIVIDAD REMOTA PRIVADA PARA COMUNICACIÓN ENTRE EMPRESAS Y EMPLEADOS"

T E S I S

QUE PARA OBTENER EL TÍTULO DE INGENIERO MECANICO ELECTRICISTA
P R E S E N T A :
RAMIRO MARTINEZ ESPINOSA

ASESOR: M. EN C. EDGAR BALDEMAR AGUADO CRUZ

SAN JUAN DE ARAGÓN, ESTADO DE MÉXICO 2003

VNIVERSIDAD NACIONAL AVPNOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGÓN
DIRECCIÓN

RAMIRO MARTINEZ ESPINOSA
P r e s e n t e

Con fundamento en el punto 6 y siguientes, del Reglamento para Exámenes Profesionales en esta Escuela, y toda vez que la documentación presentada por usted reúne los requisitos que establece el precitado Reglamento; me permito comunicarle que ha sido aprobado su tema de tesis y asesor.

TÍTULO:
"PROPUESTA DE CONECTIVIDAD REMOTA PRIVADA PARA COMUNICACIÓN ENTRE EMPRESAS Y EMPLEADOS"

ASESOR: M. en C. EDGAR BALDEMAR AGUADO CRUZ

Aprovecho la ocasión para reiterarle mi distinguida consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 1 de julio de 2003.

LA DIRECTORA

ARQ. LILIA TURCOTT GONZÁLEZ

U.N.A.M. ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGON
DIRECCION

C p Secretaria Académica
C p Jefatura de Carrera de Ingeniería Mecánica Eléctrica
C p Asesor de Tesis

LTG/AIR/lla

VNIVERSIDAD NACIONAL AVFNOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN – UNAM

JEFATURA DE CARRERA DE INGENIERÍA MECÁNICA ELÉCTRICA

OFICIO: ENAR/JAME/1078/2003.

ASUNTO: Sínodo

LIC. ALBERTO IBARRA ROSAS
SECRETARIO ACADÉMICO
P R E S E N T E

Por este conducto me permito relacionar los nombres de los Profesores que sugiero integren el Sínodo del Examen Profesional del alumno: **RAMIRO MARTÍNEZ ESPINOSA,** con Número de Cuenta: **09237867-4,** con el tema de tesis: **"PROPUESTA DE CONECTIVIDAD REMOTA PRIVADA PARA COMUNICACIÓN ENTRE EMPRESAS Y EMPLEADOS".**

PRESIDENTE:	**ING. RAÚL BARRÓN VERA**	**OCTUBRE**	**78**
VOCAL:	**ING. ELEAZAR MARGARITO PINEDA DÍAZ**	**OCTUBRE**	**80**
SECRETARIO:	**ING. ADRIÁN PAREDES ROMERO**	**MAYO**	**90**
SUPLENTE:	**M. en C. EDGAR BALDEMAR AGUADO CRUZ**	**MARZO**	**94**
SUPLENTE:	**ING. PRÓCORO PABLO LUNA ESCORZA**	**ENERO**	**96**

Quiero subrayar que el Director de Tesis es el M. en C. Edgar Baldemar Aguado Cruz, quien esta incluido basándose en lo que reza el Reglamento de Exámenes Profesionales de esta Escuela.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Bosques de Aragón, Estado de México, 21 de noviembre de 2003.
EL JEFE DE CARRERA

ING. RAÚL BARRÓN VERA

C.c.p.- Lic. Ma. Teresa Luna Sánchez.- Jefa del Depto. de Servicios Escolares.
C.c.p.- M. en C. Edgar Baldemar Aguado Cruz.- Asesor de Tesis.
C.c.p.- Alumno.
RBVamce.

AGRADECIMIENTOS:

A mi Padre:

Por su gran Apoyo, Fortaleza y Sabiduría. Eres un gran hombre, Papá.

A mi Madre:

Por su Paciencia, Fe y Comprensión que siempre me brinda. Eres una mujer ejemplar, Mamá.

A mis Hermanos:

Juan Manuel, Adán, Víctor Hugo y Guadalupe Isabel por su gran apoyo incondicional que me han brindado en todas las situaciones difíciles y complicadas en mi vida. Son unos Hermanos incomparables.

Gracias a mi familia por su entrega, amor, paciencia y cariño que me han dado a lo largo de mi vida y sobre todo por esa gran fe que siempre han depositado en mí. Sin el apoyo de ustedes no lo hubiera logrado. Los quiero mucho.

A Dios:

Por estar siempre a mi lado en los momentos más complicados y difíciles, ayudándome a no decaer y dándome fortaleza para continuar...

A mis Amigos:

Con quienes compartí grandes experiencias y momentos inolvidables, gracias por su gran amistad.

Por último, también quiero agradecer a esas personas que de alguna manera han formado parte de mi ser y que me han acompañado en las diferentes etapas de mi vida dejándome gratos recuerdos.

ÍNDICE

CAPÍTULO 1
INTRODUCCIÓN

CAPÍTULO 2
ANTECEDENTES

CAPÍTULO 3
GENERALIDADES DE TELECOMUNICACIONES

CAPÍTULO 4
CONCEPTOS BÁSICOS DE REDES

CAPÍTULO 5
CONECTIVIDAD Y SEGURIDAD

CAPÍTULO 6
REQUERIMIENTOS MÍNIMOS PARA LA CONEXIÓN REMOTA.

CAPÍTULO 7
DISEÑO DE LA RED PRIVADA

CAPÍTULO 1

INTRODUCCIÓN

1.1 PROBLEMÁTICA

La compañía TESYS S.A. DE C.V. (Tecnología en Soluciones y Sistemas S.A. de C.V) ofrece servicios de diseño y desarrollo de sistemas de cómputo, servicio y mantenimiento a estos sistemas y la renta de recursos con habilidades especificas por función y tiempo. Debido al tipo de servicios que ofrece esta compañía, hoy en día, un gran número de sus empleados realizan la mayoría de sus actividades desde las instalaciones mismas del cliente, ya sea porque sus tareas así lo requieren o por que el cliente así lo prefiere. Aun así estos empleados deben presentarse muy seguido en las instalaciones principales de la compañía a entregar personalmente sus reportes de actividades y avance, reportes de horas de trabajo, cambios en los requerimientos, revisiones de propuestas y todo lo relacionado con recursos humanos tales como solicitud de vacaciones, actualización de datos personales, etc. Esto implica que estos empleados trabajen sus ocho horas con el cliente, ocupen una o más horas en transportarse a las instalaciones de la compañía y que en algunos casos tengan que esperar a que se desocupe un equipo de trabajo para poder realizar dichas actividades administrativas, lo cual provoca grandes perdidas de tiempo de los empleados, inconformidad, y lentitud en las actividades administrativas, llegando incluso algunas veces a perder algunas opciones de negocios debido a la lentitud con que se genera y se presenta una propuesta de solución.
Del mismo modo aún y cuando las oficinas principales de TESYS se encuentran en la Ciudad de México, algunos de sus clientes tienen oficinas e instalaciones también en el interior de la República, lo cual, por las circunstancias antes mencionadas provoca una gran cantidad de viajes a los empleados que estén atendiendo a estos clientes en específico, así por ejemplo, un empleado debe trabajar de lunes a jueves en las instalaciones del cliente en provincia y utilizar el viernes para viajar a la ciudad de México, presentarse a la oficina y presentar todos los documentos correspondientes a su trabajo y facturación, para que se pueda realizar el cobro correspondiente, se revisen y en dado caso se aprueben los cambios a las propuestas o contratos que se tengan con este cliente, así mismo este tipo de empleados deben presentarse en las oficinas principales en la Ciudad de México cada ves que tengan necesidad de realizar algún tramite con recursos humanos tales como solicitud de vacaciones, pago de viáticos, etc. Por las razones antes mencionadas TESYS ha considerado la idea de eliminar todos estos clientes de provincia, lo cual resulta inconveniente ya que esto implicaría la perdida de los negocios principales en la Ciudad de México; es decir, los clientes que se deben visitar en provincia son en todos los casos sucursales de algún cliente que se tiene en la ciudad de México.

Aparte de los empleados que TESYS tiene trabajando la mayoría del tiempo en las instalaciones del cliente, también cuenta con un gran equipo de empleados que trabajan casi siempre en instalaciones propias de la compañía, este equipo de personas son los que trabajan en el diseño y desarrollo de productos de computo terminados (en estos casos el diseño y las pruebas de las soluciones se hacen en instalaciones propias de la compañía), y algunos empleados mas, que trabajan en Help Desk o equipos de soporte a aplicaciones o productos, en cuyo caso se trabaja vía telefónica o desde un chat de Internet.

Debido a la variedad, calidad y precios de los servicios que ofrece, TESYS es una compañía que se encuentra en pleno crecimiento, ya que últimamente se ha logrado la firma de nuevos contratos de negocios, lo cual implican tanto la entrada de más dinero como la contratación de nuevo personal para la atención de todos estos nuevos negocios, y la directiva se ha percatado que aunado a estos nuevos negocios se tienen nuevos retos y nuevas problemáticas de tipo administrativo y financiero que no se tenían en el pasado y que no se habían contemplado, ya que a medida que el número de empleados aumenta es mucho más difícil proveerles de un espacio y un equipo de trabajo en las instalaciones de la compañía lo que ha provocado últimamente que las propuestas de negocios para los nuevos prospectos no estén listas a tiempo, más lentitud en los procesos administrativos, mayor desconcierto e inconformidad en los empleados y lo más grave, atraso en las entregas de resultados en los proyectos que se tienen actualmente. Todo esto ha

llamado grandemente la atención de la dirección, la cual sabe que estos problemas propios del crecimiento no bien planeados deben ser solucionados gastando lo menos posible, por que como se mencionó anteriormente, TESYS es una compañía comprometida a proporcionar el mejor servicio a los mejores precios. Con el objeto de seguir cumpliendo con este compromiso y de seguir siendo una opción viable en el mercado de servicios y diseños de sistemas, la dirección ha concluido que la renta de un edificio o parte de él, no es una solución viable debido a los gastos de renta y servicios que eso representaría, sin contar además con la necesidad de más espacios de estacionamiento que se requerirían para los nuevos empleados.

Tomando en cuenta las consideraciones anteriores TESYS necesita una solución que resuelva principalmente dos grandes problemas:

1. Los empleados que trabajan en instalaciones del cliente deben poder presentar sus reportes de avances, facturaciones y actividades propias de recursos humanos desde dichas instalaciones; es decir, se requiere que los empleados sean capaces de accesar y actualizar bases de datos de la compañía sin tener que trasladarse a las oficinas principales de esta.

2. Se debe reducir la necesidad de lugares físicos para empleados en instalaciones de la compañía, promoviendo en los casos que así convenga, el trabajo desde casa o teletrabajo (los empleados candidatos a este tipo de trabajo, serian aquellos que trabajan en el diseño y desarrollo de sistemas, y aquellos que trabajan en equipos de soporte vía telefónica o por medio de algún chat de Internet, tomando en cuenta que todos estos empleados deben accesar y actualizar bases de datos de la compañía desde su casa.)

1.2 PROPUESTA DE SOLUCIÓN

Con el objeto de solucionar la problemática anterior se propone un sistema de conexión remota que abarque alguno de los dos escenarios de este tipo de conexión.

1.2.1 Primer Escenario. Pasarela para Red Privada (VPN Gateway)

A manera de reducir el movimiento de los empleados desde las instalaciones del cliente a las oficinas de TESYS, la necesidad de lugares de trabajo en las instalaciones de la compañía, los viajes al interior de la República y la lentitud en los tiempos de respuesta de procesos administrativos, se propone la creación de una Red Privada Virtual (VPN por sus siglas en Ingles; Virtual Private Network) por medio de la cual se logrará la conexión remota entre la PC portátil y la red LAN de la compañía; de esta manera los empleados tendrán la capacidad de conectarse a la red de TESYS con solo tener un acceso a Internet, ya sea en la Ciudad de México o en el interior de la República. El propósito principal de este escenario es que los empleados se puedan conectar desde las oficinas de los clientes por medio de una conexión telefónica.
Para lograr esta conexión se requiere la construcción de un túnel entre la red telefónica pública y la red LAN de TESYS (mediante un acceso dedicado), lo cual funcionará mediante la instalación de un software en cada PC portátil. Las comunicaciones en una VPN están protegidas ya que en este tipo de redes solo se permite la comunicación entre direcciones pertenecientes a la misma, aun así, con el objeto de robustecer la seguridad, se propone que la información que se transmite esté siempre encriptada al momento de realizar cualquier intercambio de información.

1.2.2 Segundo Escenario. Servidor para Acceso Remoto (RAS)

Para este tipo de conexión se requiere que TESYS cuente con un servidor de acceso remoto RAS (Remote Server Access), un banco de 30 módems y dos enlaces E1 de 30 troncales digitales cada uno para la conectividad de los usuarios de acceso remoto. Además, como en el primer escenario, la compañía deberá proveer a los empleados una PC portátil con el software necesario para hacer este tipo de conexión. Para lograr este tipo de conexión los empleados deberán comunicarse al o los números telefónicos asignados a los enlaces E1, los cuales recibirán la llamada y la asignaran a una línea desocupada en ese momento y por medio del RAS obtendrán el acceso a la LAN. Al igual que en el primer escenario se propone que la información se transmita en forma encriptada.

Para llevar a cabo cualquiera de las dos soluciones anteriores, serán candidatos los empleados que trabajen en el desarrollo y diseño de aplicaciones o soluciones completas, en equipos de soporte y mantenimiento o help desk (este tipo de empleados ya de por sí atiende a sus clientes de forma remota desde instalaciones de la compañía), y algunos de los empleados de las áreas de recursos humanos, calidad y gerencia, ya que como se menciona anteriormente el objetivo principal es crecer él numero de empleados sin aumentar considerablemente los gastos en servicios. Pero en el caso de que el crecimiento no sea el esperado con esta solución se puede pensar en reducir los costos de operación que se tienen actualmente en las instalaciones de TESYS.

1.3 OBJETIVO

Optimizar la conectividad entre la compañía TESYS y sus empleados, considerando los siguientes puntos:

a) Reducir los gastos de locación que tiene la compañía por medio de la facilidad de acceso remoto para los empleados desde su casa promoviendo el teletrabajo o trabajo desde casa.

b) Disminuir el número de viajes que realizan los empleados que atienden clientes en el interior de la republica por medio de la conexión remota desde cualquier parte de la republica.

c) Agilizar los trámites administrativos y reducir los tiempos de respuesta por medio del acceso remoto a las bases de datos de TESYS para consultas y actualizacion de las mismas.

1.4 METODOLOGÍA

Se propone describir paso a paso el diseño del sistema de comunicación remota por medio del cual los empleados de TESYS serán capaces de conectarse y comunicarse remotamente a las bases de datos de la red local de TESYS.

Lo anterior será posible mediante la configuración de una red local en la que se tengan los servidores necesarios para soportar las bases de datos de las diferentes áreas de la compañía, tales como el servidor de diseño y desarrollo de aplicaciones, el servidor de recursos humanos, el servidor de correo electrónico, etc. Y una vez que ya se tienen conectados los servidores se deben conectar todas las estaciones de trabajo, computadoras de escritorio y espacios disponibles para las portátiles de los empleados que tengan que trabajar de manera permanente o esporádicamente en instalaciones de la compañía.

Una vez diseñada la red local se deberá escoger el tipo de enlace dedicado que se va a contratar, para la conexión permanente de la red a Internet y se procederá a la elección de la VPN o del RAS con su respectivo banco de módems de tal manera que se pueda atender 200 usuarios internos y hasta 100 usuarios remotos. Ya teniendo la conectividad por la parte de la red LAN de TESYS solo restara la contratación de los usuarios de acceso remoto "Dial up" que se asignaran a los empleados para que estos se puedan conectar remotamente.

A continuación se presenta una gráfica que muestra de manera simple como quedaría el sistema de comunicación remota ya terminado, el cual por cierto incluye una conexión a otras redes locales (por medio de la WAN).

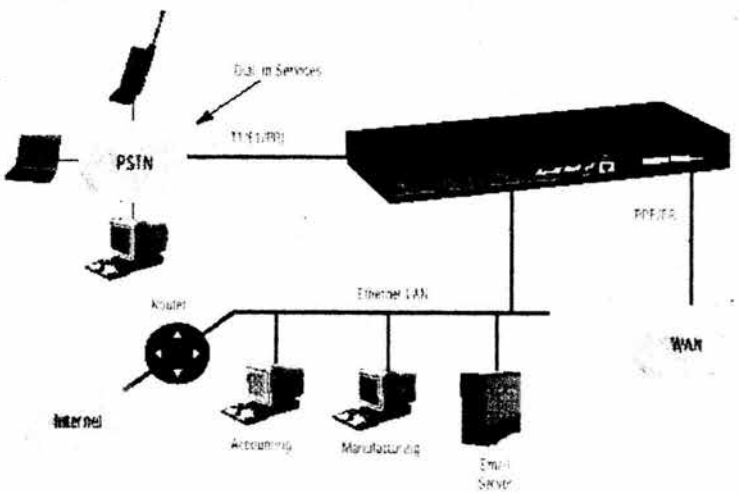


Figura 1.1 Sistema de conexión remota.

Las telecomunicaciones se han convertido en un satisfactor de necesidades cotidianas de un importante número de habitantes y corporaciones de este planeta. Sin embargo, pocos se han preguntado cómo opera cada sistema y qué importancia tienen en un mundo donde la transmisión de información a distancia es un fenómeno común y cada vez más necesario.

En el capítulo 2, realizaremos una remembranza sobre las telecomunicaciones en nuestro país, desde su nacimiento, crecimiento y maduración.
Partiendo desde el primer servicio de telecomunicaciones que fue la telegrafía, precedido de la telefonía así como de los cambios y crecimientos estructurales debido al ámbito social y económico del país. También se menciona las acciones más relevantes en materia de telecomunicaciones, en el México actual. En otro punto se considera la Historia del Internet a nivel mundial de una manera cronológica desde su nacimiento hasta nuestros días. También es considerado la Historia del Internet en México. Por último se hace mención de conexiones remotas entre redes o usuarios, así como de algunos de los tipos de conexiones y métodos de ejecución a utilizar dependiendo de la aplicación, velocidad de transmisión, voz datos, vídeo, etc.

En el capítulo 3, dentro de las generalidades de telecomunicaciones partiremos del modelo OSI que es un sistema de interconexión estructurado por 7 diferentes niveles, los cuales son descritos uno a uno, explicando su funcionalidad y los diferentes dispositivos y protocolos aplicados a estos niveles. Posteriormente analizaremos los tipos de señales analógicas y digitales que a su vez son clasificadas en periódicas y no periódicas dependiendo del dominio del tiempo y la frecuencia, continuando con el espectro de frecuencia y ancho de banda. Otro factor a considerar es la modulación (analógica y digital) que es la técnica a emplear para la modificación de una señal, con la finalidad de facilitar la transportación de información a través de un medio de comunicación. Por otro lado se hace mención de las características de la transmisión de datos y de los medios (guiados y no guiados) a través de los cuales viajará la información, continuando con la aplicación y señalización de troncales de voz. Este capítulo también contendrá una sección para la detección y corrección de errores, esto con la finalidad de garantizar que la información enviada desde un emisor sea la misma que llegue a un receptor, por lo cual es necesario de métodos que verifiquen la integridad de la información.

Capítulo 4, las redes de información se clasifican de acuerdo a su extensión y el tipo de topología, por lo cual se definirán los tipos de redes y los tipos de topología a utilizar para una cierta red. Se definirá la funcionalidad y requerimientos básicos de lo que es una red privada virtual (VPN), la cual mediante la creación de un túnel (encapsulación) se dará la transferencia de datos de un sitio a otro, garantizando que los paquetes de información que van encriptados lleguen a su destino remoto. Posteriormente se analizará la red de telefonía pública, que es la que nos permitirá establecer una llamada entre dos usuarios en cualquier parte de nuestro planeta. Nuestro análisis comenzará desde la realización de una llamada, iniciada por un usuario origen pasando a través de centrales telefónicas hasta llegar al usuario destino. Dentro del capítulo se incluirá una breve historia del Red Digital de Servicios Integrados (RDSI). Para comprender nuestro análisis, como primer punto se definirá la Estructura General de la RDSI, así como de las ventajas que esta tiene, canales de acceso, topología y configuraciones de acceso de la RDSI. Otro punto analizar son los tipos de servicio con los que esta red digital cuenta y de cómo se da la transmisión y señalización de datos. Consecuentemente se hará énfasis en la configuración física y niveles de conexión de la red óptica sincrona (SONET),que es el mecanismo de transporte multiplexado y como tal es portador de servicios de banda ancha, así como de los dispositivos y protocolos utilizados en un sistema de transmisión SONET.

Capítulo 5, los equipos de conectividad y los mecanismos de seguridad son los dispositivos que ayudarán que se logre la comunicación remota de forma segura entre la empresa y los empleados en este capítulo se realizará un estudio detallado de estos equipos de conectividad necesarios para el objetivo de nuestra compañía, como son: ruteadores, conmutadores, concentradores, módems, pasarelas y puentes. Los mecanismos de seguridad son basados en un conjunto de elementos tales como: certificados digitales, criptografía simétrica y de clave pública, firmas digitales, listas de certificados revocados, muros de fuego etc; así como de los requisitos para una comunicación segura, Autenticidad, confidencialidad, integridad y no repudio.

Un mecanismo de seguridad es el SSL (Secure Socket Layer) que es la capa de seguridad la cual permitirá la confidencialidad y autentificación en las transacciones por Internet, usado principalmente en aquellas transacciones donde se intercambian datos confidenciales tales como: Números de tarjeta de crédito o contraseñas de acceso a sistemas privados.

El mecanismo de seguridad importante a considerar, es el muro de fuego (Firewall), el cual es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de la red privada y el Internet. El muro de fuego determinará cual de los servicios de red podrán accesar dentro de ella por los que están fuera de la red. Para que el muro de fuego sea confiable es necesario que todo el tráfico de información a través del Internet deberá pasar por el muro donde podrá ser inspeccionada la información a través de los diferentes componentes de este sistema.

Capítulo 6, en este capítulo se mencionará aspectos importantes para la conectividad de redes, la configuración ideal para la intranet de la compañía y las características necesarias para la conexión remota. Dentro de este capítulo también nos enfocaremos en el estudio de los componentes básicos para poder establecer la conexión remota y analizaremos los aspectos técnicos de algunos de los principales tipos de marcas de los equipos existentes en el mercado nacional.

Capítulo 7, Dada la problemática de TESYS, en este capítulo se dará la solución a este problema, enfocándonos al diseño total de un sistema de conexión remota privada basado en nuestro primer escenario que es el diseño de una red privada virtual (VPN Gateway). Se planteará un estudio económico comparativo entre los dos escenarios de solución propuestos en nuestro primer capítulo, Red Privada Virtual con pasarela (Gateway) y el Servidor de Acceso Remoto (RAS). Posteriormente justificaremos los equipos a utilizar dentro del diseño y configuración de nuestra red. Conjuntamente a esto analizaremos las posibilidades de crecimiento y viabilidad de nuestra red, tomando en consideración un 10% anual, esto con el fin de no realizar una nueva inversión a corto plazo.

Una vez adquiridos estos conocimientos se podrán aplicar para la creación del diseño de nuestra red. Sin embargo es necesario tomar en cuenta que, la creación de una red remota privada dependerá de las necesidades de cada empresa en particular, en cuanto a la comunicación interna, acceso de la información, aplicaciones requeridas para la mejora del flujo de trabajo, etc. De esta manera se logrará implementar una red remota privada altamente eficiente, escalable y segura que son las características principales de una VPN.

CAPÍTULO 2

ANTECEDENTES

2.1 HISTORIA DE LAS TELECOMUNICACIONES

El crecimiento y la maduración de las telecomunicaciones, la disminución de los costos reales, y el aumento en disponibilidad, confiabilidad, seguridad y conectividad de éstas ha sido producto de avances en diversos campos del conocimiento como la ingeniería espacial y la aeronáutica, pasando por la ciencia de materiales la física, y hasta la tecnología digital (electrónica y computación).

Aunque muchos de estos avances han tenido su origen en el uso militar, otros no menos importantes tuvieron sus inicios en aplicaciones civiles, como es el caso del teléfono (cuyos inicios fue la búsqueda de su inventor, Graham Bell en 1876, de un sistema que permitiera visualizar las señales de voz y ayudarse en sus labores de enseñanza a personas sordomudas; hasta convertirse en uno de los aparatos de comunicación más utilizados por las sociedades del presente siglo.)

2.1.1Historia de la Telegrafía en México.

El primer servicio de telecomunicaciones en nuestro país fue el telegráfico. El 10 de mayo de 1849, el Presidente de la República, José Joaquín Herrera, otorgo la primera concesión al Sr. Juan de la Granja, periodista español nacionalizado mexicano. El 5 de noviembre de 1851, el General Mariano Arista, Presidente de la República, inauguró este servicio entre la Cd. de México y Nopalucan, Pue., con lo que apenas seis años después de haberse inaugurado el servicio en los Estados Unidos de América y a cinco de haberse establecido en Francia, nuestro país contaba con el servicio telegráfico. Un año siete meses después, la línea México-Nopalucan se extendió hasta el puerto de Veracruz.

En 1853, se inauguró la línea México-Guanajuato y un año después se transmitían alrededor de 50 mil telegramas a través de 608 kilómetros de la línea telegráfica. Hacia 1870, el telégrafo disponía de 8 mil kilómetros de líneas y contaba con un tráfico de 222 mil mensajes anuales.

En 1880, se determina que el servicio telegráfico dependa de las autoridades federales y en 1891 la Dirección de Telégrafos Federales se incorpora a la nueva Secretaría de Comunicaciones y Obras Públicas; en ese año se enlazan algunas oficinas telegráficas mexicanas con la Western Union Telegraph Co. Y se crea la Compañía Telefónica y Telegráfica Mexicana, misma que prestaba el servicio telegráfico internacional. En 1910 este servicio se complementó con la radiotelegrafía que empezaba a tener auge en nuestro país. En la Constitución de 1917 se estableció que la prestación al servicio telegráfico, quedaba reservado al Estado. En agosto de 1986, por decreto presidencial, se creó Telégrafos Nacionales como organismo descentralizado, con el objeto principal de prestar el servicio de telégrafos. Por decreto de noviembre de 1989 se crea Telecomunicaciones de México para garantizar la prestación de los servicios estratégicos de telecomunicaciones reservadas al Estado y aquellos prioritarios que le sean encomendados por el Ejecutivo Federal.

2.1. 2. Historia de la Telefonía en México.

El servicio telefónico inició en nuestro país el 13 de marzo de 1878, con una conferencia entre la Cd. de México y Tlalpan, únicamente dos años después de que Alejandro Graham Bell, llevó a cabo la primera comunicación telefónica de larga distancia en el mundo, entre las ciudades de Boston y Salem en los Estados Unidos de Norteamérica.

En sus inicios la red telefónica mexicana, interconectó 6 comisarías de policía, la Inspección General, la Oficina del Gobernador de la Cd. de México y el Ministerio de Gobernación.

En 1881 la Compañía Telefónica y Telegráfica Mexicana obtuvo la concesión para prestar el servicio telefónico y posteriormente se le otorgaron ampliaciones a esta concesión. En 1883 tuvo lugar la primera conferencia telefónica internacional, misma que se realizó entre Matamoros, Tamps. Y Brownsville, Tex.

En 1888 se publicó el primer directorio telefónico del país y en 1890 se contaba con 1,110 suscriptores del servicio telefónico.

El 18 de febrero de 1903 la Compañía de Teléfonos Ericsson, S.A. de C.V. inició operaciones únicamente en el D.F. En 1926 se le otorgó una nueva concesión por 50 años.

En 1947 Teléfonos de México, S.A. de C.V. (Telmex) adquirió los bienes y derechos sobre la concesión de la Compañía de Teléfonos Ericsson, S.A. de C.V., y en 1950 enlazó sus líneas con la red de la Compañía Telefónica y Telegráfica Mexicana, S.A., la cual se le había otorgado concesión en 1881. En el mismo año de 1947, Telmex compró las instalaciones de esta empresa y se le otorgó una nueva concesión por 50 años. Para 1956, se disponía de 375,000 aparatos, con una densidad de 1.2 aparatos por cada 100 habitantes. A partir de entonces, el Gobierno Federal apoyó en forma importante los programas de desarrollo telefónico debido a que registraba un gran rezago en la atención de la demanda del servicio. Así, diversas medidas de carácter financiero se instrumentaron para fortalecer la infraestructura. En 1963 se inició la participación accionaría del Estado en la prestación del servicio Telefónico hasta alcanzar posteriormente, el 51% del capital social.

En 1960, había en el país cerca de 532,000 aparatos en servicio y en 1970 se alcanzó la cifra de 1.5 millones. Durante ese lapso la tasa de crecimiento media anual fue de 12 por ciento. El permanente rezago en la atención de la demanda de servicios y los montos crecientes de recursos requeridos para ampliar y modernizar la infraestructura, fueron factores determinantes para que en 1990, se decidiera privatizar la empresa Teléfonos de México S.A. de C.V., al mismo tiempo que se modificó su título de concesión y se amplió el plazo de éste por 50 años. En esta oportunidad se impuso a la empresa metas específicas en cuanto a crecimiento y calidad de servicios; asimismo, se incorporaron condiciones más transparentes en cuanto a la fijación de las tarifas.

2.1.3 Cambio Estructural de las telecomunicaciones en México (90's)

Antecedentes

Con anterioridad a 1989, prácticamente no existió competencia en la prestación de los servicios de telecomunicaciones, toda vez que la actividad del sector estaba representada en más del 95%, por el servicio telefónico proporcionado por Teléfonos de México, S.A. de C.V. (Telmex), en el ámbito nacional, a excepción del estado de Baja California y San Luis Río Colorado, Son., en donde opera Teléfonos del Noroeste, S.A. de C.V. (Telnor), filial de Telmex.

En forma incipiente operaban distintos servicios de radiocomunicaciones y con una gran dinámica, pero sin tanta significación hasta ese entonces, participaban los servicios satelitales. De este modo, la gran problemática se centraba en el subsector telefónico por su preponderancia en el

ámbito social y económico del país. En esos años, Telmex, confrontaba una problemática compleja para encarar y resolver sobre bases sanas la expansión y desarrollo del servicio de telefonía básica, fundamentalmente en materia de servicio local. Diversos aspectos técnicos, administrativos y financieros se conjugaban como elementos restrictivos del crecimiento de la empresa que contrastaba con las fuertes exigencias sociales de una mayor oferta y calidad del servicio telefónico.

En efecto, a finales de 1990, Telmex contaba solamente con 5´355,000 líneas, de las cuales el 70% eran de tecnología analógica y el 30% de tecnología digital. La red subterránea, en un 40% tenía una antigüedad de más de 40 años.

La densidad telefónica registraba 6.5 líneas por cada 100 habitantes, mientras que países con economías similares a la nuestra contaban con alrededor de 20 líneas por cada 100 habitantes. Además, se tenía un rezago alrededor de 1´500,000 solicitudes de nuevas líneas, con tiempos de espera para la instalación de hasta 24 meses.

En materia de casetas públicas, a finales de 1989 se tenían sólo 40,000 que promediaban 0.5 casetas por cada 1,000 habitantes contra el promedio de 5 casetas en países con economías equivalentes.

Entre los principales factores que originaron esta situación, se identificaron los siguientes:

a) La crisis económica originada en 1982 debilitó las finanzas de la empresa.

b) El complejo marco laboral y administrativo limitaba el avance tecnológico.

c) La política tarifaría y fiscal restringían los ingresos de la empresa. Existían subsidios cruzados entre servicios y el impuesto al servicio telefónico encarecía el precio al consumidor final.

d) La compleja normatividad y restricciones al gasto y endeudamiento impuesta a las empresas públicas a las cuales pertenecía Telmex.

e) La inadecuada regulación que carecía de estímulos y obligaciones para mejorar la cobertura y calidad del servicio.

f) El daño a la red telefónica con motivo del sismo de 1985.

Acciones relevantes a partir de 1990

Con el propósito de reestructurar, acelerar el crecimiento y modernizar las telecomunicaciones en nuestro país, a partir de 1990 se ha llevado a cabo acciones que han modificado el marco regulatorio de las telecomunicaciones, lo cual ha conducido a un cambio estructural del sector.

Entre las acciones más destacadas se citan las siguientes:

a) El concesionamiento bajo un esquema de competencia de la telefonía celular.

b) La publicación del Reglamento de Telecomunicaciones.

c) La desincorporación y el nuevo título de concesión otorgado a Teléfonos de México, S.A. de C.V.

d) La entrada en vigor de la Ley Federal de Telecomunicaciones

e) La creación de la Comisión Federal de Telecomunicaciones.

A continuación se comentan los dos aspectos más relevantes en el proceso de cambio del marco de regulación de las telecomunicaciones: La privatización de Telmex y la Ley Federal de Telecomunicaciones.

Titulo de Concesión de Telmex

Con fundamento en los artículos 32 y 68 de la Ley Federal de Entidades Paraestatales, el Ejecutivo Federal decidió la privatización de Telmex, cuyo proceso, llevado a cabo por la Secretaría de Hacienda y Crédito Público, concluyó en el mes de diciembre de 1990. Luego de un estudio de las diversas ofertas, para la adquisición del porcentaje de acciones del gobierno federal, la decisión favoreció al Grupo Carso, asociado con dos empresas de telecomunicaciones de reconocido prestigio internacional como son France Telecom. (Francia) y South Western Bell (E.U.A.) De este modo, el gobierno dejó de tener la participación mayoritaria en el capital social de Telmex y se modificaron los términos y condiciones de la concesión otorgada el 10 de marzo de 1976.

La modificación al título de concesión, publicada en el Diario Oficial de la Federación de fecha 10 de diciembre de 1990, se llevó a cabo para adecuarlo al avance tecnológico y asegurar que Telmex cumpliera con los compromisos de cobertura, calidad y precio de los servicios, así como para promover una competencia equitativa con otras empresas de telecomunicaciones. La concesión ampara a Telmex para construir, instalar, mantener, operar y explotar una red pública telefónica por un periodo de 50 años contados a partir del 10 de marzo de 1976, con apertura en todo el territorio nacional a excepción del área concesionada a Telnor.

Algunos de los aspectos novedosos incorporados al título de concesión son:

a) El alcance de los servicios concesionados se hizo más amplio

b) Se abrió la competencia del servicio local

c) Se incluyo un esquema de regulación tarifaría.

d) En los primeros 4 años de operación debería expandir el número de líneas en operación del servicio básico en 12% anual.

e) Ofrecer el servicio telefónico básico con conmutación automática en todas las poblaciones del país con más de 5,000 habitantes y las que contarán con más de 500 habitantes, según el censo de población y vivienda de 1990, tuvieran acceso al servicio telefónico al menos mediante una caseta pública o agencia de larga distancia.

Ley Federal de Telecomunicaciones

En junio de 1995, entró en vigor la Ley Federal de Telecomunicaciones que constituye el elemento jurídico central de la nueva regulación en esta materia. Derivado de dicha Ley, se han expedido los Planes Técnicos Fundamentales de Numeración y Señalización, las Reglas de Servicio de Larga Distancia, las Reglas para prestar el Servicio de Larga Distancia Internacional, el Reglamento de Telefonía Pública y el Reglamento de Comunicación Vía Satélite. Asimismo, este ordenamiento jurídico ha permitido un mayor énfasis a las relaciones internacionales de México en materia de telecomunicaciones dentro del marco de globalización mundial.

La Ley Federal de Telecomunicaciones y su reglamentación contemplan, fundamentalmente:

a) Nuevas disposiciones para el uso y administración del espectro radioeléctrico.

b) Apertura a la competencia en las diferentes áreas y servicios.

c) Mayor transparencia en el procedimiento de concesionamiento de redes públicas de telecomunicaciones.

d) Asignación de concesiones que usen espectro por medio de licitación pública.

e) Interconexión e interoperabilidad de redes públicas de telecomunicación.

f) Apertura a la inversión privada en materia satelital, permitiéndose la competencia de satélites extranjeros.

Para que la Secretaría de Comunicaciones y Transportes, como entidad reguladora, pueda cumplir con mayor eficacia las acciones y objetivos, la propia Ley Federal de Telecomunicaciones establece cambios estructurales en su organización y funcionamiento, por lo que en agosto de 1996 se creó la Comisión Federal de Telecomunicaciones como órgano administrativo desconcentrado con autonomía técnica y operativa para regular la expansión y calidad de las telecomunicaciones.

Crecimiento de la Infraestructura

A partir del proceso de privatización de Telmex, el sector de las telecomunicaciones en México ha crecido siete veces más rápido que la economía en su conjunto y pasó de representar el 1.6% del PIB en 1990 al 3.1% en 1996. Todos los subsectores han experimentado un acelerado crecimiento:

a) De 1990 a marzo de 1999, el número de líneas telefónicas pasó de 5.3 millones a 10 millones, lo que representa un crecimiento en términos relativos de 88.6%

b) La digitalización de la planta telefónica en el periodo de 1990 a marzo de 1999 pasó de 29% a cerca del 97% en el renglón de conmutación. Por lo que se refiere al rubro de transmisión, la red se encuentra totalmente digitalizada.

c) El crecimiento de los principales servicios de radiocomunicación en cuanto a suscriptores en el periodo 1990-1998, fue de 63.9% en Radiotelefonía Móvil con Tecnología Celular; 39.3% en radiolocalización Móvil de Personas y 77.7% en Radiocomunicación Móvil Especializada de Flotillas. El número absoluto de usuários a marzo de 1999 en estos servicios es de aproximadamente 3.7 millones en Radiotelefonía Móvil con Tecnología Celular, 800 miles en Radiolocalización Móvil de Personas y 149.3 miles en Radiocomunicación Móvil Especializada de Flotillas.

2.1.4 Las Telecomunicaciones en el México actual.

La nueva regulación de las telecomunicaciones en nuestro país ha propiciado cambios estructurales en el sector. Así, esta forma regulatoria ha modificado la industria de un cuasimonopolio estatal a un esquema basado en una economía de mercado. El crecimiento y modernización del sector, al cual ya se ha hecho referencia anteriormente, ha permitido en términos generales una sensible mejoría en la calidad de los servicios, diversificar los mismos y reducir las tarifas, principalmente, en los servicios de larga distancia.

No obstante lo anterior, uno de los aspectos medulares pendientes, es la baja penetración de la telefonía local en la población y su desigual distribución geográfica. En consecuencia, uno de los principales objetivos en este campo, es el de incrementar en forma acelerada la tele densidad y mejorar tanto social como geográficamente su penetración. En todo caso, la estrategia y acciones para avanzar en este renglón, debe conjugarse con la oferta creciente de nuevos servicios, eficientes, de calidad y accesibles a más usuarios, considerando desde luego las condiciones necesarias que le confiera viabilidad a la industria en el largo plazo.

En este marco, las líneas de estrategia para avanzar en la integración de más y mejor infraestructura, debe considerar fundamentalmente los aspectos siguientes:

a) Consolidar la apertura a la competencia en todas las áreas.

b) Fomentar condiciones de sana competencia.

c) Promover una adecuada cobertura social y rural de redes y servicios.

d) Fortalecer la rectoría del Estado en este campo.

e) Fomentar la investigación y desarrollo tecnológico

f) Aprovechar los servicios de valor agregado y las nuevas aplicaciones tecnológicas en tareas de carácter social

g) Aprovechar el espectro de uso oficial en renglones de seguridad pública y cobertura social.

h) Aprovechar el espectro radioeléctrico para mejorar la tele densidad

i) Ampliar la cobertura y tele densidad de la telefonía pública

j) Promover y vigilar la eficiente interconexión de las redes públicas de telecomunicaciones

2.2. HISTORIA DEL INTERNET

La historia de Internet comienza realmente en el año 1962. Las pocas computadoras de esa época tenían memorias de núcleos magnéticos con capacidad para almacenar unos pocos miles de caracteres. Los programadores, sin embargo las ensamblaban para hacer rendir con enorme ingenio a esos pocos caracteres, por ejemplo, procesando modelos de simulación y de programación lineal en una computadora tal como la IBM 1401 que fue pensada para ser simplemente una impresora y que justamente se caracterizaba por tener originalmente 14000 posiciones de memoria. El mundo de las comunicaciones estaba en ese entonces en manos de IT&T. Existía en esa época un proyecto estratégico del DOD, Deparment of Defense (Departamento de Defensa de los Estados Unidos), denominado ARPA por Advanced Reserch Projects Agency (Agencia para proyectos de Investigación Avanzada). Clasificado a su vez como proyecto de alto riesgo y de incalculables beneficios, sienta las bases de la red ARPA o ARPANET, la cual mucho más tarde se convertiría en Internet.

En 1992, 30 años más tarde:

a) Internet tenía un millón de computadoras conectadas.

b) ARPANET ya no existía.

c) Los anchos de banda eran 20 millones más grandes.

A continuación un cuadro que muestra los avances del Internet a través de los años desde su nacimiento y hasta la actualidad:

Años 50	A finales de la década de los 50 nace ARPA, la Agencia de Proyectos de Investigación Avanzada, en el seno del Departamento de Defensa de los Estados Unidos.
Años 60	A principio de los años 60, la idea de una red descentralizada flotaba entre diversas instituciones americanas, como el Massachusetts Institute of Technology (MIT) y la Corporación RAND.
1961	Leonard Kleinrock del MIT publicó en julio de 1961 el primer trabajo sobre "conmutación de paquetes" (la tecnología que permitía dividir los datos en paquetes y que estos recorrieran rutas distintas para llegar a un mismo destino). El Pentágono, a través de ARPA financió la puesta en marcha de una prueba práctica. Kleinrock convenció a Lawrence G. Roberts de la posibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red.

1962	La primera descripción documentada a cerca de las interacciones sociales que podrían ser propiciadas a través del networking (trabajo en red) está contenida en una serie de memorándums escritos por J.C.R. Licklider, del Instituto de Tecnología de Massachusetts, en agosto de 1962. En ellos Licklider discute sobre su concepto de Galactic Network (red galáctica). Licklider concibió una red interconectada globalmente a través de la que cada uno pudiera acceder desde cualquier lugar a datos y programas. En esencia, el concepto era muy parecido a la Internet actual. Licklider fue el principal responsable del programa de investigación en computadoras de la DARPA (Defense Advaced Research Project Agency, la posterior denominación de la ARPA) desde Octubre de 1962. Paralelamente, entre 1962 y l964 la RAND Corporation publicó artículos escritos por Paul Baran sobre "Redes de Comunicación Distribuidas". Inactiva o fuera de servicio. Baran promovió el uso de redes de conmutación de paquetes de datos (Packet Switching Networks) que permitiesen que la información transmitida se dividiese en paquetes del mismo tamaño e importancia y se transmitieran a través de los nodos en los cuales se encontrara la ruta más eficiente para que al llegar a su destino se reagruparan en el orden que tenían previamente.
1964	Es en el marco de la RAND Corporation que, para solucionar el problema, en 1964 se propone una red que no disponga de una autoridad central y se sugiere un diseño que desde el principio está preparado para trabajar en un entorno fragmentado. Todos los nodos deberían tener un estatus parecido y cada uno de ellos tendría autonomía y poder suficientes para generar, vehicular y recibir mensajes que a su vez pudieran ser separados en paquetes y ser enviados por separado. Cada paquete tendría su origen en un nodo concreto y llegaría otro nodo de destino específico.
1966	A finales de 1966 Lawrence G. Roberts se trasladó a la DARPA a desarrollar el concepto de red de ordenadores y rápidamente confeccionó su plan para ARPANet (literalmente "la red de ARPA"), publicándolo en 1967. En la conferencia en que presentó el documento se exponía también un trabajo sobre el concepto de red de paquetes a cargo de Donald Davies y Roger Scantlebury del NPL. Scantlebury le habló a Roberts sobre su trabajo en el NPL así como sobre el de Paul Baran y otros en RAND. La palabra packet (paquete) fue adoptada a partir del trabajo del NPL y la velocidad de la línea propuesta para ser usada en el diseño de ARPANet fue aumentada desde 2,4 Kbps hasta 50 Kbps.
1967	Para pasar de la teoría a la práctica, Licklider y Roberts presentan en 1967 sus estudios en la Association for Computing Machinery Symposium. Allí se discuten los primeros planes para ARPANet, a partir de un estudio de Laurence Roberts titulado Multiple Computer Networks and Intercomputer Comunication. Un año más tarde se diseñan los primeros programas y el primer hardware específico para redes.
1968	En 1968 el Laboratorio Físico Nacional en Inglaterra estableció la primera red de prueba basada en estos principios. En el mismo año, el primer diseño basado en estos principios de envío de paquetes de información, realizado por Lawrence Roberts, fue presentado en la ARPA. La nueva red llamada ARPANet recibe el disparo de salida.

1969	Al año siguiente, el Departamento de Defensa dio el visto bueno para comenzar la investigación en ARPANet. El primer nodo de ARPANet fue la Universidad de California en Los Angeles. Pronto le siguieron otros tres nodos: la Universidad de California en Santa Bárbara, el Instituto de Investigación de Stanford y la Universidad de Utah. Estos sitios constituyeron la red original de cuatro nodos de ARPANet. Los cuatro sitios podían transferir datos en ellos en líneas de alta velocidad para compartir recursos informáticos. El protocolo de comunicaciones que usarían estos primeros nodos se llamó NCP /Network Control Protocol), que, más tarde, evolucionaría hasta el actual TCP/IP. El primer nodo, en UCLA, lo desarrolló la compañía BBN (Bolton, Beranek and Newman), ensamblando un Interface Message Processor (IMP, la máquina que gestionaría los mensajes, antecesora de los routers actuales) en un microordenador Honeywell DDP 516. Esos ordenadores tenían sólo 12K de memoria y parecían armarios de casi media tonelada. En 1969 apareció el primer ARPANet (Request For Comment). Los RFC, documentos emitidos Periódicamente, se han convertido en un conjunto en las normas y estándares de Internet. Literalmente, una "solicitud para comentario", en su origen eran preguntas formuladas por estudiantes que no sabían qué acción tomar ante la falta de normativas. Es la respuesta a dicha pregunta o la iniciativa de tomar un camino particular ante la falta de orientación lo que convierte la RFC en norma.
Años 70	Durante este periodo, esta red fue de acceso restringido a los investigadores y a las empresas privadas que participaban en proyectos financiados por la administración.
1970	Kevin MacKenzie se inventa el primer emoticón: Empieza a funcionar la primera lista de correo de forma sumergida. Se denominaba SF Lovers y estaba dirigida a amantes de la ciencia ficción. Vinton Cerf escribe por primera vez la palabra Internet. La escena tiene lugar a principios de los setenta en un hotel de San Francisco. Vinton, considerado el padre de la red, escribió la palabra Internet en el dorso de un sobre intentando explicar a sus compañeros la idea que había tenido sobre cómo distribuir información a través del a red que entonces se conocía como Internet. Este diseño sería la base del protocolo TCP/IP, que rige aún las comunicaciones por Internet.
1971	El comienzo de la década de los setenta vio el crecimiento de la popularidad del correo electrónico sobre redes de almacenamiento y envío. En 1971, ARPANet había crecido hasta 15 nodos con 23 ordenadores hosts (centrales). En este momento, los hosts de ARPANet comienzan a utilizar un protocolo de control de redes, pero todavía falta la estandarización. Además, había muy diferentes tipos de hosts, por lo que el progreso en desarrollar los diferentes tipos de interfaces era muy lento. La cultura llegaba pronto al nuevo medio: en 1971 Michael Hart creaba el Proyecto Gutenberg, para crear y difundir textos electrónicos gratuitamente (el estándar ASCII databa de 1968).

1972	Nace la posibilidad de realizar un Telnet. El primer programa específicamente diseñado para el email se atribuye a Ray Tomlinson, de la BBN (Bolton, Beranek and Newman), en 1972. Se remitió el primer mensaje de correo electrónico usándose el conocido símbolo de la arroba, @. El símbolo @ se convirtió en el símbolo del correo electrónico por pura casualidad. Ray Tomlinson necesitaba un signo que separara el nombre del usuario del de la máquina. Se limitó a bajar los ojos hacia el teclado (un teletipo modelo 33 trabajando con un ordenador Tenex) y escogió la arroba porque necesitaba que no fuera una letra. En los ahora 37 nodos en EE. UU. La expansión en ARPANet era muy fácil debido a su estructura descentralizada. Mientras tanto, el primitivo proyecto ARPANet se preparaba para unirse con otras redes: de satélite (el primero comercial se había lanzado en 1962), de radio terrestre, y de otros tipos, siempre y cuando compartieran la conmutación de paquetes. Robert Kahn introdujo esta "arquitectura abierta" en 1972: se la llamó Internetting, porque servía para la relación entre redes (net, en inglés).
1973	Durante el mes de septiembre de 1973 hubo una importante reunión en Brighton (Inglaterra) donde los americanos mostraron por primera vez a los europeos el funcionamiento de ArpaNet. Para que ello fuera posible tuvieron que realizar un enlace vía satélite, provisional durante unos días, que transportaba los datos a través del Atlántico. Lein Kleinrock volvió a los Angeles unos días antes que finalizara el congreso y cuando llegó a casa se dio cuenta que se había dejado una máquina de afeitar y descubrió que, efectivamente, en Brighton aún estaba conectado Larry Roberts. Kleinrock le pidió a Roberts que le recuperara su máquina de afeitar y éste lo hizo. La sorpresa fue que días más tarde Kleinrock fue acusado de haber realizado un uso indebido de material militar (que incluía de hecho hasta un satélite). El lío montado convenció a los militares de que era mejor separar a los usuarios civiles de su red y así fue como se escindió la red militar de la civil según se puede leer en algunas historias de la web en Internet. Nace la posibilidad de realizar un FTP.
1974	En 1974 se estableció el Transmission Control Protocol (TCP), creado por Vinton Cerf y Bob Kahn que luego fue desarrollado hasta convenirse en el Transmission Control Protocol/Internet Protocol (TCP/IP). TCP convierte los mensajes en pequeños paquetes de información que viajan por la red de forma separada hasta llegar a su destino donde vuelven a reagruparse. IP maneja el direccionamiento de los envíos de datos, asegurando que los paquetes de información separados se encaminan por vías separadas a través de diversos nódulos, e incluso a través de múltiples redes con arquitecturas distintas. El TCP/IP ha sido la clave técnica que ha permitido el crecimiento exponencial de Internet sin colapsar toda la red de comunicaciones. Antes de la popularización de Internet gracias a la aparición del WWW, esta red ya se había consolidado como una red internacional de ordenadores gracias a este protocolo de comunicaciones.
1975	En julio de 1975 ARPANET fue transferido por DARPA a la Agencia de Comunicaciones de Defensa.
1976	Aparecen los nodos por paquetes conmutados y las puertas de acceso.

1977	Aparece la primera lista de correo. Se trataba de TheryLink y agrupaba a casi un centenar de científicos. En 1979 nacería Usenet y hoy hay más de 50.000 newsgroups o grupos de noticias en el mundo. El crecimiento tan brutal de las listas obligó en 1987 a crear las jerarquías (las primeras fueron .comp, .news y .misc).
1979	Nace Usenet. Creada por tres estudiantes: Tom Truscott, Jim Ellis y Steve Bellovin. Usenet es un servicio de grupos de noticias, las populares "news". Ven la luz por primera vez los smileys o emoticones El crecimiento de ARPANet hizo necesario algunos órganos de gestión: el Internet Configuration Control Board fue formado por ARPA en 1979. Más tarde se transformó en el Internet Activities Board y en la actualidad es el Internet Architecture Board of the Internet Society.
1980	Aparecen las primeras aplicaciones TCP/IP. Internet ya tiene 212 servidores.
1982	ARPANet adopta el protocolo TCP/IP como estándar. Se crea la EuNet (European Unix Network). La "European Unix Network" (EuNet), conectado a ARPANet, se creó en 1982 para proporcionar servicios de correo electrónico y servicios Usenet a diversas organizaciones usuarias en los Países Bajos, Dinamarca, Suecia e Inglaterra.
1983	ARPANet en sí mismo permaneció estrechamente controlado por el departamento de defensa hasta 1983 cuando su parte estrictamente militar se segmentó convirtiéndose en MILNET. El Pentágono se retira de Arpanet y crea Milnet. Internet ya dispone de 562 servidores. Es en 1983 cuando se considera que nació realmente la Internet, al separarse la parte militar y la civil de la red. En ese momento ya la compartían 500 servidores (ordenadores interconectados). En el mismo año se creó el sistema de nombres de dominios (.com, .edu, etc., más las siglas de los países), que prácticamente se ha mantenido hasta ahora. En la constitución y crecimiento de esta nueva "red de redes" que pronto contó con nodos en Europa, las agencias federales norteamericanas prestaron mucho apoyo, financiando la infraestructura, por ejemplo.
1984	Se introduce el DNS (Domain Name Server). En 1984 el número de servidores conectados a la red había ya superado los 1.000. Dado que el software de TCP/IP era de dominio público y la tecnología básica de Internet (como ya se denominaba esta red internacional extendida) era algo anárquica debido a su naturaleza, era difícil evitar que cualquier persona en disposición del necesario hardware (normalmente en universidades o grandes empresas tecnológicas) se conectase a la red desde múltiples sitios. En 1984 William Gibson novelaba el nuevo mundo y acuñaba el término "ciberespacio". Al año siguiente se forjaba Well, la primera comunidad comercial de usuarios.

1985	La National Science Fundation (NSF) establece en este año cinco centros para superordenadores configurando con ello la principal red que utilizaría la comunidad científica a partir de se momento. Lo que hace es conectar seis centros de supercomputación. Internet tiene ya 1961 servidores. En abril aparecen los primeros dominios con letra (antes eran con números). Los primeros dominios con letras en aparecer fueron: acmu.edu, purdue.edu, rice.edu y ucla.edu, todos en activo aún por supuesto y todos universitarios también por supuesto. El primer dominio comercial en aparecer es algo no aclarado. Para algunos fue simbolics.com (un fabricante de software y hardware para el lenguaje de inteligencia artificial Lisp, esta página ya no funciona) y para otros think.com. En junio del mismo año apareció el primer dominio gubernamental, css.gov y en julio mitre.org. El primer dominio de un país fue en julio de ese mismo año para Gran Bretaña: co.uk
1986	La National Science Foundation (NSF) de EE.UU. inició el desarrollo de NSFNET que se diseñó originalmente para conectar cinco superordenadores. Su interconexión con Internet requería unas líneas de altísima velocidad. Esto aceleró el desarrollo tecnológico de Internet y brindó a los usuarios mejores infraestructuras de telecomunicaciones. Otras agencias de la Administración norteamericana entraron en Internet, con sus inmensos recursos informáticas y de comunicaciones: NASA y el Departamento de Energía. Un acontecimiento muy importante era que los proveedores comerciales de telecomunicaciones en EE. UU. y Europa empezaron a ofrecer servicios comerciales de transporte de señales y acceso
1987	En 1987 el número de servidores conectados a Internet superaba ya los 10.000.
1988	Internet ya dispone de 56.000 servidores. El día 1 de noviembre de 1988 Internet fue "infectada" con un virus de tipo "gusano". Hasta el 10% de todos los servidores conectados fueron afectados. El acontecimiento subrayó la falta de adecuados mecanismos de seguridad en Internet, por lo cual DARPA formó el Computer Emergency Reponse Team (CERT), un equipo de reacción rápida que mantiene datos sobre todas las incidencias en red y sobre las principales amenazas.
1989	Nace RIPE para interconectar las redes europeas. Tim Berners-Lee, investigador en el centro europeo CERN de Suiza, elaboró su propuesta de un sistema de hipertexto compartido: era el primer esbozo de la World Wide Web. Como el ARPANet veinte años atrás, su propósito era poner en comunicación a los científicos. La WWW es una creación europea fruto del trabajo de Tim Berners-Lee y Robert Cailauu que en 1989 trabajan conjuntamente desde el Centro Europeo de Física de Partículas (CERN) en Ginebra. Su objetivo era buscar una herramienta de trabajo para crear y leer textos a través de una red que permitía intercomunicar a los físicos de todo el mundo. La web, basada en el concepto del hipertexto, ha sido un soporte excelente para la introducción de las denominadas aplicaciones multimedia en las comunicaciones telemáticas. En Internet aun es posible encontrar una captura de pantalla del ordenador personal de Tim Berners-Lee, un Next, en que se ve el primer navegador de todos y como era la web cuando solo tenía un usuario.

	Berners-Lee creó el HTML, el HTTP y las URL. Berners-Lee es muy crítico con el uso comercial de la web y de hecho renunció a una empresa que había creado al inventar el web, empresa denominada WebSoft. Actualmente trabaja en el MIT en los Estados Unidos y sigue tan despistado como siempre según algunas fuentes. Jarkko Oikarinen, un joven finlandés, decidió modificar el comando talk del Unix para permitir que diversas personas pudieran charlar de forma simultánea. Así nace el chat, el Internet Relay Chat (IRC) que permite que se pueda conversar en la red. En 1989 el número de servidores conectados a Internet alcanza ya los 100.000. En este mismo año, se inauguró también la primera conexión de un sistema de correo electrónico comercial a Internet (MCI y Compuserve). Una nueva época estaba a punto de empezar, la de la explotación comercial de Internet. RPANet como entidad se extinguió en 1989/90, habiendo sobrepasado con mucho los objetivos y metas que tenía en su origen. Los usuarios de la red apenas lo notaron, ya que las funciones de ARPANet no solamente continuaron, sino que mejoraron notablemente a través de nuevos órganos más representativos de la utilización actual de la red (muchas instituciones (de la NASA al Departamento de energía) ya habían creado sus propias redes, que podían comunicarse entre sí y el número de servidores en la red superaba los 100.000). Nace Archie. Hasta ese momento nadie se había planteado jamás la hipótesis de que en Internet las cosas pudieran tener un orden, en crear algo parecido a un directorio vaya. Las direcciones eran tan pocas que se suponía todo el mundo las conocía. Por este motivo, se inicio el primer catálogo (un programa denominado Archie) tuvo tal éxito que colapsó el tráfico en los Estados Unidos y Canadá tan pronto se supo de su existencia. Por este motivo la Universidad MacGill de Montreal obligó a su autor a cerrarlo. Por suerte lo hizo después de que Archie ya estuviera replicado en otros ordenadores. Archie fue el precedente de Gopher y Veronica y de alguna remota manera el primer intento de directorio de recursos de Internet.
1990	Creación de la Electronic Frontier Foundation. Internet ya tiene 313.000 servidores. En 1990 redes de diversos países como España, Argentina, Austria, Brasil, Chile, Irlanda, Suiza y Corea del Sur se conectaron también a NSFNET.
1991	Una Ley del Congreso de los Estados Unidos aprueba la creación de la red nacional para la investigación y la educación (NREN) que extiende los servicios a todos los niveles educativos. Este mismo año se permite por primera vez el acceso a Internet del sector privado a través de conexiones alternativas a la red que estaba subvencionada con dinero público. Las empresas multinacionales aprovecharán este servicio que les permitirá reducir costos cundo conectan con sus delegaciones en todo el mundo. En febrero de 1991 es la fecha que se cita como la invención del denominado Spam, él envió masivo de correo electrónico no solicitado. Según estas fuentes todo empezó inocentemente: se trataba de enviar mensajes a un niño de 9 años llamado Craig Shergold gravemente enfermo. El muchacho intentaba batir el record mundial de cartas recibidas y lo

	consiguió. Ello dio ideas a algunas empresas y en abril de 1994 una empresa de abogados, Center&Siegel tuvo el dudoso honor de empezar a usar comercialmente el correo electrónico para envíos masivos no solicitados. La venganza que recibieron de la red por lo visto aun les dura. En marzo de 1991 Tim Berners-Lee pone en marcha el primer navegador de la web (que funcionaba aún con línea de comandos de modo que a años luz del lujo actual). Tim, el creador de la web, ya había creado en el año 1980 programas hipertextuales. En el CERN guardan la página original con los primeros servidores que se crearon. Es una página de noviembre de 1992, cuando solo había 26 ordenadores capaces de servir páginas web. La página advierte de que su contenido es una reliquia para la posteridad, para no confundir a despistados. El crecimiento tan espectacular que se ha producido en Internet, ha sido en gran medida a la creación del sistema capaz de incorporar imágenes, gráficos y sonido en las transmisiones, y no solo caracteres como hasta entonces: El World Wide Web (Telaraña de cobertura mundial). La incorporación de este método, ha permitido la entrada en Internet de aplicaciones y servidores más comerciales, y por lo tanto un crecimiento en el número de usuarios domésticos de todo el mundo. En 1991 se retiraron las restricciones de NFS al uso comercial de Internet. Ese mismo año también se Conectaron más países a la NSFNET incluyendo: Croacia, Hong Kong, República Checa, Sudáfrica, Singapur, Hungría, Polonia, Portugal, Taiwan y Túnez.
1992	Internet ya tiene 1.136.000 servidores Con más de un millón de servidores en la red crea la Internet Society, la "autoridad" de la red. Nacía como el lugar donde pactar los protocolos que harían posible la comunicación. Se trataba de una coordinación técnica, que no intervenía en los nacientes problemas de libre expresión: acababan de crearse la Electronic Frontier Foundation, defensora de los "ciberderechos", y el más famoso sistema abierto de criptografía: Pretty Good Privacy.
1993	Aparece el primer visualizador gráfico de páginas web: Mosaic, el antecesor de Netscape.El conocido navegador WWW Mosaic se desarrolló en el National Center for Supercomputing. Con la extensión de los ordenadores personales y el lanzamiento del primer navegador de la WWW popular, Mosaic, en 1993, ya había llegado el momento de "surfear la Web" (la expresión se registró por primera vez ese mismo año). En 1993 el número de servidores Internet sobrepasa los 2.000.000. También NSF patrocina la formación de una nueva organización, InterNIC, creada para proporcionar servicios de registro en Internet y bases de datos de direcciones. Internet ya tiene 1.776.000 servidores.
1994	En mayo se entregan los primeros premios a webs en la Primera Conferencia Internacional sobre la Web que se realiza en Ginebra. La lista de ganadores aún está en Internet. El número de servidores de Internet alcanza los 3.800.000 en 1994. Las primeras tiendas Internet empiezan a aparecer junto con "emisores" de radio on-line. El conflicto potencial entre los internautas tradicionales y los nuevos usuarios se manifestó con el tumulto que causó un gabinete legal americano que introdujo publicidad en Internet. En 1994 se abre el primer ciberbanco.

1995	Los principios de la Internet pública y masiva tuvieron anécdotas más o menos curiosas. America Online intentó por ejemplo en 1995 prohibir el uso de la palabra "pechos" Especialmente críticos fueron los médicos que preguntaban como podían por ejemplo informar sobre el cáncer de pecho sin usar la palabra en cuestión. En octubre de 1995 Netscape puso en la red el primer navegador. Para celebrarlo sus desarrolladores hicieron una fiesta con pizzas e instalaron un apantalla gigante para ver en la Silicon Graphics como empezaban a descolgarse navegadores. El primer usuario de Netscape fue un japonés y a medianoche los desarrolladores se dieron cuenta que el servidor indicaba qué versión era la que la gente se estaba bajando así que pusieron un sonido diferente para la de Windows, Mac y Unix que se oía cada vez que empezaba un download. Aparece RealAudio, que transmitirá sonido y voz por la red. En 1995 había más de 5 millones de servidores conectados a Internet. La espina dorsal de NSFNET empezaba a ser sustituido por proveedores comerciales interconectados.
1996	Internet ya tiene más de 9.400.000 servidores
1997	En 1997 ya hay 17 millones de servidores en la red.
1999	A partir de aquí las estadísticas se nublan: el tremendo crecimiento de la red, unido a la autonomía de su funcionamiento, hace que grandes zonas de sus contenidos estén en la penumbra: Según datos de 1999 el conjunto de los grandes buscadores de páginas en la Malla Mundial sólo conoce el contenido de menos del 50% de la red. La Última iniciativa, Internet 2, propone crear un espacio aparte y de más calidad de comunicaciones para instituciones de investigación.
2000	Hoy en día Internet está formada, no solamente de restos de la ARPANet original, sino que también incluye redes como la Academia Australiana de Investigación de redes (AARNET), la NASA Science Internet (NSI), la Red Académica de Investigación Suiza (SWITCH), por no mencionar las miles de redes de mayor o menor tamaño de tipo educativo y de investigación.

2.2.1 Historia del Internet en México.

Con la conexión de varios países al Internet, se ve le necesidad de la creación de organismos propios de las naciones que se encarguen de administración y supervisión de los recursos de Internet; Estas organizaciones fueron llamadas NIC por sus siglas en Ingles (NIC; Network Information Center).

El 1ro. De Febrero de 1989, el ITESM, Campus Monterrey establece conexión directa a Internet, y esta fecha es la que se conoce como el nacimiento de la NIC-México.

Merit Network, Inc. Establece Febrero de 1989 como la fecha de conexión de México a NFSNET (Internet). En esos momentos se conecta la primera máquina en Internet bajo el dominio mx: dns.mty.itesm.mx con la dirección 131.178.1.1.

Esta máquina, una Microvax-II, digital, fue el primer servidor de nombres para el dominio.mx. Lo fue hasta el 6 de Septiembre de 1993 (fecha del 50 aniversario del sistema ITESM), la sustituyó una Sun SPARC Classic con 48 MB en RAM y 400 MB en disco. En ese entonces no se requirió de una administración dedicada, ya que no existían muchos nombres de dominio.

Para 1992 había sólo 45 dominios bajo .mx de los cuales 40 eran académicos y 5 eran comerciales. Incluso .mx fue plano hasta Octubre de 1993, cuando en una reunión de los principales actores de las redes en México, se acordó crear los subdominios COM.MX, GOB.MX, y es en esa misma junta (en la Universidad de Monterrey) donde se decide no crear el subdominio EDU.MX. A principios de 1995 eran poco más de 100 nombres de dominio ubicados bajo .mx. Y sería precisamente a solicitud de la UdeM se discutiera la creación del dominio .edu.mx, y como resultado del consenso en la discusión del tema, el 4 de septiembre de 1996 se crea el edu.mx el cual junto con .mx representaba a dominio educativo. A mediados de 1997 se limita el registro de dominios académicos al .edu.mx.

Después del "boom" del WWW en México, se registró un incremento considerable en el número de dominios registrados mensualmente, lo que requirió una administración dedicada, así como la puesta en marcha de algunos servicios, tales como: Registro en línea de nombres de dominio, solicitud de IP's, registro de ISP en el país, solicitud de ASN, todo ello a través páginas de WEB.

En Octubre de 1995, se hace oficial la designación del ITESM, Campus Monterrey como NIC para México, lo que hace oficial el trabajo que se había venido desarrollando desde 1989. Por primera vez en 6 años del domino nacional, hay mas dominios comerciales que dominios educativos. A finales de año los dominios comerciales representaban el 55% de un total de 326 nombres de dominio bajo .mx

Durante 1996 se adquiere un nuevo equipo, una SUN SPARC 20, 256 MB RAM. Se empiezan a desarrollar servicios de registro automatizados y eficientes. A finales de este año hay 2838 nombres de dominios bajo .mx y el 80% de ellos eran dominios comerciales.

El crecimiento acelerado en el número de dominios hace necesario un mantenimiento de Bases de Datos actualizadas y en línea para la operación diaria del Internet en México, por lo que NIC-México evoluciona y en Enero de 1997 empieza a funcionar la Base de Datos WHOIS para el dominio .mx. En este mismo año se realiza la primera. Reunión de Información y Retroalimentación de NIC-México en la que se busca informar de los últimos acontecimientos en Internet y obtener retroalimentación. Se fijan cuotas de cobro por registro y mantenimiento de los dominios. Los dominios de entidades gubernamentales sobrepasan los 100 y el total de dominios registrados hasta 1997 es de 7251.

Para 1998 se tenían 10,000 nombres de dominio registrados y pagados lo que permite adquirir una infraestructura más robusta y confiable: Un enlace de 128K con UNINET, uno de 256K con AVANTEL y 10MB con el ITESM, Campus Monterrey; servidores SUN 450, 250, Ultra 2 y Sparc 20 y equipo de ruteo cisco 7200 y 2500. En Marzo de este mismo año se disminuyeron las tarifas de registro y mantenimiento en 30%. A mediados de este año se realizo la primera depuración de nombres que no tenían una resolución correcta o que tuvieran pagos pendientes.

Durante 1998 surge la necesidad de asociarse con otros dominios nacionales para compartir información y discutir políticas de nombres de dominio. Es el 21 de Agosto de 1998 cuando NIC-México es co-fundador y representante interino de LACTLD, organización que agrupa a los dominios nacionales de Latinoamérica.

En Abril de 1999, NIC-México recibe la primera solicitud del Instituto Mexicano de la Propiedad

Industrial (IMPI) para suspender un dominio por cuestiones de propiedad intelectual. El dominio en disputa fue nestle.com.mx. Para mediados de este año son más de 20,000 los dominios registrados bajo .mx. Para septiembre se contaba ya con un nuevo sistema de registro que permitía actualización de información en línea.

2.3 CONEXIÓN REMOTA

Las conexiones remotas se establecen entre redes o usuarios situados en puntos lejanos de tal forma que pueden compartir los recursos de la red tales como las bases de datos, los archivos de información y el correo electrónico.

2.3.1 Conexión remota entre redes locales.

Cuando se establece una conexión remota entre redes, normalmente se dedica una estación de trabajo en cada red al puente remoto.

Cuando se conecta una red local a otra, puede que más de un usuario necesite usar el puente a la vez. De aquí la necesidad de determinar previamente el nivel de comunicación, de forma que se configure el equipo, software y conexiones necesarios. Las decisiones se basarán en los siguientes puntos:

a) Número de usuarios que van a necesitar acceder a la conexión.

b) Tipo de las aplicaciones y de acceso a los archivos.

c. ¿Se transferirán archivos?

d) ¿Se usará el correo electrónico?

Si se determina que la conexión remota va a tener una gran actividad, serán esenciales líneas de comunicación de alta velocidad. Una actividad poco continua puede permitir el uso de líneas de menor velocidad pero más baratas.

Tipos de Conexiones.

La velocidad de la línea de conexión a menudo determina el tipo de conexión a utilizar.

a). Modems

Los módems estándar transmiten a velocidades entre los 2400 y los 9600 baudios, que normalmente no resultan adecuadas para las conexiones entre redes locales.

b) Redes de conmutación de paquetes.

De idéntica forma que una red permite que muchos usuarios puedan conectarse a ella y utilizar el sistema de cableado común, las redes de datos públicas les permiten conectar con una red de comunicaciones a nivel mundial que les ofrece posibilidades de transmisión de voz y datos a alta velocidad a un costo relativamente bajo. Para ello utilizan líneas telefónicas existentes, microondas y equipos vía satélite.

Para transmitir información se utiliza un método denominado conmutación de paquetes, en oposición a la conmutación de circuitos. Una línea de conmutación de circuitos es como una línea de voz concreta que utiliza para llamar a un amigo en la misma ciudad. Estas líneas permanecen abiertas para servir a una sola llamada hasta que cuelgan quienes llaman. A continuación se pueden utilizar las líneas para establecer otra conexión. Por otro lado, con la conmutación de paquetes se comparten las conexiones entre nodos por parte de varios usuarios, optimizando el uso de la línea y reduciendo los costos. La voz y los datos se convierten en paquetes que se transmiten continuamente por la red. Los paquetes de muchas llamadas distintas pueden ir entremezclados a medida que atraviesan las líneas; así se asegura que no hay ningún tiempo muerto en la conexión. El punto final debe ordenar, reorganizar y distribuir los paquetes a los conferenciantes adecuados.

Los diseñadores de sistemas pueden utilizar los servicios de conmutación de paquetes para establecer conexiones entre redes. Para acceder a las redes de conmutación de paquetes se utiliza un estándar internacional denominado X.25. Debido a que las líneas de conmutación de paquetes no son dedicadas, puede accederse a ellas sólo cuando son necesarias.

c) Líneas de servicio digital directo (Direct Digital Service, DDS).

Las líneas de servicios digitales directas funcionan a velocidades de hasta 56Kbps y hasta 64Kbps. Las líneas DDS poseen una alta fiabilidad, al usar un protocolo síncrono. Por lo general son más costosas que la implementación de los métodos X.25; sin embargo, el aumento de velocidad puede ser necesario cuando las redes deben transferir archivos u ofrecer acceso directo a archivos.

d) Enlaces T1 y T3.

Son líneas digitales de alta velocidad que se utilizan cuando es necesario un alto rendimiento entre los dos puntos. T1 se puede utilizar cuando se necesita acceso inmediato a la información de última hora, Las líneas T1 se pueden subdividir también en varios canales para voz, vídeo y datos. Los más modernos enlaces T3 ofrecen velocidades de hasta 44.736Mbits por segundo. Estas velocidades son apropiadas para las grandes empresas que necesitan centralizar sistemas de procesamiento para aplicaciones vitales. Los usuarios remotos necesitan un enlace a gran velocidad para mantener un nivel razonable de rendimiento.

2.3.2 Conexión remota entre una estación remota y una red local.

La conexión se puede establecer a través de modems y líneas telefónicas estándar, en tales conexiones se han de tener en cuenta tanto la seguridad como la velocidad de transmisión. Netware ofrece seguridad mediante restricciones en la conexión de los usuarios remotos, similares a las de los usuarios locales. El software de comunicaciones de Novell también permite llamar de nuevo al usuario remoto tras la llamada inicial, asegurándose así de qùe el punto remoto es el que ha sido autorizado para conectarse. Respecto a la velocidad de comunicación, siempre que sea posible, se usaran los módems de alta velocidad. Existen además paquetes como Norton Lambert close-Up o el PC-Any-Ware, que permiten a las estaciones de trabajo remotas acceder a la red como si estuvieran conectadas directamente. A través de la conexión sólo se transmite la información de pantalla y las ordenes de teclado, mejorando de esta forma el acceso.

Estos paquetes necesitan una máquina local dedicada a llevar a cabo las tareas de procesamiento del usuario remoto.

Métodos de Ejecución

Existen dos métodos para sesiones con estaciones remotas:

a) Ejecución remota.

Todo el procesamiento tiene lugar en la estación remota. Todos los archivos de programas y datos tienen que ser transmitidos por las líneas de comunicaciones para ser procesados en la estación del usuario, salvo cuando los archivos ya hayan sido copiados previamente en la estación. Este método no es recomendable si se necesita transferir grandes cantidades de información por las líneas. Resulta útil en conexiones ocasionales para usuarios que envían o reciben uno o dos archivos hacia o desde la red local.

b) Ejecución local.

Este método conecta la estación remota con una estación dedicada de la red local. Todo el procesamiento se lleva a cabo en la estación dedicada; la visualización de la pantalla es reflejada en la estación remota, y el usuario puede introducir órdenes en el teclado.

Envío de datos.

Viendo el protocolo del modelo OSI como escalones, la información que se envía baja por la escalera en su recorrido hacia el cable, mientras que la información que se recibe sube la escalera.

a) Nivel 7.

En el séptimo nivel del modelo OSI, el nivel de aplicación. El texto se introduce en una estación utilizando una aplicación que ofrece una interfaz de usuario. La aplicación puede ser un sistema de correo electrónico que solicita el nombre y la dirección del receptor.

b) Nivel 6.

En el sexto nivel del modelo OSI, el nivel de presentación. Se encarga de la presentación de caracteres, números y otra información. Si los datos van a ser usados por un tipo de aplicación o computadora distintas, puede que sea necesario realizar alguna conversión.

c) Nivel 5.

En el quinto nivel del modelo OSI, el de sesión. En una red, las estaciones emisora y receptora tienen que utilizar los mismos parámetros de comunicaciones. El nivel de sesión coordina y sincroniza los dos sistemas, y mantiene la sesión de comunicaciones.

d) Nivel 4.

En el cuarto nivel del modelo OSI, el de transporte. Aísla a las capas superiores de los detalles de la red. En algunos casos, la aplicación es libre de realizar a otras tareas mientras los datos son transferidos en segundo plano.

e) Nivel 3.

En el tercer nivel del modelo OSI, el de red. Define como va a fluir la información de una estación a otra. Si existe una conexión entre redes, puede que sea necesario dirigir los paquetes hacia dispositivos especiales que separan una red de otra.

f) Nivel 2.

En el segundo nivel del modelo OSI, el de enlace de datos. Se preparan los paquetes de datos para su envío por la red. Este nivel tiene un enlace directo con la placa de red y su conexión con la red.

g) Nivel 1.

Al primer nivel, el nivel físico. Es el sistema de cableado.

Cuando el paquete llega a su destino, se invierte el proceso cuando el destinatario recibe el paquete. El usuario abre el paquete y el archivo, que será presentado en la pantalla usando una aplicación.

Una vez que ya se estudiaron algunos de los antecedentes que consideramos importantes y básicas para nuestra propuesta de conectividad remota para TESYS, en el próximo capítulo procederemos al estudio y explicación de las generalidades de telecomunicaciones que consideramos indispensables para el desarrollo de este trabajo de investigación.

CAPÍTULO 3

GENERALIDADES DE TELECOMUNICACIONES

3.1 EL MODELO OSI

3.1.1 Antecedentes del Modelo OSI

Durante los años 60 y 70 se crearon muchas tecnologías de redes, cada una basada en un diseño específico de hardware. Estos sistemas eran construidos de una sola pieza, lo que podríamos llamar una arquitectura monolítica; esto significa que los diseñadores debían ocuparse de todos los elementos involucrados en el proceso; podemos suponer que estos elementos forman una cadena de transmisión que tiene diversas partes: Los dispositivos físicos de conexión, los protocolos software y hardware usados en la comunicación; los programas de aplicación que realizaban la comunicación y la interfaz hombre-máquina que permiten al humano utilizar la red. Este modelo, que considera la cadena como un todo monolítico, es poco práctico, pues el más pequeño cambio puede implicar alterar todos sus elementos.

El diseño original de Internet del Departamento de Defensa Americano disponía un esquema de cuatro capas, aunque data de los 70 es más o menos el que se sigue utilizando:

Capa Física.

La capa Física o de Acceso de Red ("Network Access Layer"), es la responsable del envío de la información sobre el sistema hardware utilizado en cada caso; se utiliza un protocolo distinto según el tipo de red física.

Capa de red.

La capa de red también llamada capa Internet ("Internet Layer"), es la responsable de enviar los datos a través de las distintas redes físicas que pueden conectar una máquina origen con la de destino de la información. Los protocolos de transmisión como el IP están íntimamente asociados a esta capa.

Capa de Transporte.

La Capa de transporte ("Host-to-Host Layer") controla el establecimiento y fin de la conexión, control de flujo de datos, retransmisión de datos perdidos y otros detalles de la transmisión entre dos sistemas. Los protocolos más importantes a este nivel son TCP y UDP (mutuamente excluyentes).

Capa de aplicación.

La capa de aplicación ("Application layer"), conformada por los protocolos que sirven directamente a los programas de usuario, navegador, e-mail, FTP, TELNET, etc.
Respondiendo a la teoría general imperante el mundo de la computación, de diseñar el hardware por módulos y el software por capas, en 1978 la organización ISO (International Standards Organization), propuso un modelo de comunicaciones para redes al que titularon "The reference model of Open Systems Interconnection", generalmente conocido como modelo OSI. Su filosofía se basa en descomponer la funcionalidad de la cadena de transmisión en diversos módulos, cuya interfaz con los adyacentes esté estandarizada. Esta filosofía de diseño presenta una doble ventaja: El cambio de un módulo no afecta necesariamente a la totalidad de la cadena; además, puede existir una cierta interoperabilidad entre diversos productos y fabricantes hardware/ software, dado que los límites y las interfases están perfectamente definidas. Esto supone por ejemplo, que dos software de comunicación distinta puedan utilizar el mismo medio físico de comunicación.

El modelo de comunicaciones para redes OSI, aunque inspirado en el de Internet no tiene más semejanzas con aquél. Está basado en un modelo de siete capas, mientras que el primitivo de Internet estaba basado en 4 capas, actualmente todos los desarrollos se basan en este modelo de 7 niveles que son los siguientes: 1 Físico; 2 de Enlace; 3 de Red; 4 de Transporte; 5 de Sesión; 6 de Presentación y 7 de Aplicación. Cada nivel realiza una función concreta, y está separado de los adyacentes por interfaces conocidas, sin que le incumba ningún otro aspecto del total de la comunicación.

3.1.2 Funcionamiento de las capas del modelo OSI

La descripción esquemática de las diversas capas o niveles que componen este modelo es como sigue:

Nivel 1 Capa física.

("Physical layer"); es la encargada de transmitir los bits de información por la línea o medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si esta es uni o bidireccional (simplex, duplex o full-duplex); también de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas. Por ejemplo, este nivel define la medidas del cable coaxial Ethernet y de los conectores BNC utilizados. Otro ejemplo de estándares relativos a esta capa son RS-232 (para más detalle ver el glosario de términos) para comunicaciones serie y X.21

Nivel 2 Capa de enlace

("Data Link layer"). Esta capa especifica como se organizan los datos cuando se transmiten en un medio particular. Por ejemplo esta capa define como son los cuadros ("Frames"), las direcciones y las sumas de control ("Checksum") de los paquetes Ethernet. Se ocupa del direccionamiento local, detección de errores ocurridos en la capa física, y control del acceso a dicha capa. Agrupa la información a transmitir en bloques ("Frames"), e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad. Los datagramas recibidos son comprobados por el receptor. Si algún datagrama se ha corrompido se envía un mensaje de control al remitente solicitando su reenvío. El protocolo PPP (para más detalle ver el glosario de términos) es ejemplo de esta capa.
La capa de enlace puede considerarse dividida en dos subcapas:

a). Control lógico de enlace LLC ("Logical Link Control")

Define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.

b). Control de acceso al medio MAC ("Medium Access Control").

Se encarga de arbitrar la utilización del medio físico cuando varios equipos compiten por su utilización simultánea. El mecanismo CSMA/ CD ("Carrier Sense Multiple Access with Collision Detection") utilizado en Ethernet (para más detalle ver el glosario de términos) es un típico ejemplo de esta subcapa.

Nivel 3 Capa de Red

("Network layer"). Esta capa se ocupa de la transmisión de los datagramas (paquetes) y de encaminar cada uno en la dirección adecuada ("Routing"), esta tarea puede ser complicada en redes grandes como Internet, pero no se ocupa para nada de los errores o pérdidas de paquetes.

Por ejemplo, define la estructura de direcciones y rutas de Internet. Esta capa puede considerarse subdividida en dos:
a). Transporte.

Encargada de encapsular los datos a transmitir (de usuario).

b). Conmutación ("Switching").

Esta parte es la encargada de intercambiar información de conectividad específica de la red (su actividad es raramente percibida por el usuario)
Los protocolos más frecuentemente utilizados en esta capa son dos: X.25 e IP ("Internet Protocol") (para más detalle ver el glosario de términos).

Nivel 4 Capa de Transporte

("Transport layer"); esta capa se ocupa de garantizar la fiabilidad del servicio, describe la calidad y naturaleza del envío de datos. Por ejemplo esta capa define cuando y como debe utilizarse la retransmisión para asegurar su llegada. Para ello divide el mensaje recibido de la capa de sesión en trozos (datagramas), los numera correlativamente y los entrega a la capa de red para su envío. Durante la recepción, si la capa de Red utiliza el protocolo IP, la capa de Transporte es responsable de reordenar los paquetes recibidos fuera de secuencia. Un ejemplo típico de protocolo usado en esta capa es TCP ("Transport Control Protocol"), que con su homólogo IP de la capa de Red, configuran la suite TCP/IP, utilizada en Internet.

Nivel 5 Capa de Sesión

("Session Layer"); es una extensión de la capa de transporte que ofrece control de diálogo y sincronización, aunque en realidad son pocas las aplicaciones que hacen uso de ella. Por ejemplo, las comunicaciones de Internet no la utilizan.

Nota: Algunos autores indican que la capa de sesión es meramente una consideración teórica de los autores del modelo sin absolutamente ninguna utilidad práctica conocida.

Nivel 6 Capa de Presentación

("Presentation layer"); Esta capa se ocupa de los aspectos semánticos de la comunicación (describe la sintaxis de los datos a transmitir), estableciendo los arreglos necesarios para que puedan comunicar máquinas que utilicen diversa representación interna para los datos. Por ejemplo describe como pueden transferirse números de coma flotante entre equipos que utilizan distintos formatos matemáticos. En realidad esta capa puede estar ausente, ya que son pocas las aplicaciones que hacen uso de ella. Esta capa es buena candidata para implementar aplicaciones de criptografía.

Nota: Con esta capa ocurre algo parecido a la anterior. En teoría cliente y servidor debían negociar el formato a utilizar, y esta función, y el correspondiente formateo de los datos, sería el objeto de esta capa. Actualmente el panorama ha cambiado; solo existe una opción para el formato de datos, a pesar de lo cual el protocolo OSI sigue negociando un esquema de codificación (el único disponible). En Internet, el único servicio que utiliza esta capa es justamente TELNET, que justamente es un servicio de acceso a servidores desde terminales remotos. En este caso, la capa de presentación es la que se encarga de configurar su terminal para conectar a un servidor de características particulares.

Nivel 7 Capa de Aplicación

("Application layer"); Esta capa describe como hacen su trabajo los programas de aplicación (navegadores, clientes de correo, terminales remotos, transferencia, etc.). Por un lado interactúan con la capa de presentación; por otro representan la interfaz con el usuario, entregándole la información y recibiendo los comandos que dirigen la comunicación.
A continuación una tabla que resume el funcionamiento de cada uno de los niveles del modelo OSI:

1	Físico	Se ocupa de la transmisión del flujo de bits a través del medio.	Cables, tarjetas y repetidores (hub). RS-232, X.21.
2	Enlace	Divide el flujo de bits en unidades con formato (tramas) intercambiando estas unidades mediante el empleo de protocolos.	Puentes (bridges). HDLC y LLC.
3	Red	Establece las comunicaciones y determina el camino que tomarán los datos en la red.	Ruteadores IP, IPX.
4	Transporte	La función de este nivel es asegurar que el receptor reciba exactamente la misma información que ha querido enviar el emisor y a veces asegura al emisor que el receptor ha recibido la información que le ha sido enviada. Envía de nuevo lo que no haya llegado correctamente.	Pasarela (gateway). UDP, TCP, SPX.
5	Sesión	Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado. Proporciona los pasos necesarios para entrar en un sistema utilizando otro. Permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez (sesiones).	Gateway.
6	Presentación	Conversión entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de ficheros con características diferentes.	Gateway. Compresión, encriptado, VT100.
7	Aplicación	Este nivel proporciona unos servicios estandarizados para poder realizar unas funciones específicas en la red. Las personas que utilizan las aplicaciones hacen una petición de un servicio (por ejemplo un envío de un fichero). Esta aplicación utiliza un servicio que le ofrece el nivel de aplicación para poder realizar el trabajo que se le ha encomendado (enviar el fichero).	X.400

Tabla 3.1 Dispositivos y Protocolos

3.2 SEÑALES

3.2.1 Señales Analógicas

Una señal x (t) es una función real o escalar de la variable de tiempo t. Por "real" se quiere decir que para cualquier valor fijo de la variable de tiempo t, el valor de la señal en el tiempo t es un número real. Cuando la variable de tiempo t toma sus valores en el conjunto de los números reales, se afirma que t es una variable de tiempo continuo y que la señal x (t) es una señal de tiempo continuo o una señal analógica.

Tipos comunes de señales analógicas son las formas de onda del voltaje y de la corriente en un circuito eléctrico, y las señales bioeléctricas como las de un electrocardiograma (ECG) o las de un electroencefalograma (EEG). Otras clases comunes de señales analógicas son las fuerzas y los pares motor aplicados a dispositivos mecánicos, las posiciones angulares o las velocidades angulares del rotor en un motor, o en una transmisión de un robot industrial y las velocidades de flujo de los líquidos o de los gases en un proceso químico.

Muchas señales que suceden en la práctica no se pueden modelar con exactitud mediante funciones matemáticas. Un ejemplo es la señal de voz que se especifica a menudo mediante un conjunto de valores de muestra.

Dos ejemplos sencillos de señales analógicas o de tiempo continuo son la función escalón unitario u (t) y la función rampa unitaria r (t).Los dibujos de estas dos funciones se muestran a continuación.

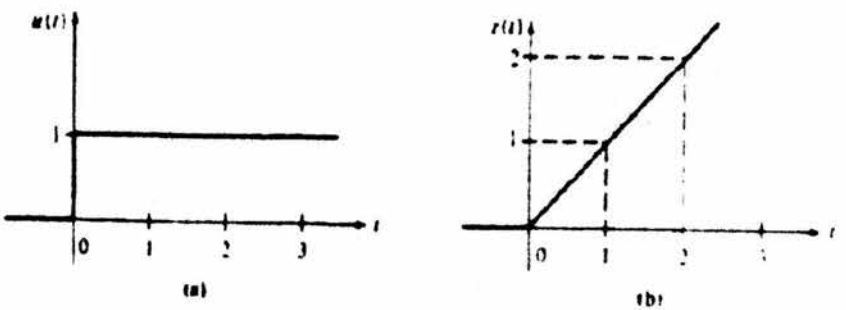


Fig. 3.1. Funciones (a) escalón unitario y (b) rampa unitaria.

Función escalón

La función escalón unitario u (t) se define en forma matemática como:

$$U(t) = \begin{cases} 1, & t \geq 0 \\ 0, & t < 0 \end{cases}$$

En este caso "escalón unitario" significa que la amplitud de u (t) es igual a 1 para t ≥ 0. Obsérvese que se ajusta a al convención de u (0) = 1. Desde un punto de vista estrictamente matemático, u (t) no esta definida en t = 0. No obstante, siempre se considera que u (0) = 1. Si K es un número arbitrario no nulo, entonces Ku(t) es la función escalón de amplitud K para T ≥ 0.

Para cualquier señal de tiempo continuo x (t), el producto de x (t) u (t) es igual x (t) para t ≥ 0 y es igual a 0 para t< 0. Por lo tanto, la multiplicación de una señal x (t) por u (t) elimina cualesquiera valores no nulos de x (t) para t < 0.

Función Rampa Unitaria

La función rampa unitaria r (t) se define en forma matemática como:

$$R(t) = \{t, \quad t \geq 0$$

$$0, \quad t < 0$$

Obsérvese que para t ≥ 0 la pendiente r (t) es igual a 1. Así r (t) tiene una pendiente unitaria, lo cual es la razón de llamarla función rampa unitaria. Si K es un escalar (numero real) arbitrario no nulo, entonces la función rampa Kr(t) tiene una pendiente K para t ≥ 0.

$$r(t) = \int_{-\infty}^{t} u(\lambda)\, d\lambda.$$

De manera reciproca, la primera derivada de r (t) con respecto a t es igual a u (t), excepto en t = 0, donde no esta definida la derivada de r (t).

Función Sinusoide

Un ejemplo muy común de una señal de tiempo continuo es la sinusoide A cos de (ωt + θ). En este caso A es la amplitud, ω es la frecuencia en radianes por segundo (Rad. /seg.), y θ es la fase en radianes. La frecuencia f en ciclos por segundo o hertz (Hz) es f = ω / 2π.

Para cualquier valor de la variable de tiempo t, se tiene que:

$$A \cos [\omega (t + 2\pi/\omega) + \theta] = A\cos (\omega t + 2\pi + \theta) = A \cos (\omega t + \theta).$$

Por tanto a la sinusoide se repite cada 2π/ω segundos; en otras palabras, la sinusoide es una señal periódica con un periodo igual a 2π/ω. En la siguiente figura aparece dibujada la sinusoide para el caso en que –π/2 < θ < 0. Obsérvese que si θ = -π/2 entonces A cos (ωt + θ) = A sen ωt.

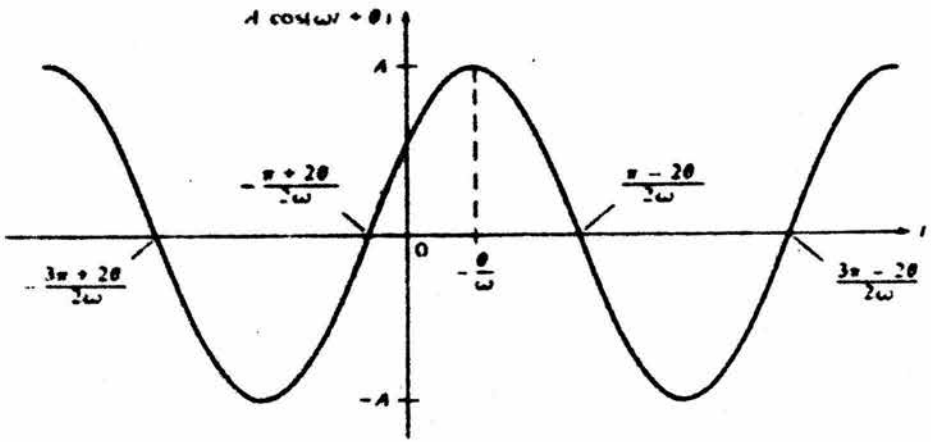


Fig. 3.2. La sinusoide A cos (ωt + θ), donde $-\pi/2 < \theta < 0$

Función Impulso

El impulso unitario δ (t), también conocido como la función delta o la distribución de Dirac, se define como:

$$\Delta (t) = 0, \quad t \neq 0$$

$$\int_{-\epsilon}^{\epsilon} \delta(\lambda)\, d\lambda = 1 \qquad \text{para cualquier número real } \epsilon > 0.$$

La primera condición establece que δ (t) es igual a cero para todos los valores no nulos de t, en tanto la segunda condición establece que el área bajo el impulso es igual a 1, por lo que δ (t) tiene un área unitaria.

Es importante señalar que el valor δ (0) de δ (t) en t = 0 no esta definido; en particular, δ (0) no es igual a infinito. El impulso unitario no es en realidad una función. En matemáticas, δ (t) se define mediante una función lineal sobre un espacio de funciones de prueba. No se considera esta definición.

Puesto que δ (t) no es una función no es posible generar una función real que tenga exactamente las mismas propiedades que δ (t). Sin embargo, se puede considerar a δ (t) como un impulso centrado en el origen con una amplitud A y una duración 1/A, donde A es un número positivo muy grande. La interpretación como impulso de δ (t) se muestra en la figura siguiente.

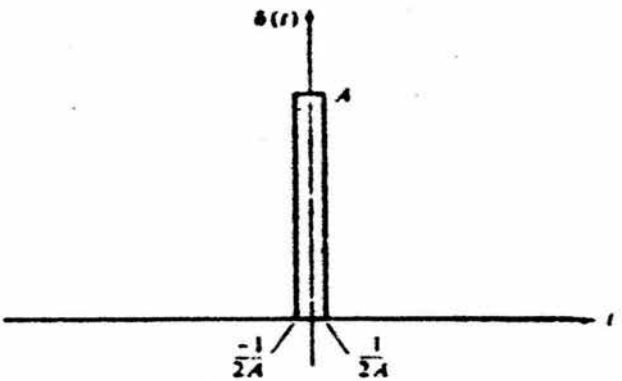


Figura 3.3 La interpretación del impulso de δ (t).

Con respecto a cualquier número real K, Kδ(t) es el impulso que tiene un área K, Se define como:

$$K\delta(t) = 0, \quad t \neq 0$$

$$\int_{-\epsilon}^{\epsilon} K\delta(\lambda)\, d\lambda = K \qquad \text{para cualquier número real } \epsilon > 0.$$

La función escalón unitario u (t) es igual a la integral del impulso δ (t); en forma mas precisa, se tiene que:

$$u(t) = \int_{-\infty}^{t} \delta(\lambda)\, d\lambda, \quad \text{todo } t \text{ excepto } t = 0.$$

Para verificar esta relación, obsérvese primero que para t < 0,

$$\int_{-\infty}^{t} \delta(\lambda)\, d\lambda = 0, \quad \text{desde } \delta(t) = 0 \text{ para todo } t < 0.$$

Para t > 0,

$$\int_{-\infty}^{t} \delta(\lambda)\, d\lambda = \int_{-\epsilon}^{t} \delta(\lambda)\, d\lambda = 1, \quad \text{desde } \int_{-\epsilon}^{\epsilon} \delta(\lambda)\, d\lambda = 1 \text{ para todo } \epsilon > 0.$$

3.2.2 Señales Digitales

Sea {a1, a2, a3,...aN} un conjunto de N números reales. Una señal digital x (KT) es una señal de tiempo discreto, cuyos valores pertenecen al conjunto finito {a1, a2,...aN}; esto es, en cada punto del tiempo KT, xK (T) = ai para alguna i, donde $1 \leq i \leq N$. De esta manera, una señal digital solo puede tener un número finito de valores diferentes.

Una señal de tiempo continuo de muestreo no es necesariamente una señal digital. Por ejemplo, la función rampa unitaria muestreada no es una señal digital puesto que r (KT) alcanza una infinidad de valores cuando K =,-2,-1,0,1,2,...

Una señal binaria es una señal digital cuyos valores son iguales a 1 o a 0; esto es, x (kt) = 0 o 1 para K =,-2,-1,0,1,2,... La función escalón unitario muestreada y la función pulso unitario son ejemplos de señales binarias.

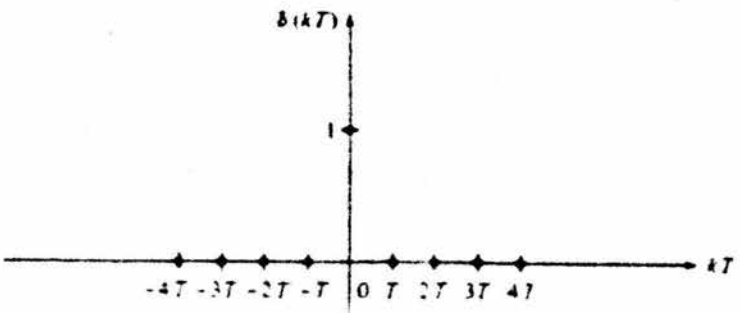


Fig. 3.4 Función escalón unitario muestreada.

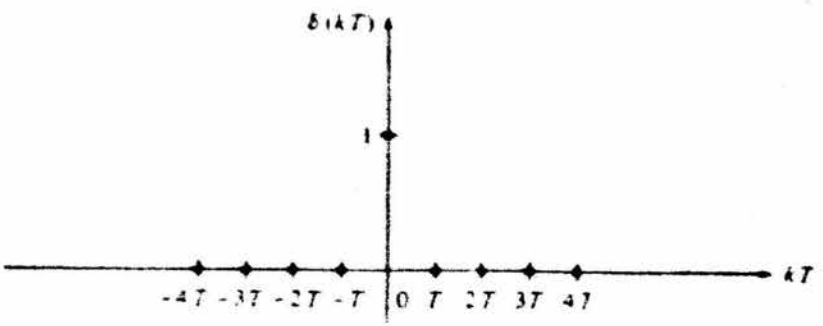


Fig. 3.5 Función pulso unitario.

3.2.3 Señales Periódicas

Sea T un número real positivo fijo. Se dice que una señal de tiempo continuo x (t) es periódica con periodo T sí

$$x(t + T) = x(t) \quad \text{para todo } t, \quad -\infty < t < \infty.$$

El periodo T es el mínimo número positivo para el cual se satisface la expresión anterior.

Debido a la propiedad anterior, una señal periódica se repite cada T segundos. Por ejemplo, x (t) = A cos ωt y x (t) = A sen ωt son señales periódicas con periodo 2π/ω. La forma de onda que se muestra en la siguiente figura es periódica con periodo T = 4.

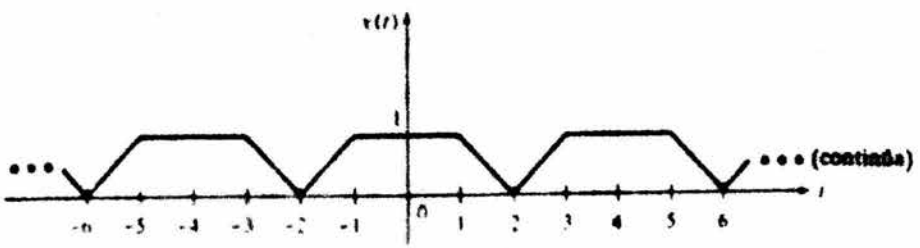


Fig. 3.6 Señal periódica con T = 4

Sea x (t) una señal periódica con periodo T. Entonces, por el teorema de Fourier, x (t) se puede expresar como una suma (en general, finita) de sinusoides.

$$x(t) = c_0 + \sum_{n=1}^{\infty} 2|c_n| \cos(n\omega_0 t + \measuredangle c_n), \qquad -\infty < t < \infty.$$

La expresión anterior par x (t) se conoce como la serie trigonométrica de fourier de la señal periódica x (t).

En la representación anterior, ωo 4es la frecuencia fundamental (en Rad. /seg.) de x(t) dada por ωo = 2π/T, donde T es el periodo. El numero co es la componente constante o de c.d. de x (t) dada por

$$c_0 = \frac{1}{T}\int_{-T/2}^{T/2} x(t)\,dt.$$

Para n = 1, lcnl es la magnitud y ∟cn es el ángulo del número complejo cn = lcnl exp (j ∟cn). Para n = 1, cn está dada por

$$c_n = \frac{1}{T}\int_{-T/2}^{T/2} x(t)e^{-jn\omega_0 t}\,dt.$$

La cn se puede calcular al integrar la expresión anterior sobre cualquier periodo completo; esto es, para cualquier numero real h,

$$c_n = \frac{1}{T}\int_{h}^{T+h} x(t)e^{-jn\omega_0 t}\,dt.$$

La componente 2 lcnl cos (nωot + ∟cn) de la serie trigonométrica de Fourier se conoce como la n-ésima armónica de la señal periódica x (t). En este caso el término é nesima armónica se refiere al hecho de que la frecuencia nωo de esta componente es n veces de la frecuencia fundamental ωo. El numero 2 lcnl es el valor pico de la n-ésima armónica.

3.2.4 Señales no Periódicas

Por medio de la transformada de Fourier es posible definir las nociones de espectros de amplitud y de fase para las señales no periódicas o aperiódicas. Los espectros asociados con una señal no periódica están definidos para todos los valores reales de ω, no solo para valores discretos de ω como en el caso de una señal periódica. La transformada de Fourier se puede generar al considerar la representación en serie de Fourier de una señal periódica. Sea x (t) una señal de tiempo continuo con x (t) = 0 para todo t > T1 y x (t) = 0 para todo t < -T1 donde >T1 es algún número positivo fijo. Se dice que dicha señal es limitada en el tiempo o que es de duración finita. Es claro que una señal x (t) limitada en el tiempo no puede ser periódica.

Dado un número positivo T > 2T1, sea $\tilde{x}_T$ (t) la señal periódica con periodo T que es igual a x (t) para –T/2 < t < T/2; esto es

$$\tilde{x}_T(t + nT) = x(t), \qquad \frac{-T}{2} < t < \frac{T}{2}, \quad n = 0, \pm 1, \pm 2,$$

Por ejemplo supongamos que x (t) es la señal que se muestra en la siguiente figura.

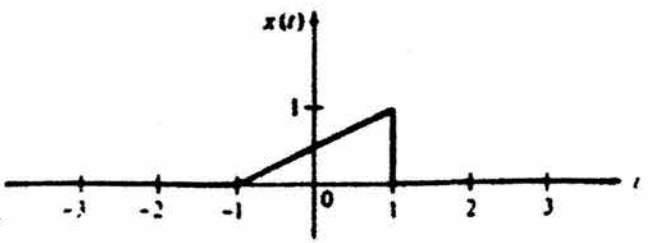


Fig. 3.7 Señal no periódica

Entonces cuando T = 3, $\tilde{x}_T(t)$ es la señal periódica que aparece a continuación.

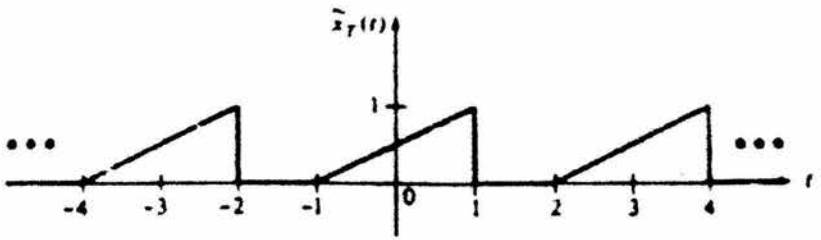


Figura. 3.8 Señal periódica

Por definición de $\tilde{x}_T(t)$, se tiene que

$$x(t) = \lim_{T \to \infty} \tilde{x}_T(t).$$

Ahora, como $\tilde{x}_T(t)$ es periódica, tiene la serie exponencial de fourier

$$\tilde{x}_T(t) = \sum_{n=-\infty}^{\infty} c_n e^{jn\omega_0 t},$$

Donde:

$$c_n = \frac{1}{T}\int_{-T/2}^{T/2} x(t)e^{-jn\omega_0 t}\,dt, \qquad n = 0, \pm 1, \pm 2, \ldots .$$

Puesto que $\tilde{x}_T(t) = x(t)$ para $-T/2 < t < T/2$ y $x(t) = 0$ para $t > T/2$ y $t < -T/2$, la expresión anterior para cn.

$$c_n = \frac{1}{T}\int_{-\infty}^{\infty} x(t)e^{-jn\omega_0 t}\,dt.$$

Ahora, definase

$$X(\omega) = \int_{-\infty}^{\infty} x(t)e^{-j\omega t}\,dt$$

Entonces

$$X(n\omega_0) = \int_{-\infty}^{\infty} x(t)e^{-jn\omega_0 t}\,dt, \qquad n = 0, \pm 1, \pm 2, \ldots ,$$

y así se reduce a

$$c_n = \frac{1}{T}X(n\omega_0), \qquad n = 0, \pm 1, \pm 2, \ldots .$$

Al sustituir esta última expresión en $\tilde{x}_T(t)$ se tiene

$$\tilde{x}_T(t) = \sum_{n=-\infty}^{\infty} \frac{1}{T}X(n\omega_0)e^{jn\omega_0 t}$$

$$= \frac{1}{2\pi}\sum_{n=-\infty}^{\infty} X(n\omega_0)e^{jn\omega_0 t}\omega_0, \quad \text{cuando } T = \frac{2\pi}{\omega_0}.$$

Ahora, cuando T - ∞, se tiene nωo → ω, ωo → dω suma de la derecha de la expresión anterior converge a al integral

$$\int_{-\infty}^{\infty} X(\omega)e^{j\omega t}\,d\omega.$$

Entonces, como $\tilde{x}_T(t) \rightarrow x(t)$ cuando T → ∞, se tiene que

$$x(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} X(\omega)e^{j\omega t}\,d\omega.$$

Esta última expresión es la representación integral de Fourier de la señal x (t) no periódica y la función x (ω) es la transformada de Fourier de x (t).

3.2.5. Dominio del tiempo y la frecuencia

Una onda senosoidal queda totalmente definida mediante su amplitud, frecuencia y fase. La traza en el dominio del tiempo muestra los cambios de la amplitud de la señal con respecto al tiempo (es una representación de la amplitud respecto al tiempo). De modo que una representación en el domino del tiempo no es posible medir la fase y la frecuencia de la señal.

Para medir la relación entre la amplitud y la frecuencia, se puede utilizar lo que se denomina una traza en el dominio de la frecuencia. En la siguiente figura se compara el dominio del tiempo (amplitud instantánea con respecto al tiempo) y el dominio de la frecuencia (máxima amplitud con respecto a la frecuencia).

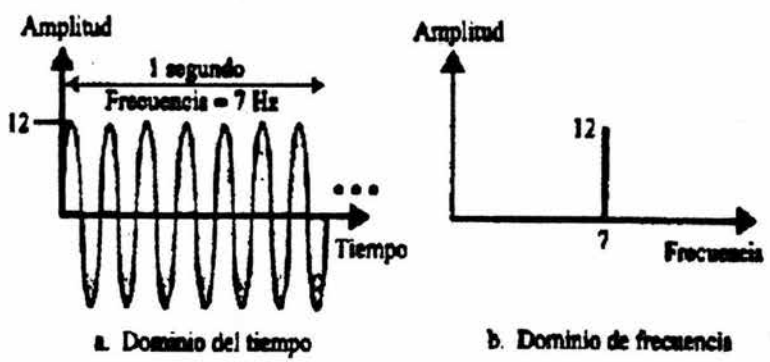


Figura 3.9 Comparación entre los dominios del tiempo y de la frecuencia.

La siguiente figura nos muestra ejemplos de trazas en el dominio del tiempo y la frecuencia para mostrar que tipo de información se adapta mejor a cada traza.

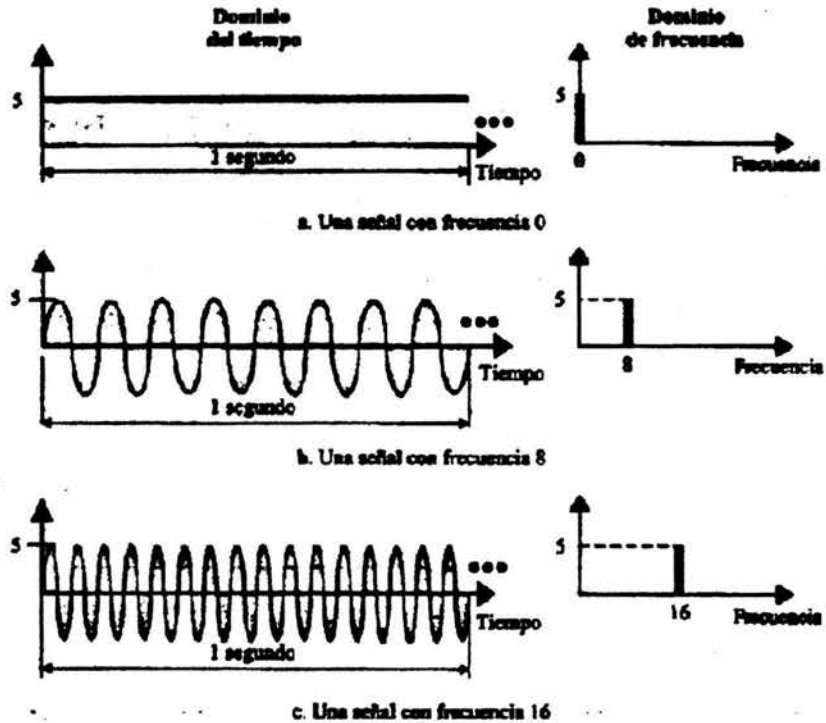


figura 3. 10 Trazas en el dominio del tiempo y la frecuencia.

De las graficas anteriores podemos deducir que una señal con una frecuencia baja en el domino de la frecuencia corresponde a una señal con un periodo largo en el dominio del tiempo, y una señal con cambios rápidos en el dominio del tiempo corresponde a una señal con frecuencias altas en el dominio de la frecuencia, es decir, los periodos en ambos dominios son proporcionales.

Anteriormente hemos hablado de las señales periódicas en forma senosoidal, sin embargo nos hace falta considerar otra clase de ondas que no están formadas por curvas suaves, ni presentan una amplitud máxima y mínima pero si muestran constancia en su forma; este tipo de señales son muy útiles en el análisis de señales. De hecho, se puede demostrar que cualquier tipo de onda periódica se puede representar como un con conjunto de ondas senosoidaldes.

Señales Descompuestas.

El concepto de la descomposición de señales se puede ver fácilmente con el siguiente ejemplo. La figura 3.11 nos muestra una señal periódica descompuesta en dos ondas senosoidales. La primera onda seno (traza central) tiene una frecuencia de 6 mientras que la segunda onda seno tiene una frecuencia 0.

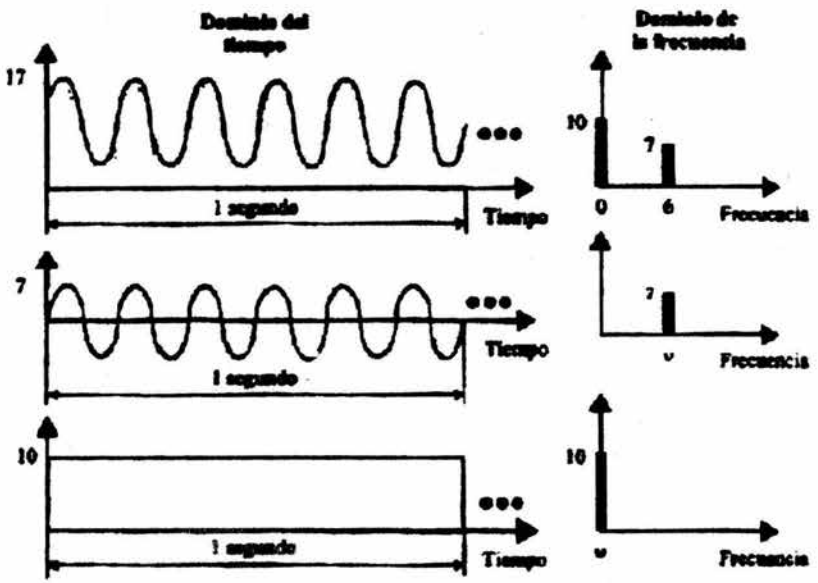


Figura 3.11 Señal periódica descompuesta

Sumando ambas graficas punto por punto se obtiene como resultado la grafica de la parte superior. Observe que la señal original se parece a una onda seno que tiene el eje de tiempo desplazado hacia abajo. La amplitud media de la señal no es 0. Este factor implica la presencia de un componente de frecuencia 0, denominado componente de corriente continua (DC, Direct Current). Este componente de DC es el responsable del desplazamiento hacia arriba en diez unidades de la onda seno.

3.2.6 Espectro de frecuencia y ancho de banda

Para continuar nuestro análisis, es necesario mencionar dos nuevos términos: espectro y ancho de banda.

Espectro de frecuencia.

El espectro de frecuencia de una señal es la colección de todas las frecuencias componentes que contiene y se muestra representado en un grafico en el dominio de la frecuencia.

Ancho de banda.

El ancho de banda de una señal es el ancho del espectro de frecuencia (ver figura 3.12).

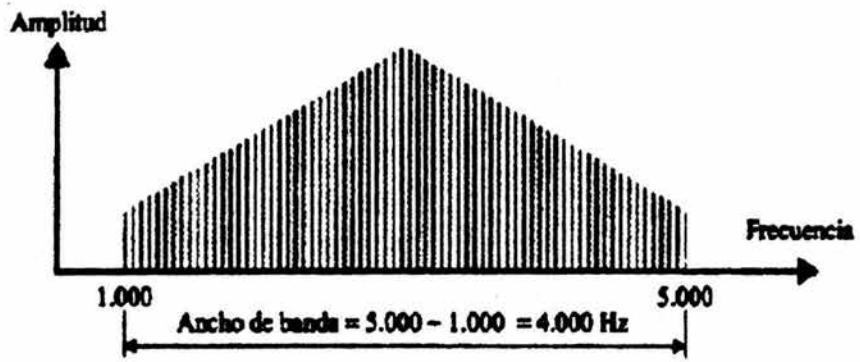


figura 3.12 Espectro y ancho de banda

En otras palabras, el ancho de banda se refiere al rango de las frecuencias componentes y el espectro de frecuencias esta relacionado con los elementos dentro de ese rango. Para determinar el ancho de banda, hay que sustraer la frecuencia mas baja de la frecuencia más alta del rango.

3.3 MODULACIÓN

La Modulación es la Técnica empleada para modificar una señal con la finalidad de posibilitar el transporte de informaciones a través de un canal de comunicación y recuperar la señal en su forma original en la otra extremidad.

Son posibles dos técnicas para la transmisión de datos la analógica y la digital. Solamente la analógica realiza modulación. Una vez que la digital usa un recurso de codificación de pulsos.

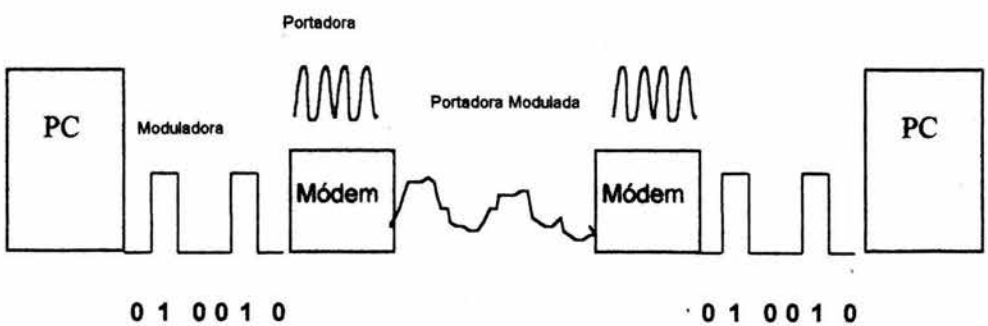


Figura 3.13. Esquema general de la modulación de una señal digital.

3.3.1 Modulación Digital

Los Módem digitales no ejecutan exactamente una modulación, sino una especie de codificación de una señal que difiere mucho con relación a una señal analógica generada por los Módem analógicos.

Técnicas de Modulación Digital

Los códigos básicos para lograr la modulación digital son:

a) Código NRZ (NonReturn to Zero – Código sin Retorno a Cero). En este tipo de código se usa un voltaje positivo para referenciar un 1 binario y un voltaje negativo para representar un 0 binario sin que la señal regrese a un valor de 0 volts en ausencia de señal.

b) Código RUZ (Return to Zero – Código de Retorno a Cero). También se le conoce como código Neutral debido a que solo posee un valor único positivo en volts para representar un 1 binario y cero volts para representar un 0 binario.

c) Código Bipolar La señal puede adquirir tres niveles.

d) Código con inversión alterada del uno (AMI): Utiliza los pulsos de diferente polaridad.

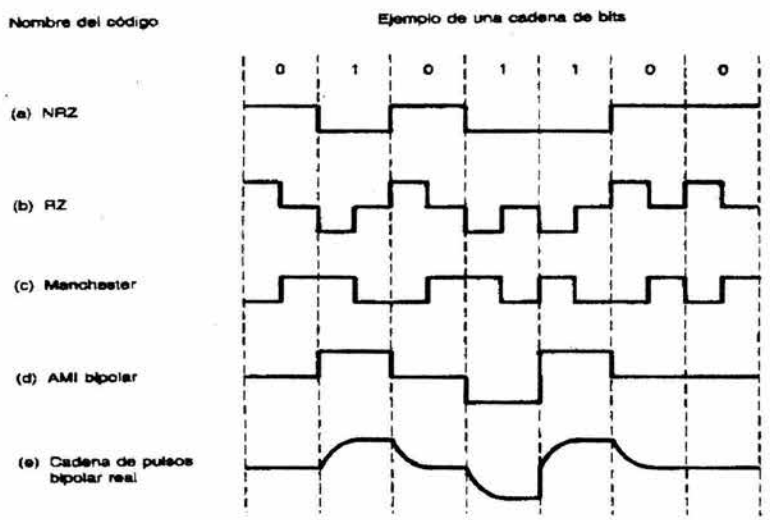


Figura 3.14. Formas de onda de la transmisión digital de datos

3.3.2 Modulación Analógica

Una señal digital generada por el equipo de procesamiento de datos es generada en la onda portadora generada por el módem, siendo que las características originales de la onda padrón son modificadas de acuerdo a la técnica de modulación utilizada por el módem y esta transporta los datos hasta la otra extremidad del enlace donde otro módem demudará la señal y la entregará a un equipo de procesamiento de datos en su forma original.

Las técnicas de modulación analógica son las siguientes:

a). ASK (Amplitud Shift – Keying – Codificación por cambio en la Amplitud).

b). FSK (Frecuency Shift Keying - Codificación por cambio de frecuencia).

c). PSK (Phase Shift – Keying – Codificación por Cambio de Face).

d). DPSK (Differential Phase Shift – Keying – Codificación por Cambio de Face Diferencial).

e). QAM (Quadrature Amplitude Modulation – Modulación por Amplitud en Cuadratura).

Modulación ASK

La amplitud de la onda es alterada de acuerdo con la variación de la señal de información. Exige un medio en que la respuesta de amplitud sea estable, ya que este tipo de modulación es bastante sensible a ruidos y distorsiones.

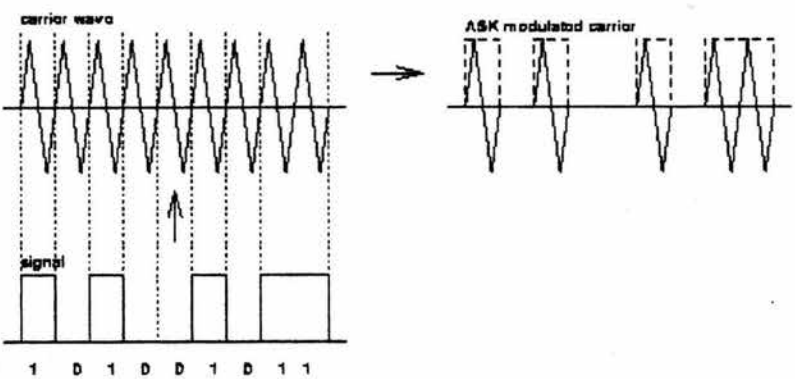


Figura 3.15. ASK (Amplitud Shift – Keying – Codificación por cambio en la Amplitud).

Modulación FSK

Consiste en un procedimiento de 2 osciladores con Frecuencias Diferentes para dígitos 0 y 1. Normalmente es usada para transmisión de datos en bajas velocidades y puede ser:

a). Coherente: Donde no ocurre variación de fase de la portadora para dígitos del mismo valor.

b) No Coherente: Donde puede ocurrir variación de fase de la portadora para dígitos del mismo valor. (Ver Figura 3.16)

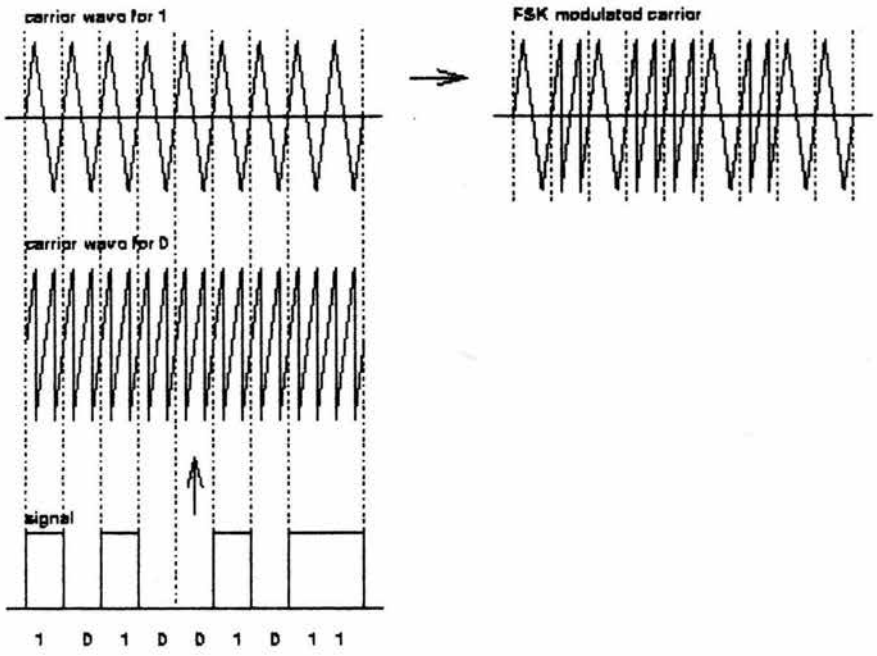


Figura 3.16. FSK (Frecuency Shift Keying - Codificación por cambio de frecuencia)

Modulación PSK

Consiste en un procedimiento de la onda portadora en función de un bit de dato (0, 1). Un bit 0 corresponde a la fase 0; en cuanto al bit 1, corresponde a la fase g . Por tanto, este ángulo está asociado con un dato al ser transmitido y con una técnica de codificación usada para representar un bit. Es decir, cada cambio de fase es como si la porción de onda que sigue a dicho cambio, se adelantara (o atrasara) con relación a lo que debiera ser una forma senoidal continua, pura. Esta forma de cambiar la señal portadora para representar combinaciones binarias, se denomina modulación en fase PSK.

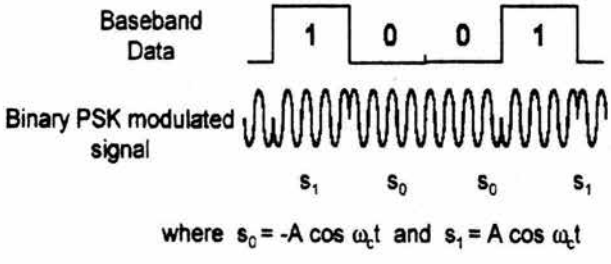


Figura 3.17. PSK (Phase Shift – Keying – Codificación por Cambio de Face).

Modulación DPSK

Variación de la modulación PSK, que tiene como característica un procedimiento de la fase de acuerdo con un dígito a ser transmitido.

Modulación QAM

Es caracterizada por la superposición de 2 portadoras en cuadratura moduladas en amplitud. Con eso al colocar 4 bits dentro de un tronco de señal y operar con tasas de 2400 bauds, se alcanza tasas de 9600 bps.

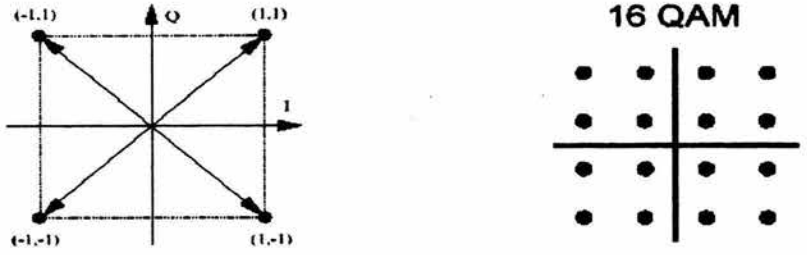


Figura 3.18. Modulación QAM a 4 bits/ bouds.

3.4 TRANSMISIÓN DE DATOS

Desde que comenzaron a popularizarse las computadoras, allá por fines de los años 60s y principios de los 70s, surgió la necesidad de comunicarlas a fin de poder compartir datos, o de poder conectar controladores de terminales tontas. En esos días lo más común era que dichas computadoras o controladores estuvieran alejados entre sí. Una de las soluciones más baratas y eficientes era la utilización de la red telefónica, ya que tenía un costo razonable y su grado de cobertura era muy amplia.

3.4.1 Características de la Transmisión de Datos

Sincronización

Para realizar la sincronización se transmite una señal que se activa y desactiva, o que varía en función de unas convenciones especificadas. Como la base de tiempos se transmite mediante los cambios de dicha línea, se puede informar así al dispositivo receptor de que debe examinar los datos en un tiempo determinado. Dicha señal se puede utilizar también para volver a sincronizar el reloj del dispositivo receptor, de forma que se alineé perfectamente con cada bit de datos que reciba.

Es decir, las señales de reloj sirven para dos funciones: Sincronizar inicialmente al receptor antes de la llegada de los datos, y mantenerlo sincronizado con los bits de datos que llegan.

Velocidad de señalización

Velocidad de señalización, es una referencia a la velocidad expresada en bauds o baudios (razón o velocidad de señalización) con el que un módem puede transmitir datos. Indica el número de bps transmitidos, lo que la velocidad de transferencia mide realmente es el número de sucesos (eventos), o cambios de señal, que se producen en 1 segundo.

Como un suceso puede codificar más de 1 bit en las comunicaciones digitales de alta velocidad, la velocidad de transferencia y los bits por segundo no son siempre sinónimos, por lo que bits por segundo es el término más exacto que debe aplicarse a los aparatos de módem. Por ejemplo, el denominado módem de 9.600 baudios que codifica 4 bits por suceso, en la práctica funciona a 2.400 baudios, aunque transmite 9.600 bps (2.400 sucesos multiplicados por 4 bits por suceso). Por consiguiente, debería llamárselo módem de 9.600 bps.

Velocidad de señalización real (Throughput).

Define la cantidad de datos que pueden enviarse a través de un módem en un cierto período de tiempo. Un módem de 9600 baudios puede tener un throughput distinto de 9600 bps debido al ruido de la línea (que puede ralentizar) o a la compresión de datos (que puede incrementar la velocidad hasta 4 veces el valor de los baudios). Para mejorar la tasa efectiva de transmisión o throughput se utilizan técnica de compresión de datos y corrección de errores.

Compresión de datos

Describe el proceso de tomar un bloque de datos y reducir su tamaño. Se emplea para eliminar información redundante y para empaquetar caracteres empleados frecuentemente y representarlos con sólo uno o dos bits.

La compresión de datos observa bloques repetitivos de datos y los envía al módem remoto en forma de palabras codificadas. Cuando el otro módem recibe el paquete lo decodifica y forma el bloque de datos original. Son dos las técnicas usadas para hacer más eficaces los movimientos de datos entre locales remotos: Compresión lógica y Compresión física.

a). Compresión lógica

Se debe procurar reducir al máximo un volumen de datos almacenados. Esta reducción, en verdad resulta de la eliminación de los campos redundantes y de un uso de la menor cantidad de indicadores lógicos posibles para los campos restantes. Un dato puede ser comprimido usando representación numérica y representación binaria (esta es la más recomendada).

b). Compresión física

Son varias las técnicas utilizadas, como la sustitución de caracteres repetidos por un comando capaz de expandirlos en la otra extremidad, o hasta la aplicación de un algoritmo que resulte menos los datos a transmitir.

Control de errores

La ineludible presencia de ruido en las líneas de transmisión provoca errores en el intercambio de información que se debe detectar introduciendo información de control. Así mismo puede incluirse información redundante que permita además corregir los errores cuando se presenten. El problema de ruido puede causar perdidas importantes de información en módem a velocidades altas, existen para ello diversas técnicas para el control de errores. Cuando se detecta un ruido en un módem con control de errores, todo lo que se aprecia es una breve inactividad o pausa en el enlace de la comunicación, mientras que si el módem no tiene control de errores lo que ocurre ante un ruido es la posible aparición en la pantalla de caracteres "basura" o, si sé esta transfiriendo un archivo en ese momento, esa parte del archivo tuviese que retransmitirse otra vez.

En algunos casos el método de control de errores está ligado a la técnica de modulación:

a). Módem Hayes V-Serie emplea modulación Hayes Express y un esquema de control errores llamado Link Access Procedure-módem (LAP-M).

b). Módem US Robotics emplea protocolos propios y emplea una modulación y control de errores también propios de US Robotics.

Existen otras tres técnicas para control de errores bastante importantes:

- Microcosm Network Protocol (MNP-1, 2, 3, 4).
- Norma V.42 (procedente del CCITT e incluye el protocolo MNP-4)
- Norma MNP 10. Corrección de errores recomendada para comunicaciones a través de enlaces móviles.

MNP

Reconocido como patrón mundial de protocolos de alto desempeño para corrección de errores y compresión en las transmisiones de datos. Este protocolo garantiza transferencia de datos libres de errores en conexiones asíncronas. Este protocolo asigna la transmisión ante ruidos y distorsiones en las líneas telefónicas. Posee diez clases pero las más conocidas son: 4, 5 y 10.

MNP clase 4

Permite tráfico con gran eficiencia gracias a las técnicas de Adaptive Packet Assembly Data Phase Optimization (Adaptación de Paquetes de Ensamblado de Datos y Optimización de la Fase). Con eso el tamaño de los paquetes es automáticamente ajustado de acuerdo con las condiciones de la línea, aumentando el desempeño y disponibilidad de enlace.

MNP clase 5

Además de aumentar la tasa de transmisión, gracias al MNP Data Compresión, la posibilidad de retransmisión también es mucho menor, ya que la cantidad de bytes en la línea también es disminuida.

MNP clase 10

Además de permitir un ajuste automático para líneas de baja calidad, un protocolo MNP 10 permite transmisiones totalmente libres de errores. El secreto de este desempeño es un componente ACE (Adverce Channel Enhancement – Mejoramiento de Canal Adverso), que a parte de asegurar la comunicación en situaciones críticas de enlace, también hace variar continuamente la tasa de transmisión a medida que la calidad de la línea sufre alguna variación, garantizando la optimización de un flujo de transmisión.

3.4.2 Medios de Transmisión de Datos.

3.4.2.1 Medios Guiados

Los medios guiados son aquellos que proporcionan un conductor de un dispositivo al otro e incluyen cables de pares trenzados, cables coaxiales y cables de fibra óptica. Una señal viajando por cualquiera de estos medios es dirigida y contenida por los límites físicos del medio.

El par trenzado y el cable coaxial usan conductores metálicos (de cobre) que aceptan y transportan señales de corriente eléctrica. La fibra óptica es un cable de cristal o plástico que acepta y transporta señales en forma de luz.

Cable de par trenzado.

El cable de par trenzado se presenta en dos formas: sin blindaje y blindado.

a) Cable de par trenzado sin blindaje (UTP)

El cable de par trenzado sin blindaje (UTP Unshield Twisted Pair) es el tipo más frecuente de medio de comunicación que se usa actualmente. Aunque es el más familiar por su uso en los sistemas telefónicos, su rango de frecuencia es adecuado para transmitir tanto datos como voz. Un par trenzado está formado por dos conductores (habitualmente de cobre), cada uno con su aislamiento de plástico de color. El aislamiento de plástico tiene un color asignado a cada banda para su identificación. Los colores se usan tanto para identificar los hilos específicos de un cable como para indicar qué cables pertenecen a un par y cómo se relacionan con los otros pares de un manojo de cables.

En el pasado se usaron dos cables planos paralelos para la comunicación. Sin embargo, la interferencia electromagnética de dispositivos tales como motores podía originar ruidos en los cables. Sí los dos cables son paralelos, el cable más cercano a la fuente de ruido tiene más interferencia y termina con un nivel de tensión más alto que el cable que está más lejos, lo que da como resultado cargas distintas y una señal dañada. Sin embargo, sí los dos cables están trenzados entre sí en intervalos regulares (entre 2 y 12 torsiones por pie), cada cable está cerca de la fuente del ruido durante la mitad del tiempo y lejos durante la otra mitad. Por tanto, con el trenzado, el efecto acumulativo de la interferencia es igual en ambos cables. Cada sección de un cable tiene una -carga- de 4 cuando esta en la parte alta del trenzado y de 3 cuando está en la parte baja. El efecto total del ruido en el receptor es 0 (14 –14. El trenzado no siempre elimina el impacto del ruido, pero lo reduce significativamente. Las ventajas del UTP son su costo y su facilidad de uso. El UTP es barato, flexible y fácil de instalar. En muchas tecnologías de LAN, incluyen Ethernet y Anillo con paso de testigo, se usa UTP de gama alta.

La Asociación de Industrias Electrónicas (EIA) ha desarrollado estándares para graduar los cables UTP según su calidad. Las categorías se determinan según su calidad del cable, que varía desde 1, para la más baja, hasta 5, para la más alta. Cada categoría de la EIA es adecuada para ciertos tipos de usos y no para otros:

Categoría 1. El cable básico del par trenzado que se usa en los sistemas telefónicos. Este nivel de calidad es bueno para voz pero inadecuado para cualquier otra cosa que no sean comunicaciones de datos de baja velocidad.

Categoría 2. El siguiente grado más alto, adecuado para voz y transmisión de datos hasta 4 Mbps.

Categoría 3. Debe tener obligatoriamente al menos nueve trenzas por metro y se puede usar para transmisión de datos de hasta 10 Mbps. Actualmente es el cable estándar en la mayoría de los sistemas de telecomunicación de telefonía.

Categoría 4. También debe tener al menos nueve trenzas por metro, así como otras condiciones para hacer que la transmisión se pueda efectuar a 16 Mbps.

Categoría 5. Usada para la transmisión de datos hasta los 100Mbps.

Conectores UTP. Los cables UTP se conectan habitualmente a los dispositivos de la red a través de un tipo de conector y un tipo de enchufe como el que se usa en las clavijas telefónicas. Los conectores pueden ser machos (el enchufe) o hembras (los receptáculos). Los conectores machos entran en los conectores hembras y tienen una pestaña móvil (denominada llave) que los bloquea cuando quedan ubicados en su sitio. Cada hilo de un cable está unido a estos enchufes son los RJ45, que tienen ocho conductores, uno para cada hilo de cuatro pares trenzados.

Cable de par trenzado blindado (STP)

El cable de par de trenzado blindado STP (STP; Shielded Twisted Pair) tiene una funda de metal o un recubrimiento de malla entrelazada que rodea cada par de conductores aislados. La carcasa de metal evita que penetre ruido electromagnético. También elimina un fenómeno denominado interferencia, que es un efecto indeseado de un circuito (o canal) sobre otro circuito (o canal). Se produce cuando una línea (que actúa como antena receptora) capta alguna de las señales que viajan por otra línea (que actúa como antena emisora). Este efecto se experimenta durante las conversaciones telefónicas cuando se oyen conversaciones de fondo. Blindando cada par de cable trenzado se pueden eliminar la mayor parte de las interferencias. El STP tiene las mismas consideraciones de calidad y usa los mismos conectores que el UTP, pero es necesario conectar el blindaje a tierra. Los materiales y los requisitos de fabricación de STP son más caros que los del UTP, pero dan como resultado cables menos susceptibles al ruido.

Cable coaxial.

El cable coaxial (o coax) transporta señales con rangos de frecuencias más altos que los cables de pares trenzados, en parte debido a que ambos medios de están construidos de forma bastante distinta. En lugar de tener dos hilos , el cable coaxial tiene un núcleo conductor central formado por un hilo sólido o enfilado (habitualmente cobre) recubierto por un aislante de material dieléctrico, que está, a su vez, recubierto por una hoja exterior de metal conductor, malla o una combinación de ambas (también habitualmente de cobre). La cubierta metálica exterior sirve como blindaje contra el ruido y como un segundo conductor, lo que completa el circuito. Este conductor exterior está también recubierto por un escudo aislante y todo el cable está protegido por una cubierta de plástico.

Los distintos diseños del cable coaxial se pueden categorizar según sus aplicaciones de radio del gobierno (RG). Cada número RG denota un conjunto único de especificaciones física, incluyendo el grosor del cable del conductor interno, el grosor y el tipo del aislante interior, la construcción del blindaje y el tamaño y el tipo de la cubierta exterior.

Cada cable definido por las clasificaciones RG está adaptado para una función especializada. Los más frecuentes son:

a). RG-8. Usado en Ethernet de cable grueso.

b). RG-9. Usado en Ethernet de cable grueso.

c). RG-11. Usado en Ethernet de cable grueso.

d). RG-58. Usado en Ethernet de cable fino.

e). RG-59. Usado para TV.

Conectores de los cables coaxiales.

A lo largo de los años, se han diseñado un cierto número de conectores para su uso en el cable coaxial, habitualmente por fabricantes que buscaban soluciones específicas a requisitos de productos específicos. Unos pocos de los conectores más ampliamente usados se han convertido en estándares. El más frecuente de todos ellos se denomina conector en barril por su forma. De los conectores de barril, el más popular es el conector de red a bayoneta (BNC, Bayonet Network Connector), que se aprieta hacia dentro y se bloquea en su lugar dando media vuelta.

Otros tipos de conectores de barril se atornillan juntos, lo que necesita más esfuerzo de instalación, o simplemente se aprietan sin bloqueo, lo que es menos seguro. Generalmente, un cable termina en un conector macho que se enchufa o se atornilla en su conector hembra correspondiente asociado al dispositivo. Todos los conectores coaxiales tienen una única patilla que sale del centro del conector macho y entra dentro de una funda de hierro del conector hembra. Los conectores coaxiales son muy familiares debido a los cables de TV y a los enchufes de VCR, que se emplean tanto los de presión como los deslizantes.

Otros tipos de conectores que se usan frecuentemente son los conectores T y los terminadores. Un conector T (que se usa en la Ethernet de cable fino) permite derivar un cable secundario u otros cables de la línea principal. Un cable que sale de una computadora, por ejemplo, se puede ramificar para conectarse a varias terminales

Fibra óptica.

Hasta este momento, se han visto cables conductores (de metal) que transmiten señales en forma de corriente. La fibra óptica, por otro lado, está hecha de plástico o de cristal y transmite las señales en forma de luz. Para comprender cómo funciona la fibra óptica es necesario explorar primero varios aspectos de la naturaleza de la luz.

La luz es una forma de energía electromagnética que alcanza su máxima velocidad en el vacío: 300.000 Kilómetros/segundo (aproximadamente, 186.000 millas/segundo). La velocidad de la luz depende del medio por el que se propaga (cuanto más alta es la densidad, más baja es la velocidad).

La luz es una forma de energía electromagnética que viaja a 300.000 kilómetros/segundo, aproximadamente 186.000millas/segundo, en el vacío. La velocidad decrece a medida que el medio por el que se propaga la luz se hace más denso.

a) Refracción.

La luz se propaga en línea recta mientras se mueve a través de una única sustancia uniforme. Sí un rayo de luz que se propaga a través de una sustancia entra de repente en otra (más o menos densa), su velocidad cambia abruptamente, causando que el rayo cambie de dirección. Este cambio se denomina refracción. Una paja que sobresale de un vaso de agua parece estar torcida, o incluso rota, debido a que la luz a través de la que la vemos cambia de dirección a medida que se mueve del aire al agua. La dirección en la que se refracta un rayo de luz depende del cambio de densidad que encuentre. Un rayo de luz que se mueva de una sustancia menos densa a un medio más denso se curva hacia el eje vertical. Los dos ángulos formados por el rayo de luz en relación al eje vertical se denominan I, para incidente y R, para refractado.

b) Reflexión.

Cuando el ángulo de incidencia se hace mayor que el ángulo crítico, se produce un fenómeno denominado reflexión (o más exactamente, reflexión completa, porque algunos aspectos de la reflexión siempre coexisten con la refracción). En este caso, ya no pasa nada de la luz al medio menos denso, porque el ángulo de incidencia es siempre igual al ángulo de reflexión.

La fibra óptica usa la reflexión para transmitir la luz a través de un canal. Un núcleo de cristal o plástico se rodea con una cobertura de cristal o plástico menos denso. La diferencia de densidad de ambos materiales debe ser tal que el rayo de luz que se mueve a través del núcleo sea reflejado por la cubierta en lugar de ser refractado por ella. La información se codifica dentro de un rayo de luz como series de destellos encendido-apagado que representan los bits uno y cero.

c). Modos de propagación

La tecnología actual proporciona dos modos de propagación de la luz a lo largo de canales ópticos, cada uno del os cuales necesita fibras con características distintas: multimodo y monomodo. A su vez, el multimodo se puede implementar de dos maneras: índice escalonado o de índice de gradiente gradual.

- El Multimodo se denomina así porque hay múltiples rayos de luz de una fuente luminosa que se mueven a través de del núcleo por caminos distintos. Cómo se mueven estos rayos dentro del cable depende de la estructura del núcleo.En la fibra multimodo de índice escalonado, la densidad del núcleo permanece constante desde el centro hasta los bordes. Un rayo de luz se mueve a través de esta densidad constante en línea recta hasta que alcanza la interfaz del núcleo y la cubierta. En la interfaz, hay un cambio abrupto a una densidad más baja que altera el ángulo de movimiento del rayo. El término de índice escalonado se refiere a la rapidez de este cambio.

- El monomodo usa fibra de índice escalonado y una fuente de luz muy enfocada que limita los rayos a un rango muy pequeño de ángulos, todos cerca de la horizontal. La fibra monomodo se fabrica con un diámetro mucho más pequeño que las fibras multimodo y con una densidad (índice de refracción) sustancialmente menor. El decrecimiento de densidad da como resultado un ángulo crítico que está muy cerca de los 90 grados para hacer que la propagación de los rayos sea casi horizontal. En este caso, la propagación de los distintos rayos es casi idéntica y los retrasos son despreciables. Todos los rayos llegan al destino – juntos- y se pueden recombinar sin distorsionar la señal.

Conectores para fibra óptica

Los conectores para el cable de fibra óptica deben ser tan precisos como el cable en sí mismo. Con medios metálicos, las conexiones no necesitan ser tan exactas siempre que ambos conductores estén en contacto físico. Por otro lado, con la fibra óptica cualquier deslineamiento o bien con otro segmento del núcleo o bien con un fotodiodo da como resultado que la señal se refleje hacia el emisor y cualquier diferencia en el tamaño de los dos canales conectados da como resultado un cambio en el ángulo de la señal. Además, la conexión debe completarse aunque las fibras conectadas no estén completamente unidas. Un intervalo entre ambos núcleos da como resultado una señal disipada; una conexión fuertemente presionada puede comprimir ambos núcleos y alterar el ángulo de reflexión.

Teniendo en cuenta estas restricciones, los fabricantes han desarrollado varios conectores que son precisos y fáciles de usar. Todos los conectores populares tienen forma de barril y conectores en versiones macho y hembra. El cable se equipa con un conector macho que se bloquea o conecta con un conector hembra asociado al dispositivo a conectar.

Ventajas de la fibra óptica.

La principal ventaja que ofrece el cable de fibra óptica sobre los pares trenzados y el cable coaxial son: inmunidad al ruido, menor atenuación de la señal y ancho de banda mayor.

a). Inmunidad al ruido. Debido a que las transmisiones por fibra óptica usan luz en lugar de electricidad, el ruido no es importante. La luz externa, la única interferencia posible, es bloqueada por el recubrimiento opaco exterior del canal.

b). Menor atenuación de la señal. La distancia de transmisión de la fibra óptica es significativamente mayor que la que se consigue en otros medios guiados. Una señal puede transmitirse a lo largo de kilómetros sin necesidad de regeneración.

c). Ancho de banda mayor. El cable de fibra óptica puede proporcionar anchos de banda (y por tanto tasa de datos) sustancialmente mayores que cualquier cable de par trenzado o coaxial. Actualmente, la tasa de datos y el uso del ancho de banda en cables de fibra óptica no están limitados por el medio, sino por la tecnología disponible de generación y de recepción de la señal.

Desventajas de la fibra óptica.

Las principales desventajas de la fibra óptica son el costo, la instalación, el mantenimiento y la fragilidad.

a). Costo. El cable de fibra óptica es caro. Debido a que cualquier impureza o imperfección del núcleo puede interrumpir la señal, la fabricación debe ser laboriosamente precisa. Igualmente, conseguir una fuente de luz láser puede costar miles de dólares, comparado a los cientos de dólares necesarios para los generadores de señales eléctricas.

b). Instalación / mantenimiento. Cualquier grieta o rozadura del núcleo de un cable de fibra óptica difumina la luz y altera la señal. Todas las marcas deben ser pulidas y fundidas con precesión. Todas las conexiones deben estar perfectamente alineadas y ser coincidentes con el tamaño del núcleo y deben proporcionar uniones completamente acopladas pero sin excesivas presiones. Las conexiones de los medios metálicos, por otro lado, se pueden hacer con herramientas de cortado y de presión relativamente poco sofisticadas.

c). Fragilidad. La fibra de cristal se rompe más fácilmente que le cable, lo que la convierte en menos útil para aplicaciones en las que es necesario transportar el hardware.

A medida que las técnicas de fabricación han mejorado y los costos se han reducido, las altas tasas de datos y la inmunidad al ruido han hecho de la fibra óptica un medio crecientemente popular.

3.4.2.2 Medios no guiados.

Los medios no guiados, o comunicaciones sin cable, transportan ondas electromagnéticas sin usar un conductor físico. En su lugar, las señales se radian a través del aire(o el agua, en algunos pocos casos, el agua) y, por tanto, están disponibles para cualquiera que tenga un dispositivo capaz de aceptarlas.

Radiofrecuencias

La sección del espectro electromagnético definido como comunicación de radio se divide en ocho rangos, denominados bandas, cada una de ellas reguladas por las autoridades gubernamentales. Estas bandas se clasifican desde frecuencia muy baja (VLF, Very Low Frecuency) a frecuencia extremadamente alta (EHF, Extremely High Frecuency).

Tipos de Propagación de las ondas de radio

La transmisión de ondas de radio utiliza cinco tipos de propagación distintos: superficie, troposférica, ionosférica, línea de visión y espacio.

La tecnología de radio considera que la tierra está rodeada por dos capas de atmósfera: la troposfera y la ionosfera. La troposfera es la porción de la atmósfera que se extiende hasta aproximadamente 45 Km. desde al superficie de la tierra (en terminología de radio, la troposfera incluye una capa de máxima altitud denominada estratosfera) y contiene aquello en lo que nosotros generalmente pensamos como el aire; Las nubes, el viento, las variaciones de temperatura y el clima en general ocurren en la troposfera, al igual que los viajes de avión. La ionosfera es la capa de atmósfera por encima de la troposfera pero por debajo del espacio. Esta más allá de lo que nosotros denominamos atmósfera y contiene partículas libres cargadas eléctricamente (de aquí el nombre).

a) Propagación en superficie.

En la propagación en superficie, las ondas de radio viajan a través de la porción más baja de la atmósfera, abrazando a la tierra. A las frecuencias más bajas, las señales emanan en todas direcciones desde al antena de transmisión y sigue la curvatura del planeta. La distancia depende de la cantidad de potencia en la señal: cuanto mayor es la potencia, mayor es la distancia. La propagación en superficie también puede tener lugar en el agua del mar.

b). Propagación troposférica.

La propagación troposférica puede actuar de dos formas. O bien se puede dirigir la señal en línea recta de antena (visión directa) o se puede radiar con un cierto ángulo hasta los niveles superiores de la troposfera donde se refleja hacia la superficie de la tierra. El primer método necesita que la situación del receptor y el transmisor esté dentro de distancias de visión, limitadas por la curvatura de la tierra en relación a la altura de las antenas. El segundo método permite cubrir distancias mayores.

c) Propagación ionosférica.

En la propagación ionosférica, las ondas de radio de más alta frecuencia se radian hacia la ionosfera donde se reflejan de nuevo hacia la tierra. La densidad entre la troposfera y la ionosfera hace que cada onda de radio se aceleres y cambie de dirección, curvándose de nuevo hacia la tierra. Este tipo de transmisión permite cubrir grandes distancias con menor potencia de salida.

d) Propagación por visión directa.

En la propagación por visión directa, se transmiten señales de muy alta frecuencia directamente de antena siguiendo una línea recta. Las antenas deben ser direccionales, estando enfrentadas entre sí, y o bien están suficientemente altas o suficientemente juntas para no verse afectadas por la curvatura de la tierra. La propagación por visión directa es compleja porque las transmisiones de radio no se pueden enfocar completamente. Las ondas emanan hacia arriba y hacia abajo así como hacia adelante y pueden reflejar sobre la superficie de la tierra o partes de la atmósfera. Las ondas reflejadas que llegan a la antena receptora más tarde que la porción directa de la transmisión puede corromper la señal recibida.

e). Propagación por el espacio.

La propagación por el espacio utiliza como retransmisor satélites en lugar de la refracción atmosférica. Una señal radiada es recibida por un satélite situado en órbita, que la reenvía de vuelta a la tierra para el receptor adecuado. La transmisión vía satélite es básicamente una transmisión de visión directa con un intermediario (el satélite). La distancia al satélite de la tierra es equivalente a una antena de súper alta ganancia e incrementa enormemente la distancia que puede ser cubierta por una señal.

f). Propagación de señales específicas.

El tipo de propagación que se usa en la radio–tranmisión depende de la frecuencia (velocidad) de la señal. Cada frecuencia es adecuada para una capa específica de la atmósfera y es más eficiente si se transmite y se envía con tecnologías adaptadas a la capa.

Propagación de las diferentes ondas de radio

a). VLF

Las ondas de frecuencia muy baja (VLF, Very Low Frecuency) se propagan como ondas de superficie, habitualmente a través del aire, pero algunas veces a través del agua del mar. Las ondas VLF no sufren mucha atenuación debido a la transmisión, pero son sensibles a los altos niveles de ruido atmosférico (calor y electricidad) activo en bajas altitudes. Las ondas VLF se usan principalmente para radio-navegación de largo alcance y para comunicación submarina.

b). LF

De forma similar al VLF, las ondas de baja frecuencia (LF, Low Frecuency) se propagan también como ondas de superficie. Las ondas LF se usan para radio-navegación de largo alcance y apra la radio balizas o localizadores de navegación. La atenuación es mayor durante el día, cuando se incrementa la absorción de las ondas por los obstáculos naturales.

c). MF

Las señales de frecuencia alta (MF, Middle Frecuency) se propagan en la troposfera. Estas frecuencias son absorbidas por la ionosfera. La absorción se incrementa durante el día, pero la mayoría de las transmisiones MF se efectúan con antenas de visión directa para incrementar el control y evitar también los problemas de absorción. Los usos de las transmisiones MF incluyen radio AM, radio marítima, buscadores audiodireccionales (RDF) y frecuencias de emergencia.

d). HF

Las señales de frecuencia alta (HF, High Frecuency) usan propagación ionosférica. Estas señales se desplazan dentro de la ionosfera, donde la diferencia de densidad las refleja de nuevo hacia la tierra. Los usos de señales HF incluyen los radioaficionados (am. radio), la radio de bandas de ciudadanos (CB), las emisiones internacionales, comunicaciones militares, comunicación de larga distancia para aviones y barcos, teléfonos, telégrafos y faxes.

e) VHF

La mayoría de las ondas de frecuencia muy alta (VHF, Very High Frecuency) usan propagación de visión directa. Los usos del VHF incluyen la televisión VHF, la radio FM, la radio AM de los aviones y la ayuda de navegación de los aviones.

f). UHF

Las ondas de frecuencia ultra alta (UHF, Ultra High Frecuency) siempre se usan en propagación de visión directa. Los usos para el UHF incluyen la televisión UHF, los teléfonos móviles, la radio celular, los buscadores y los enlaces de microondas. La comunicación con microondas comienza en la frecuencia 1 Ghz de la banda de UHF y continúa hasta las bandas SHF y EHF.

g). SHF

Las ondas de frecuencia súper alta (SHF, Súper High Frecuency) se transmiten usando principalmente propagación por visión directa y algo de propagación espacial. Los usos del SHF incluyen las microondas terrestres y satélite y la comunicación radar.

h). EHF

Las ondas de frecuencia extremadamente alta (EHF, Extremely High Frecuency) usan la propagación espacial. Los usos para el EHF son predominantemente científicos e incluyen radar, satélite y comunicaciones experimentales.

i) Microondas terrestres

Las microondas terrestres no siguen la curvatura de la tierra y por tanto necesitan equipo de transmisión y recepción por visión directa. La distancia que se puede cubrir con una señal por visión directa. La distancia que se puede cubrir con una señal por visión directa depende principalmente de la altura de la antena: cuantas más altas sean alas antenas, más larga es la distancia que se puede ver. La altura permite que la señal viaje más lejos sin ser interferida por la curvatura del planeta y eleva la señal por encima de muchos obstáculos de la superficie, como colinas baja y edificios altos que de otra forma bloquearían la transmisión. Habitualmente, las antenas se montan sobre torres que a su vez están construidas sobre colina s o montañas. Las señales de microondas se propagan en una dirección concreta, lo que significa que son necesarias dos frecuencias para una comunicación en dos sentidos, como por ejemplo una conversación telefónica. Una frecuencia se reserva para la transmisión por microondas en una dirección y la otra para la transmisión en la otra. Cada frecuencia necesita su propio transmisor y receptor. Actualmente, ambas partes del equipo se combinan habitualmente en un equipo denominado transceptor, lo que permite usar una única antena para dar servicio a ambas frecuencias y funciones.

Para incrementar la distancia útil de las microondas terrestres, se puede instalar un sistema de repetidores con cada antena. La señal recibida por una antena se puede convertir de nuevo a una forma transmisible y entregarla a la antena siguiente. La distancia mínima entre los repetidores varía con la frecuencia de la señal y el entorno en el cual se encuentran las antenas. Un repetidor puede radiar la señal regenerada a al frecuencia original o con una nueva frecuencia, dependiendo del sistema.

Las microondas terrestres con repetidores constituyen la base de la mayoría de los sistemas de telefonía contemporánea alrededor del mundo.

Para las comunicaciones con microondas terrestres se usan dos tipos de antenas:

- Parabólicas.

Una antena parabólica se basa en la geometría de una parábola: cada línea paralela a la línea de simetría (línea de vista) refleja la curva en ángulos tales que inciden en un punto común denominado foco. El plato parabólico funciona como un embudo, capturando un amplio rango de ondas y dirigiéndose a un punto común. De esta forma, se recupera más señal de lo que sería posible con un receptor de punto único. Las transmisiones de salida se radian a través de un cornete apuntando al disco. Las microondas golpean el disco y son deflexionadas hacia fuera en sentido contrario al camino de recepción.

- b) de Cornete

Una antena de cornete se parece a una cuchara gigante. Las transmisiones de salida son radiadas hacia arriba de un mástil (que se parece al mango) y deflexionadas hacia fuera en transmisiones recibidas son recolectadas por la forma del a cuchara del cornete, de forma similar a la antena parabólica, y son deflexionadas mástil abajo.

j) Comunicación vía satélite

Las transmisiones vía satélite se parecen mucho más a las transmisiones con microondas por visión directa en la que las estaciones son satélites que están orbitando la tierra. El principio es el mismo que con las microondas terrestres, excepto que hay un satélite actuando como una antena súper alta y como repetidor. Aunque las señales que se transmiten vía satélite siguen teniendo que viajar en línea recta, las limitaciones impuestas sobre la distancia por la curvatura de la tierra son muy reducidas. De esta forma, los satélites retransmisores permiten que las señales de microondas se puedan transmitir a través de continentes y océanos con un único salto. Las microondas vía satélite pueden proporcionar capacidad de transmisión y desde cualquier localización en la tierra, sin importar lo remota que esta sea. Esta ventaja hace que las comunicaciones de alta calidad estén disponibles en lugares no desarrollados del mundo sin necesidad de hacer grandes inversiones en infraestructura de tierra. Por supuesto, los satélites en si mismos son extremadamente caros, pero alquilar tiempo o frecuencias de uno de ellos puede ser relativamente barato.

La propagación por línea de vista necesita que las antenas emisoras y receptoras estén fijas/estáticas con respecto a la localización de las demás en todo momento (una antena debe poder ver a la otra). Por esta razón, un satélite que se mueve más deprisa o más despacio que la rotación de la tierra es útil únicamente para periodos de tiempo cortos (de la misma forma que un reloj parado solamente es exacto dos veces al día). Para asegurar una comunicación constante, el satélite debe moverse a la misma velocidad que la tierra de forma que parezca que está fijo en un cierto punto. Estos satélites se llaman geosincrónicos.

Debido a que la velocidad orbital depende de la distancia desde el planeta, solamente hay una órbita que puede ser geosincrónica. Esta órbita se produce en el plano ecuatorial y está aproximadamente a 36.000 kilómetros de la superficie de la tierra. Pero un único satélite geosincrónico no puede cubrir toda la tierra. Un satélite en órbita tiene contacto por línea de vista con un gran número de estaciones, pero la curvatura de la tierra sigue haciendo que gran parte del planeta todavía no se pueda ver. Por ello, es necesario tener un mínimo de tres satélites equidistantes entre sí en órbita geosincrónica para proporcionar una transmisión global completa. Las frecuencias reservadas para la comunicación por microondas vía satélite están en el rango de los gigahertzios (GHz). Cada satélite envía y recibe dos bandas distintas. La transmisión desde la tierra al satélite se denomina enlace ascendente. La transmisión desde el satélite a la tierra se denomina enlace descendente.

3.5 TRONCALES DE VOZ

Hoy en día, el sistema telefónico se organiza como una jerarquía altamente redundante, de múltiples niveles. Cada teléfono tiene dos alambres de cobre que salen de él y que van directamente a la oficina final más cercana de la compañía de teléfonos (también llamada oficina central local). Por lo general, la distancia es de 1 a 10 Km., y en las ciudades es menor que en las áreas rurales. La concatenación del código de área y los tres primeros dígitos del número telefónico especifican de manera única una oficina final. Las conexiones de dos hilos entre el teléfono de cada suscriptor y la oficina final se conocen en el negocio como lazo local. Si un suscriptor conectado a una oficina final determinada llama a otro suscriptor conectado la misma oficina final, el mecanismo de conmutación dentro de la oficina establece una conexión eléctrica directa entre los dos lazos locales. Esta conexión permanece intacta mientras dura la llamada. Si el teléfono al que se llama está conectado a otra oficina final, se tiene que usar un procedimiento diferente. Cada oficina final tiene varias líneas salientes a uno o más centros de conmutación cercanos, llamados oficinas de cargo (o, si están dentro de la misma área local, oficinas tándem). Estas líneas se llaman troncales de conexión con cargo. Si sucede que tanto la oficina final de quien llama como la de quien es llamado tienen una troncal de conexión a la misma oficina de cargo (algo muy probable si no están muy alejadas), la conexión se puede establecer dentro de la oficina. de cargo. En la siguiente figura se muestra una red telefónica que consiste únicamente en teléfonos (los puntos pequeños), oficinas finales (los puntos grandes) y oficinas de cargo (los marcos). Si el que llama y el que es llamado no tienen una oficina de cargo en común, la trayectoria se deberá establecer en un nivel más alto de la jerarquía. Hay oficinas primarias, seccionales y regionales que forman una red que conecta a las oficinas de cargo. Las centrales de cargo, primarias, seccionales y regionales se comunican entre sí mediante troncales intercargo de gran ancho de banda (llamadas también troncales Ínter oficinas). La cantidad de tipos diferentes de centros de conmutación y su topología varían de país a país dependiendo de su densidad telefónica. La siguiente figura muestra como se podría enrutar una conexión de media distancia.

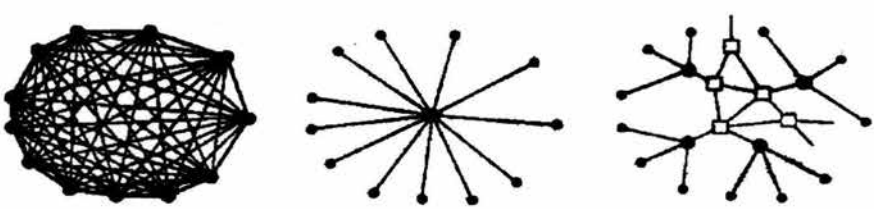


Fig. 3.19

Red completamente Conmutadora centralizada Jerarquía de dos niveles Interconectada.

3.5.1 Señalización entre las troncales de voz

Entre las oficinas de conmutación o troncales de voz se usan ampliamente cables coaxiales, microondas y, en especial, fibra óptica. En el pasado, la señalización en todo el sistema telefónico era analógica, con la señal de voz real transmitida como un voltaje eléctrico del origen al destino. Con el advenimiento de la electrónica digital y las computadoras, se ha hecho posible la señalización digital. En este sistema se permiten sólo dos voltajes, por ejemplo -5 volts y +5 volts.

Ventajas de la señalización Digital.

Este esquema tiene muchas ventajas sobre la señalización analógica:

a). La primera es que aunque la atenuación y la distorsión son más severas cuando se envían señales de dos niveles que cuando se usan módems, es fácil calcular qué tan lejos se puede propagar una onda y todavía ser reconocible. Se puede insertar un regenerador digital en ese punto de la línea para restablecer la señal a su valor original, ya que existen solamente dos posibilidades. Una señal digital puede pasar a través de una cantidad arbitraria de regeneradores sin pérdida de señal y viajar de este modo grandes distancias sin pérdida de información. En contraste las señales analógicas siempre sufren cierta pérdida de información cuando se amplifican, y esta pérdida es acumulativa. El resultado neto es que se puede lograr que la transmisión digital tenga una tasa de errores baja.

b). Una segunda ventaja de la transmisión digital es que se pueden intercalar voz, datos, música e imágenes (por ejemplo, televisión, fax y vídeo) para aprovechar de forma más eficiente los circuitos y el equipo.

c). Otra ventaja es que son posibles velocidades de transmisión de datos mucho más altas con las líneas existentes.

d). Una tercera ventaja es que la transmisión digital es mucho más económica que la analógica, puesto que no es necesario reproducir exactamente una forma de onda analógica después de atravesar tal vez cientos de amplificadores en una llamada transcontinental; basta poder distinguir correctamente un 0 de un 1.

e). Por último, el mantenimiento de un sistema digital es más fácil que el de uno analógico. Un bit transmitida se recibe bien o no, con lo que se simplifica el rastreo de problemas.

En consecuencia, todas las troncales de larga distancia dentro del sistema telefónico se están convirtiendo rápidamente a tecnología digital. El sistema antiguo utilizaba transmisión analógica por cables de cobre; el nuevo emplea transmisión digital por fibra óptica.

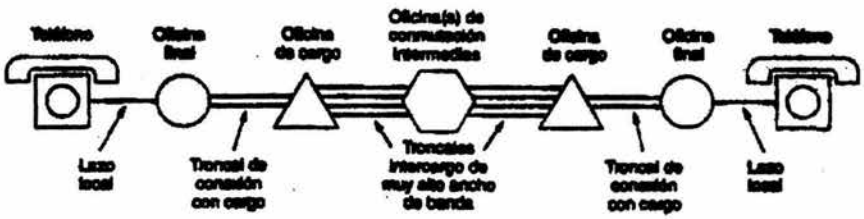


Figura 3.20 Ruta típica de un circuito para una llamada de media distancia

3.6 DETECCIÓN Y CORRECCIÓN DE ERRORES

Para cumplir el objetivo propuesto al principio del presente trabajo, se tiene que garantizar que la información enviada desde el emisor sea la misma que le llega al receptor, por lo cual se requiere de métodos que verifiquen la integridad de la información. A continuación explicaremos los métodos de detección y corrección de errores mas utilizados en la actualidad.

3.6.1 Tipos de errores

Siempre que una señal electromagnética se transmite de un punto a otro, es susceptible de sufrir interferencias impredecibles debidas al calor, el magnetismo, y diversas influencias de la electricidad. Si la señal transporta datos binarios codificados, tales interferencias pueden alterar el contenido de la información enviada. Cuando existe un error de bit, se cambia un 0 por un 1 o un 1 por un 0. En un error de ráfaga, se cambian múltiples bits.

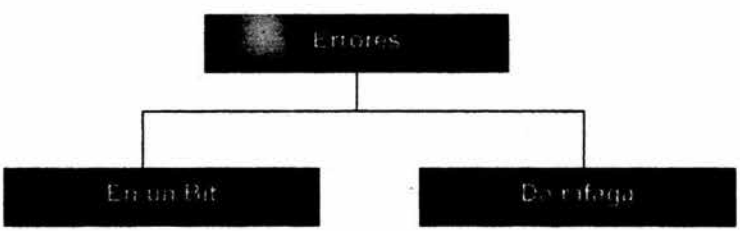


Figura 3.21. Tipos de Errores

Error de bit

El termino error de bit significa que únicamente un bit de una unidad de datos determinada (tal como un byte, unidad de datos o paquete) cambia de 1 a 0 o de 0 a 1.La figura 3.22 muestra el efecto de un error de bit de una unidad de datos. Para entender el impacto de este cambio, imagine que cada grupo de 8 bits es un carácter ASCII con un 0 añadido a la izquierda. En la figura, se ha enviado el carácter 00000010 (ASCII STX) que indica comienzo del texto, pero se ha recibido 00001010 (ASCII LF), que significa salto de línea.

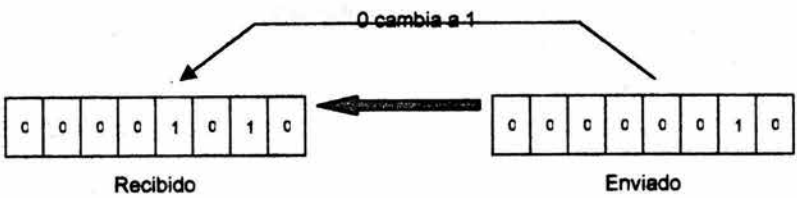


Figura 3.22 Error de bit

Los errores en un único bit son el tipo menos probable es una transmisión de datos en serie. Para ver porqué, imagine que un emisor envía datos a 1 Mbps. Esto significa que cada bit dura únicamente 1/1000000 segundos, o 1 µs. Para que ocurra un error de bit, el ruido debe tener una duración de solo 1 µs, lo que es muy raro; normalmente el ruido dura mucho mas que eso.

Sin embargo, puede ocurrir que un error de bit si se están enviando datos usando transmisión paralela. Por ejemplo, si se usan ocho cables para enviar los ocho bits de un byte al mismo tiempo y uno de los cables es ruidoso, se puede corromper un bit de cada byte.

Error de ráfaga

El termino error de ráfaga significa que dos o mas bits de la unidad de datos han cambiado de 1 a 0 o de 0 a 1.

La figura 3.23 muestra el efecto de un error de ráfaga sobre una unidad de datos. En este caso, se ha enviado 0100010001000011, pero se ha recibido 0101110101000011. Observe que un error de ráfaga no significa necesariamente que los errores se produzcan en bits consecutivos. La longitud de la ráfaga se mide desde el primero hasta el último bit correcto. Algunos bits intermedios pueden no ser corruptos.

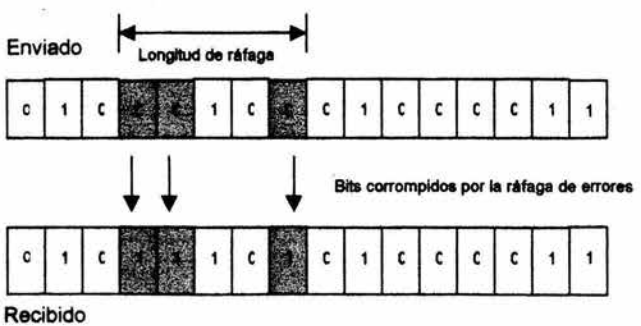


Figura 3.23 Error de ráfaga de longitud cinco

La presencia de errores de ráfaga es mas probable en las transmisiones serie. La duración del ruido es normalmente mayor que la duración de un bit, lo que significa que cuando el ruido afecta a los datos, afecta a un conjunto de bits. El número de bits afectados depende de la tasa de datos y de la duración del ruido. Por ejemplo, si se esta envinado información a 1 Kbps, un ruido de 1/100 segundos puede afectar a 10 bits, si se envían datos a 1 Mbps, el mismo ruido podría afectar a 10000 bits.

3.6.2. Detección de errores

Incluso si se conoce que tipo de error pueden existir, ¿seremos capaces de reconocer uno cuando lo veamos? Si existe una copia de lo que se esta transmitiendo para poder compararla, por supuesto que seriamos capaces. Pero ¿que ocurre si no tenemos una copia de la original? Es este caso no se podría saber si ha habido un error en la transmisión sino hasta finalizar la transmisión y verificar si tiene sentido. Que una maquina comprobara los errores de esta forma seria costoso, lento, y de un valor cuestionable.

Redundancia

Un mecanismo de detección de errores que satisfaga estos requisitos sería enviar dos veces cada unidad de datos. El dispositivo receptor sería entonces capaz de hacer una comparación de cada unidad de datos. Cualquier discrepancia indicaría un error y se podría corregir mediante un mecanismo apropiado.

Este sistema sería completamente exacto (las probabilidades de introducir errores exactamente en los mismos bits de ambas copias serian infinitesimalmente pequeñas), pero también seria insoportablemente lento. No solamente se doblaría el tiempo para la transmisión, sino que además habría que añadir el tiempo necesario para comparar cada bit a bit. El concepto de inclusión de la información extra en la transmisión con el único fin de comparar es bueno. Pero en lugar de repetir todo el flujo de datos, se puede añadir un grupo más pequeño de bits al final de cada unidad. Esta técnica se denomina redundancia porque los bits extra son redundantes a la información; se descartan tan pronto se comprueba la exactitud de la transmisión.

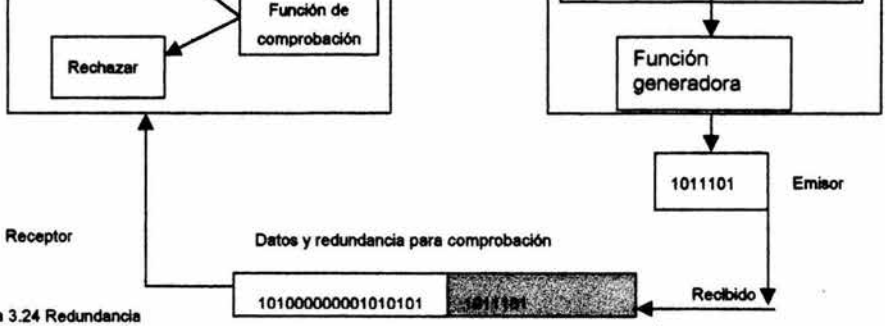


Figura 3.24 Redundancia

La figura 3.24. muestra el proceso de uso de los bits redundantes para comprobar la exactitud de una unidad de datos. Una vez que se ha generado el flujo de datos, se pasa a través de un dispositivo que lo analiza y le añade un código redundante codificado apropiadamente. La unidad de datos ahora alargada con varios bits (siete en la ilustración) viaja por el enlace hasta el receptor. El receptor pasa todo el flujo a través de una función de comprobación. Sí el flujo de bits recibido pasa los criterios de comprobación, la porción de datos de la unidad de datos se acepta y los bits redundantes son descartados.

En las comunicaciones de datos se usan cuatro tipos de comprobaciones de redundancia: verificación de redundancia vertical (VRC, vertical redundancy check) (también llamada verificación de paridad), verificación de redundancia longitudinal (LRC, longitudinal redundancy check), verificación de redundancia cíclica (CRC, cycle redundancy check) y suma de comprobación (checksum). Las tres primeras VRC, LRC, y CRC se implementan habitualmente en el nivel físico para que se puedan usar en el enlace de datos. La cuarta, la suma de comprobación, se usa principalmente en los niveles más altos.

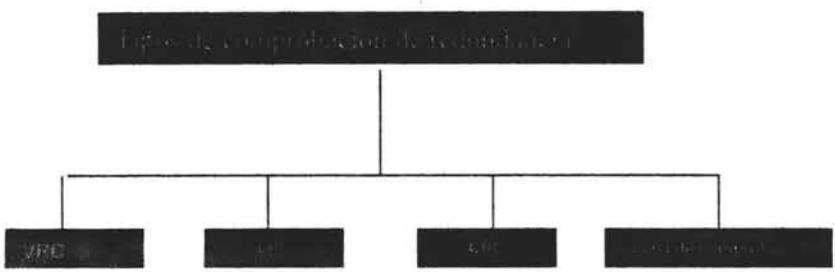


Figura 3.25. Tipos de comprobación de redundancia

3.6.3 Corrección de errores

Los mecanismos mostrados hasta el momento detectan errores pero no los corrigen. La corrección de error se puede conseguir de dos formas. En la primera, cuando se descubre un error, el receptor puede pedir al emisor que reenvié toda la unidad de datos. Con la segunda, el receptor puede usar un código corrector de errores que corrija automáticamente determinados errores. En teoría, es posible, corregir cualquier error automáticamente en un código binario. Sin embargo, los códigos correctores de errores son mas sofisticados que los códigos detectores de errores y necesitan mas bits de redundancia. El numero de bits necesarios para corregir un error de varios bits o un error de ráfaga es tan alto que en la mayoría de los casos su uso no resulta eficiente. Por esta razón, la mayoría de la corrección se limita a errores de uno, o tres bits.

Corrección dos de errores en un único bit

El concepto subyacente en la corrección de errores se puede comprender más fácilmente examinando el caso más sencillo: errores de un único bit. Como se menciono anteriormente, los errores en un único bit se pueden detectar añadiendo un bit de redundancia (paridad) a la unidad de datos (VRC). Un único bit adicional puede detectar errores en un único bit en cualquier secuencia de bits porque debe distinguir únicamente dos condiciones: error o no error.

Un bit de dos estados (0 y 1). Estos dos estados son suficientes para este nivel de detección. Pero ¿que ocurre si además de detectar errores en un único bit se requieren corregir?. Dos estados son suficientes para detectar un error, pero no para corregirlo.

Un error se produce cuando el receptor lee un bit 1 como un 0 o un 0 como un 1. Para corregirlo el error, el receptor únicamente debe invertir el valor del bit alterado. Sin embargo, para hacer eso, debe saber en que bit esta el error. Por lo tanto el secreto de la corrección de errores es localizar el bit o bits alterados.

Por ejemplo, para corregir un error de bit en un carácter ASCII, el código de corrección de error debe determinar cual de los siete bits a cambiado. En este caso, es necesario distinguir entre ocho estados distintos: no-error, en posición 1, error en posición 2, etc, hasta el error en la posición 7. Esto necesita suficientes bits de redundancia para mostrar los ocho estados. Aparentemente resultaría eficaz añadir un código de redundancia de tres bits porque estos tres bits pueden mostrar ocho estados distintos (000 a 111) y, por lo tanto, pueden indicar la posición de las ocho posibilidades distintas. Pero, ¿qué ocurre si hay un error en los propios bits de redundancia? Siete bits de datos (el carácter ASCII) mas tres bits de redundancia son 10. Sin embargo, tres bits pueden identificar únicamente ocho posibilidades. Por tanto, es necesario añadir más bits para cubrir las posibles posiciones del error

Bits de Redundancia

Para calcular el número de bits de redundancia (r) necesarios para corregir un número de bits de datos determinado (m), es necesario encontrar una relación entre m y r. La figura 3.26 muestra m bits de datos con r bits redundantes añadidos. La longitud del código resultante es m+r.

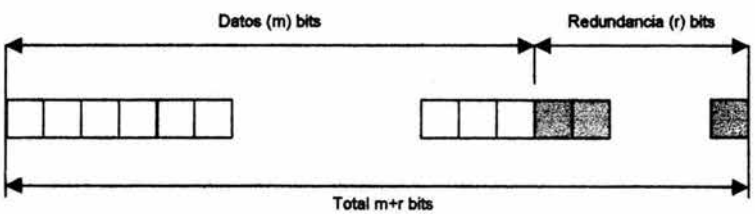


Figura 3.26 Bits de datos y de redundancia

Sí el número de bits en una unidad transmisible es m+r, entonces r debe ser capaz de indicar al menos m+r+1 estados distintos. De todos ellos, un estado significa que no hay error y m+r estados indican la existencia de un error en cualquier de las m+r posiciones.

Por lo tanto es necesario descubrir m+r+1 estados con r bits; y r bits pueden indicar 2^r estados distintos. Por lo tanto, 2^r debe ser igual o mayor que m+r+1.

$$2^r >= m+r+1$$

El valor de r se puede determinar despejando el valor de m (la longitud original de la unidad de datos a transmitir). Por ejemplo, si el valor de m, es 7 (como en el código ASCII de siete bits), el valor mas pequeño de r que puede satisfacer esta ecuación es 4.

$$2^4 >= 7+4+1$$

1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

Tabla 3.2 Relación entre bits de datos y de redundancia

Una vez que ya se describieron algunas de las generalidades de telecomunicaciones más importantes en el próximo capitulo procederemos al estudio y explicación de los conceptos básicos de redes que consideramos indispensables para el desarrollo de este trabajo de investigación.

CAPÍTULO 4

CONCEPTOS BÁSICOS DE REDES

4.1 TIPOS DE REDES DE COMPUTADORAS

Las redes de información se pueden clasificar según su extensión y su topología. Una red puede empezar siendo pequeña para crecer junto con la organización o institución. A continuación se presenta los distintos tipos de redes disponibles:

4.1.1 Redes de Área Local (LAN)

Una red LAN es un sistema de comunicaciones de alta velocidad diseñado para interconectar desde dos hasta cientos de computadoras y otros dispositivos de procesamiento de datos ubicados dentro de un área relativamente pequeña como puede ser un departamento de su empresa, un grupo de trabajo o en un piso de un edificio de varios pisos. A su vez, las redes LAN se pueden interconectar con otras LAN en otros pisos o en otros edificios, lo que se conoce como "internetworking", para formar una red empresarial o internetwork. Las redes LAN de hoy, utilizan tecnología de acceso compartido, esto quiere decir que todos los dispositivos conectados a la red comparten un mismo medio de comunicación, usualmente cable UTP (par trenzado).

4.1.2 Red de Área Metropolitanas (MAN)

Una red MAN es una red que se expande por pueblos o ciudades y se interconecta mediante diversas instalaciones públicas o privadas, como el sistema telefónico o los suplidores de sistemas de comunicación por microondas o medios ópticos.

4.1.3 Diferentes Arquitectura de Redes (WAN y Redes Globales)

Las WAN y redes globales se extienden sobrepasando las fronteras de las ciudades, pueblos o naciones. Los enlaces se realizan con instalaciones de telecomunicaciones públicas y privadas, además por microondas y satélites. fibra óptica. La tecnología de redes LAN más usada en estos días es Ethernet, utilizada por más del 80% de las instalaciones de redes LAN.

4.2 VPN

Dado que la red de TESYS es una red que se extiende sobre un área geográfica amplia y contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones) de manera remota es necesario que cumpla con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes WAN reducen en tiempo y dinero los gastos de las empresas, esta gran ventaja ayudará a TESYS ya que cuenta con usuarios remotos a varios kilómetros de distancia, pero también es cierto que este tipo de redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia.

4.2.1 ¿Qué es una VPN?

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación de los paquetes de datos, a distintos puntos remotos mediante el uso de una infraestructura pública de transporte.
Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. (ver figura 4.1)

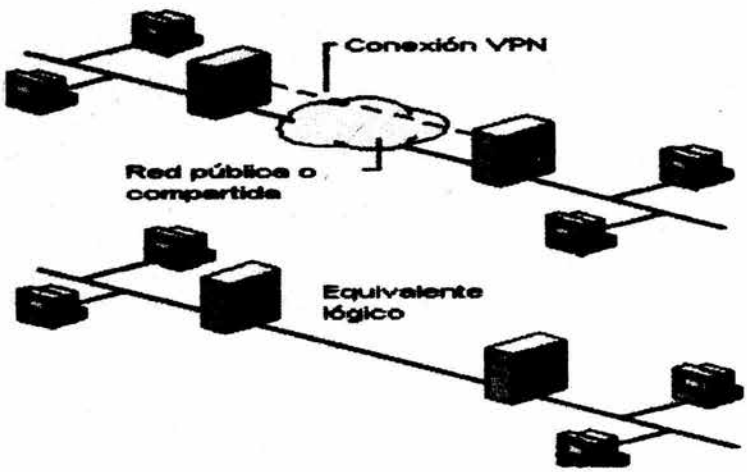


Figura 4.1 Túnel por medio de la red pública

Figura 4.2 Funcionamiento de la VPN

En la figura anterior (figura 4.2) se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando al firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a la nube de Internet donde se

genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad garantizada, con un ancho de banda también garantizado lleguen a su vez al destino remoto.

Las VPN pueden enlazar las oficinas corporativas de TESYS con los socios, con los usuarios móviles, con oficinas remotas mediante los protocolos como Internet, IP, IP Sec, Frame Relay, ATM como lo muestra la figura 4.3 a continuación.

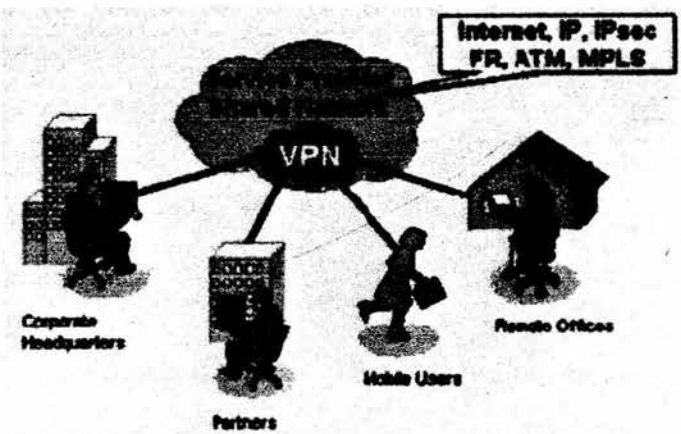


Figura 4.3 Formas de enlace VPN

4.2.2 Tecnología de Túnel

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos, a esto se le conoce como encapsulación, además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

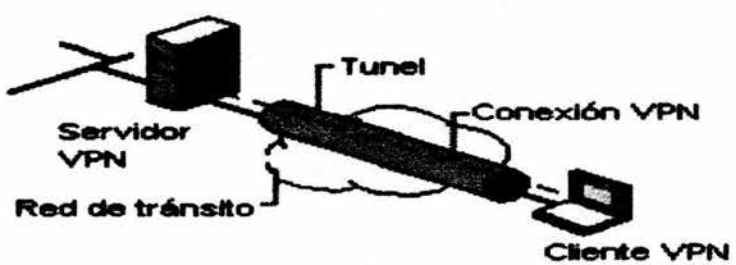


Figura 4.4. Encapsulamiento de los datos

El servidor busca mediante un ruteador la dirección IP del cliente VPN y en la red de tránsito se envían los datos sin problemas.

4.2.3 Requerimientos básicos de una VPN

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

a) Identificación de usuario

b) Administración de direcciones

c) Codificación de datos

d) Administración de claves

e) Soporte a protocolos múltiples

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quién acceso, que información y cuando.

Administración de direcciones

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Codificación de datos

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

Administración de claves

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

Soporte a protocolos múltiples

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquetes de Internet (IPX) entre otros.

4.2.4 Herramientas de una VPN

a) VPN Gateway
b) Software
c) Firewall
d) Ruteador

4.2.5 Ventajas de una VPN

Dentro de las ventajas más significativas podemos mencionar, además de la integridad, confidencialidad y seguridad de los datos:

a) Reducción de costos.
b) Sencilla de usar.
c) Sencilla instalación del cliente en cualquier PC Windows.
d) Control de Acceso basado en políticas de la organización.
e) Herramientas de diagnostico remoto.

f) Los algoritmos de compresión optimizan el tráfico del cliente.
g) Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

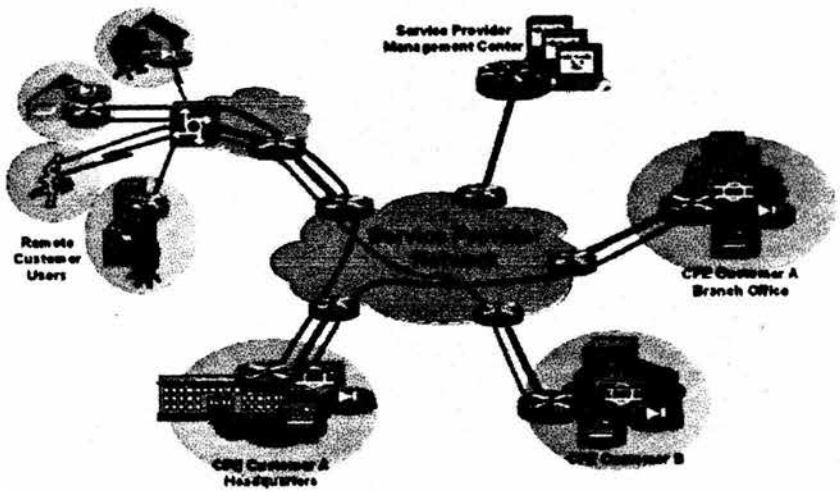


Figura 4.5 Diagrama de una VPN

4.3 TOPOLOGÍAS

La topología o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio. Existe un número de factores a considerar para determinar cual topología es la más apropiada para una situación dada. Existen tres topologías comunes:

4.3.1 Topología tipo anillo

Las estaciones están unidas unas con otras formando un círculo por medio de un cable común (Figura 4.6). El último nodo de la cadena se conecta al primero cerrando el anillo. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Con esta metodología, cada nodo examina la información que es enviada a través del anillo. Si la información no está dirigida al nodo que la examina, la pasa al siguiente en el anillo. La desventaja del anillo es que si se rompe una conexión, se cae la red completa.

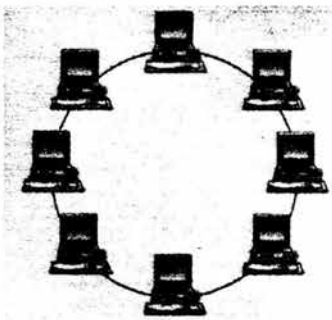


Figura 4.6Topología de anillo

4.3.2 Topología tipo estrella

La red se une en un único punto, normalmente con un panel de control centralizado, como un concentrador de cableado (Figura 4.7). Los bloques de información son dirigidos a través del panel de control central hacia sus destinos. Este esquema tiene una ventaja al tener un panel de control que monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red.

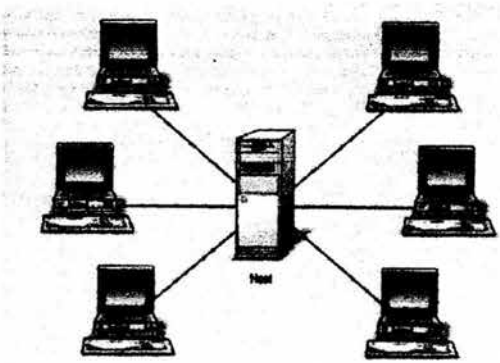


Figura 4.7 Topología de estrella

4.3.3 Topología tipo bus

Las estaciones están conectadas por un único segmento de cable (Figura 4.8). A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo. Los nodos en una red de "bus" transmiten la información y esperan que ésta no vaya a chocar con otra información transmitida por otro de los nodos. Si esto ocurre, cada nodo espera una pequeña cantidad de tiempo al azar, después intenta retransmitir la información.

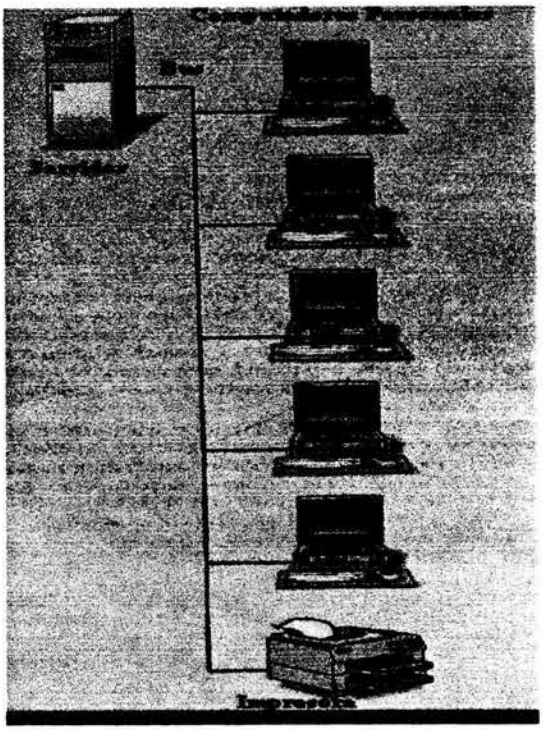


Figura 4.8 Topología tipo bus

4.3.4 Topologías Híbridas

El bus lineal, la estrella y el anillo se combinan algunas veces para formar combinaciones de redes híbridas (Figura 4.9).

Anillo en estrella:

Esta topología se utiliza con el fin de facilitar la administración de la red. Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo.

"Bus" en estrella:

El fin es igual a la topología anterior. En este caso la red es un "bus" que se cablea físicamente como una estrella por medio de concentradores.

Estrella jerárquica:

Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada par formar una red jerárquica.

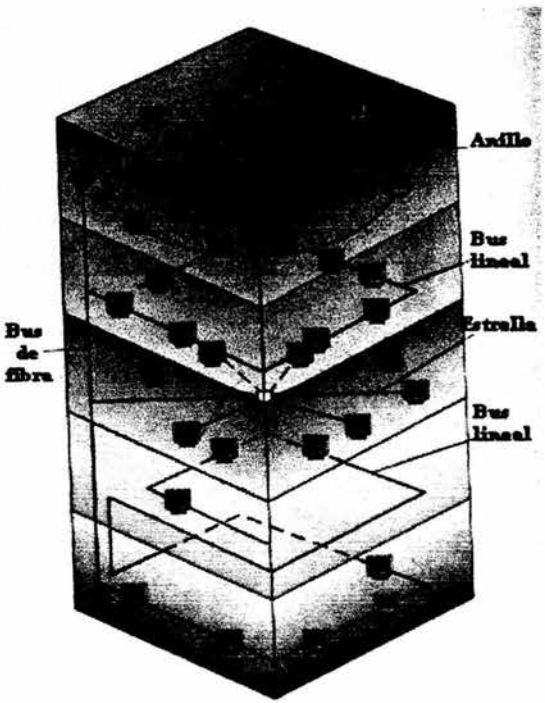


Figura 4.9 Topologías Híbridas

4.4 LA RED DE TELEFONÍA PÚBLICA

La red telefónica es la de mayor cobertura geográfica, la que mayor número de usuarios tiene, y ocasionalmente se ha afirmado que es "el sistema más complejo del que dispone la humanidad". Permite establecer una llamada entre dos usuarios en cualquier parte del planeta de manera distribuida, automática, prácticamente instantánea. Este es el ejemplo más importante de una red con conmutación de circuitos.

4.4.1 Realización de una llamada

Una llamada iniciada por el usuario origen llega a la red por medio de un canal de muy baja capacidad, el canal de acceso, dedicado precisamente a ese usuario denominado línea de abonado. En un extremo de la línea de abonado se encuentra el aparato terminal del usuario (teléfono o fax) y el otro está conectado al primer nodo de la red, que en este caso se llamó central local. La función de una central consiste en identificar en el número seleccionado, la central a la cual está conectado el usuario destino y enrutar la llamada hacia dicha central, con el objeto que ésta le indique al usuario destino, por medio de una señal de timbre, que tiene una llamada. Al identificar la ubicación del destino reserva una trayectoria entre ambos usuarios para poder iniciar la conversación. La trayectoria o ruta no siempre es la misma en llamadas consecutivas, ya que ésta depende de la disponibilidad instantánea de canales entre las distintas centrales.

Con esta arquitectura es muy probable que dos llamadas entre una pareja de usuarios ocupen diferentes rutas, lo cual frecuentemente se refleja también en la calidad de la llamada que los usuarios perciben.

4.4.2 Centrales Telefónicas

Es evidente que por la dispersión geográfica de la red telefónica y de sus usuarios existen varias centrales locales, las cuales están enlazadas entre sí por medio de canales de mayor capacidad, de manera que cuando ocurran situaciones de alto tráfico no haya un bloqueo entre las centrales. Existe una jerarquía entre las diferentes centrales que les permite a cada una de ellas enrutar las llamadas de acuerdo con los tráficos que se presenten. Los enlaces entre los abonados y las centrales locales son normalmente cables de cobre, pero las centrales pueden comunicarse entre sí por medio de enlaces de cable coaxial, de fibras ópticas o de canales de microondas. En caso de enlaces entre centrales ubicadas en diferentes ciudades se usan cables de fibras ópticas y enlaces satelitales, dependiendo de la distancia que se desee cubrir. Como las necesidades de manejo de tráfico de los canales que enlazan centrales de los diferentes niveles jerárquicos aumentan conforme incrementa el nivel jerárquico, también las capacidades de los mismos deben ser mayores en la misma medida; de otra manera, aunque el usuario pudiese tener acceso a la red por medio de su línea de abonado conectada a una central local, su intento de llamada sería bloqueado por no poder establecerse un enlace completo hacia la ubicación del usuario destino (evidentemente cuando el usuario destino está haciendo otra llamada, al llegar la solicitud de conexión a su central local, ésta detecta el hecho y envía de regreso una señal que genera la señal de "ocupado").
La red telefónica está organizada de manera jerárquica. El nivel más bajo (las centrales locales) está formado por el conjunto de nodos a los cuales están conectados los usuarios. Le siguen nodos o centrales en niveles superiores, enlazados de manera tal que entre mayor sea la jerarquía, de igual manera será la capacidad que los enlaza. Con esta arquitectura se proporcionan a los usuarios diferentes rutas para colocar sus llamadas, que son seleccionadas por los mismos nodos, de acuerdo con criterios preestablecidos, tratando de que una llamada no sea enrutada más que por aquellos nodos y canales estrictamente indispensables para completarla (se trata de minimizar el número de canales y nodos por los cuales pasa una llamada para mantenerlos desocupados en la medida de lo posible).
Asimismo existen nodos (centrales) que permiten enrutar una llamada hacia otra localidad, ya sea dentro o fuera del país. Este tipo de centrales se denominan centrales automáticas de larga distancia. El inicio de una llamada de larga distancia es identificado por la central por medio del primer dígito (en México, es el "0"), y el segundo dígito le indica el tipo de enlace (nacional o internacional; En este último caso, el tercer dígito indicara el país de que se trata). A pesar de que el acceso a las centrales de larga distancia se realiza en cada país por medio de un código propio, éste señala, sin lugar a dudas, cuál es el destino final de la llamada. El código de un país es independiente del que origina la llamada

Funciones básicas de las Centrales Telefónicas

Cada central realiza las siguientes funciones básicas:

a) Cuando un abonado levanta el auricular de su aparato telefónico, la central lo identifica y le envía una "invitación a marcar".
b) La central espera a recibir el número seleccionado, para, a su vez, escoger una ruta del usuario fuente al destino.

c) Si la línea de abonado del usuario destino está ocupada, la central lo detecta y le envía al usuario fuente una señal ("tono de ocupado").

d) Si la línea del usuario destino no está ocupada, la central a la cual está conectado genera una señal para indicarle al destino la presencia de una llamada.

e) Al contestar la llamada el usuario destino, se suspende la generación de dichas señales.

f) Al concluir la conversación, las centrales deben desconectar la llamada y poner los canales a la disposición de otro usuario, a partir de ese momento.

g) Al concluir la llamada se debe contabilizar su costo para su facturación, para ser cobrado al usuario que la inició.

4.4.3 Servicios que ofrece la Red Telefónica

El servicio básico ofrecido al público en general, por medio de la red pública telefónica, es el de comunicación de voz, es decir, la transmisión bidireccional de señales de voz, con el objeto de que dos usuarios puedan establecer y sostener una conversación. Este servicio, como ya se ha explicado, tiene básicamente dos componentes: 1) etapa de señalización, que incluye la selección del número del destinatario, la identificación de una ruta por medio de la conmutación, la reservación de la misma y el timbrado; y 2) etapa de transmisión, que consiste en la conversión de las señales acústicas en señales eléctricas, su transporte a través de los medios de comunicación, y la conversión de señales eléctricas nuevamente en acústicas para ser entregadas al destinatario.

Servicio de Fax

Utilizando la red telefónica, pueden ser transmitidos documentos impresos o escritos; esto es lo que se conoce como "facsímil" o "fax". Este servicio se originó en Japón, debido a la dificultad de transmitir los caracteres escritos del japonés vía un procesador de texto. La penetración del servicio en el mercado se vio fuertemente impulsada por el establecimiento y adopción de normas internacionales desde una etapa temprana de su desarrollo (la falta de estas normas fue una desventaja definitiva para muchos otros servicios). Hasta hace unos 15 años se podía considerar la tecnología del facsímil como un gigante dormido, pero su uso se incrementó notablemente al legalizarse y liberalizarse en muchos países y al avance de la tecnología, permitiendo transmisiones de alta velocidad y alta calidad, lo cual también tuvo como consecuencia la reducción del costo de los aparatos de fax y una simplificación en su operación. Actualmente se está estudiando la definición de normas para facsímil a color. De hecho, están en desarrollo sistemas nuevos que serían una mezcla de lo que actualmente es el facsímil y las fotocopiadoras. Los tiempos de transmisión se han reducido de seis a menos de un minuto por página tamaño carta; las resoluciones han aumentado al pasar de 1728 píxeles ("píxel" proviene del inglés "picture element") hasta 3456 píxeles por línea barrida, y al cambiar de 3.85 píxeles/ mm hasta 15.75 píxeles/ mm.

Servicios Digitales

Considerando la amplia cobertura de la red telefónica y los desarrollos tecnológicos de las últimas décadas, muchos esfuerzos se han dirigido hacia la posibilidad de transmitir señales digitales sobre la misma infraestructura, lo cual aumentaría de manera considerable la cantidad de servicios que podrían ser ofrecidos por medio de esta red. De lograrse esto, la red telefónica sería transporte de bits (unos y ceros), sin importarle la fuente o el servicio que genera dichos bits. El razonamiento para lograr lo anterior es el siguiente: si a través de la red telefónica se pueden transmitir señales eléctricas que corresponden al rango de frecuencias que genera el hombre al producir sonidos hablados, entonces, si se generan tonos en este mismo rango que correspondan a los símbolos binarios "1" y "0" se podrían realizar transmisiones digitales binarias.

Este proceso se conoce como modulación, y, el inverso, es decir, extraer del canal o de la red los tonos para generar nuevamente los símbolos binarios, es la de modulación. Con base en estos dos términos, los equipos que realizan estas operaciones para transmisión de datos, se denominan módems. Los módems han evolucionado rápidamente: en la década de los sesenta podían ser transmitidos hasta 300 bits por segundo (bps) con un éxito aceptable; posteriormente, pasando por etapas de 600, 1200, etc. se ha logrado contar con módems disponibles comercialmente que manejan tasas de transmisión de 9600 bps. En algunos casos se pueden efectuar transmisiones de 19200 bps. Con esto se inició la comunicación entre computadoras y equipos digitales, en general utilizando la red pública telefónica. Por ejemplo, en sus orígenes, esto permitió realizar lo que en los años setenta se conocía como "procesamiento remoto", es decir, contando con una terminal de computadora, un par de módems (uno para cada extremo del canal de comunicaciones) y una línea telefónica, se podía interactuar remotamente con una computadora sin tener que estar físicamente en el mismo lugar que la máquina.

Otros Servicios de Telecomunicaciones.

Al igual que en el caso de los equipos de fax, también fue indispensable el establecimiento de reglas claras que permitieran la comunicación entre los módems, para compensar efectos de retrasos en la red (originados por la conmutación) y desde luego, por los efectos del ruido en las líneas. Estos logros en materia de transmisión de datos fomentaron el desarrollo de nuevos servicios de telecomunicaciones por medio de la red telefónica. Por ejemplo el videotexto, originalmente concebido como un servicio de información que emplearía monitores de televisión para desplegar texto originado en bases de datos remotas, transmitido a través de líneas telefónicas de la red pública, la cual es accesada por medio de un módem de baja velocidad.
Otros ejemplos consisten en servicios tales como la consulta remota a bases de datos, correos electrónicos (envío de mensajes entre computadoras), transmisión de archivos entre computadoras, y en general, servicios que exploten las ventajas de las técnicas de procesamiento digital de señales.

Las centrales modernas (los nodos de la red) están basadas en sistemas totalmente digitales, lo cual contribuye a que se puedan ofrecer al usuario servicios tan sencillos como conferencias de voz, transmisión de datos y videoconferencias; y tan rudimentarios como dar de alta la línea de un nuevo usuario, indicar el número que llama, transferir llamadas a otro número telefónico, etc. La clave para explotar el potencial de la infraestructura digital está, por una parte, en el hardware, y por la otra en el software, cada día de mayor importancia. Entre los servicios nuevos, que gracias a la digitalización de las centrales han podido ofrecerse al público, se encuentran las llamadas de larga distancia sin costo para el que las inicia (en México LADA 800), las llamadas con abono al que las recibe (el servicio 1-900 en Estados Unidos) y diversos tipos de señalización como la presencia de un tono que avisa a los interlocutores la llegada de otra llamada durante su conversación. Varias de las funciones que realizan las centrales, también pueden ser efectuadas por conmutadores privados, que en realidad son pequeñas centrales telefónicas. Entre ellas están la búsqueda de personas, la selección y la configuración de grupos, la disponibilidad de distintos modos de operación para diferentes horarios, la restricción de llamadas de larga distancia y la asignación de privilegios en general a cada una de las extensiones, el almacenamiento de información sobre llamadas y de las extensiones que las originaron, la puesta en espera de llamadas, la disponibilidad de directorios en línea, etcétera.

4.5 RED DIGITAL DE SERVICIOS INTEGRADOS (RDSI)

4.5.1 Breve historia de la RDSI

Década de los 60´s:

Se encuentra la solución a un viejo problema, la pérdida de calidad de sonido en las llamadas a larga distancia. La solución consistía en utilizar canales de larga distancia digitales; en estos canales la voz era digitalizada y enviada como datos numéricos, volviéndola a convertir en una señal analógica en el otro extremo de la línea. Puesto que en los enlaces digitales la información no sufre deterioro, las llamadas continentales podían tener la misma calidad de sonido que las llamadas locales. El esquema de digitalización elegido fue tomar muestras, que en Europa eran de 8 bits y en EE.UU. de 7 bits, a una velocidad de 8000 muestras por segundo; esto significaba que estos canales debían funcionar a 64000 bits por segundo en Europa (8 bits * 8000 muestras) y 56000 bits por segundo en EE.UU. (7 bits * 8000 muestras).

Década de los 70´s:

Las compañías telefónicas se enfrentan a un nuevo desafío; las grandes empresas están interesadas en poder interconectar sus computadoras para satisfacer esta nueva demanda se crean las primeras redes experimentales de transmisión de datos.

Década de los 80´s:

Exactamente en al año de 1984 se reúne la asamblea general de la CCITT (organismo, dependiente de la ONU, tiene como función establecer los estándares técnicos utilizados en telefonía, con el fin de garantizar la compatibilidad entre los equipos de las diferentes compañías) para hablar de los canales digitales, del imparable aumento de las comunicaciones por ordenador y de las nuevas demandas ya aparecidas o de previsible aparición (fax, vídeo, texto, videoconferencia, televisión por cable, y se toma una decisión histórica: la red telefónica mundial deberá reconvertirse en una red de transmisión de datos. El plan es que, en el siglo XXI, las típicas líneas analógicas utilizadas por los teléfonos de voz se habrán sustituido por líneas digitales capaces de ofrecer cualquier tipo de servicio, inventando o por inventar; esta nueva red se bautiza con el nombre de RDSI (Red Digital de Servicios Integrados).

Década de los 90´s:

Muchos países han completado la construcción de la RDSI; puede ponerse en marcha la RDSI. En la red telefónica, el canal de voz es la unidad básica de funcionamiento; esto significa que la RDSI estará formada por grupos de canales de 64 kbps. En Europa y 56 kbps. En EE.UU., lo que también supone que esta deberá ser la velocidad de los canales RDSI.

4.5.2 La RDSI en la Actualidad.

Según la definición establecida por la UIT (Unión Internacional de Telecomunicaciones) es una red que procede por evolución de la Red Digital Integrada y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto definido de interfaces formalizadas. Más comúnmente puede describirse como una red que procede por evolución de la red telefónica existente que, al ofrecer conexiones digitales extremo a extremo, permite la integración de multitud de servicios en único acceso, independientemente de la naturaleza de la información a transmitir, y del equipo terminal que la genere.

Esta red coexiste con las redes convencionales de telefonía y datos e incorpora elementos de interfuncionamiento para su interconexión con dichas redes, tendiendo a convertirse en la única y universal Red de Telecomunicaciones.

Las principales características de la RDSI son las siguientes:

a) Conectividad extremo a extremo.

b) Conmutación de circuitos a 64 Kbit/s.

c) Uso de vías separadas para la señalización y para la transferencia de información, lo que confiere al sistema en su conjunto una gran flexibilidad y potencia.

Estructura General de la RDSI:

a) Redes de Acceso y Tránsito:

Es la misma Red Integrada Digital, la cual está constituida básicamente por centrales de conmutación digital conectadas mediante sistemas de transmisión digital.

b) Centrales de Conmutación Digital:

Realizan principalmente conexiones por conmutación de circuitos a 64 Kbit/s. También contienen elementos necesarios para soportar el sistema de señalización por canal común. Son, además, elementos inteligentes que pueden dar soporte a facilidades adicionales y servicios de valor añadido, tanto para los usuarios como para la propia explotación de la red.

c) Acceso de Usuario.

Constituye el elemento diferenciador entre la RDSI y la RTC, al permitir extender la conectividad digital hasta el terminal de usuario mediante unas configuraciones normalizadas. Incluye las instalaciones interiores propias del usuario así como el bucle del abonado (conexión con la central local).

En el acceso de usuario se requiere de dos partes principales a saber, la instalación interior del usuario y la red local.

La instalación interior del usuario esta formada por los equipos terminales de usuario y por una red interior que conecta dichos terminales a la línea de transmisión digital. Ciertas instalaciones de usuario pueden contener, además, equipos de conmutación local como, por ejemplo, centralitas digitales.

La red local esta formada por los sistemas de transmisión digital entre la instalación de usuario y la central local y, en ocasiones, por otros elementos auxiliares de conexión como por ejemplo, los multiplexores.

d) Nodos especializados: Pueden ser de diversos tipos, como por ejemplo, servicios de valor añadido, interconexión de redes, centros de explotación en red, etc.

Ventajas de la RDSI.

Las ventajas de la RDSI frente a la RTC son resumibles en tres grupos, estos son ventajas en cuanto a velocidad, ventajas en cuanto a la no-necesidad de múltiples dispositivos o interfaces (líneas telefónicas), y ventajas en cuanto a la señalización:

a) Velocidad.

Existe un límite superior en cuanto a la cantidad de información que una línea telefónica analógica puede soportar (transmitir). Actualmente este límite está en los 56 kbps usando un equipo especial. Usualmente los módems mas extendidos tienen una velocidad máxima de transmisión de 56 kbps, aunque están limitados por la calidad de la conexión analógica y es rara la vez que van a velocidades mayores de 26.4 o 28.8 kbps. RDSI, en cambio, permite tener múltiples canales digitales, y permite que operen simultáneamente a través del mismo cable telefónico. El cambio empieza cuando las centrales de conmutación de las redes telefónicas empiezan a soportar conexiones digitales ya que este esquema permite un radio de transmisión de datos mucho mayor que el permitido por las líneas analógicas. Un canal RDSI Básico (BRI), usando un protocolo adicional para el canal (como BONDING, o Multilink - PPP) soporta una velocidad de transferencia de hasta 128 kbps (sin compresión de datos de ningún tipo).

b) Múltiples Dispositivos.

Antes, era necesario tener una línea telefónica para cada dispositivo que se quisiera usar simultáneamente. Por ejemplo, era necesaria una línea telefónica para un teléfono, otra para un fax, otra para el ordenador y otra para un sistema de videoconferencia en caso de que se quisieran usar todos estos aparatos simultáneamente. Por lo tanto estar bajando un fichero, mientras estas hablando por teléfono o viendo una animación real en una pantalla de vídeo puede necesitar un número excesivamente alto de líneas telefónicas (sobre todo en precio). En cambio, la RDSI nos permite combinar diferentes fuentes de datos digitales y enrutar cada una de ellas al destino adecuado. Debido a que la línea es digital, es más fácil mantener los niveles de ruido e interferencias bajo mínimos mientras combinamos todas las señales que recibimos de los distintos dispositivos. RDSI técnicamente se refiere a un grupo específico de servicios digitales que nos son dados a través de una sola interfase estándar. Sin RDSI, serían necesarios diferentes interfaces para cada dispositivo.

c) Señalización

Con RDSI, la compañía de teléfonos, en lugar de mandar un voltaje de llamada a la campana de nuestro teléfono ("Señal 'InBand'") nos mandará un conjunto de señales digitales en un canal separado ("señal 'Out-of-Band'"). El canal 'Out-of-Band' permite no "molestar" a conexiones que previamente hayamos establecido y el restablecimiento de llamada es muy rápido.

Canales de Acceso

Para la transferencia de información y señalización se han definido en los RDSI los siguientes tipos de canales digitales (o vías de transferencia de la información):

Canal B

Es un canal a 64 Kbit/s, que transporta la información generada por la terminal del usuario.

b) Canal D

Es una canal a 16 ó 64 Kbit/s., Dependiendo de la estructura de acceso del abonado, que se utiliza para transportar la señalización en la interfaz usuario-red. También puede utilizarse para transmitir información de usuario a baja velocidad.

c) Canal n x 64

Permite la transferencia de información de usuario a velocidades superiores a 64 Kb/s. Los valores válidos para n serán desde 2 hasta 30.

d) Canales H

Los canales H, proporcionan una manera de agregar canales B. Son implementados del siguiente modo: H0 = 384 kbps. (6 canales B) H10 = 1472 kbps (23 canales B) H11 = 1536 kbps (24 canales B) H12 = 1920 kbps (30 canales B) Para tener acceso a un servicio BRI es necesario contratar una línea telefónica RDSI. Los usuarios también necesitarán un equipo especial terminal para poder habilitar la comunicación con la compañía telefónica o con otros terminales RDSI.

4.5.3 Topologías de Acceso Básico

La red interior de usuario, en general, no es sino un cable de dos pares que discurre desde la TR1 según distintas topologías hasta un punto extremo en el que se conectarán, siempre, unas resistencias de terminación. A lo largo de este cable se encuentran una serie de rosetas en número variable. Atendiendo a la configuración del cableado, podemos distinguir entre tres tipos de configuración del acceso básico:

Bus Pasivo Corto.

En esta configuración, se dispone de un cable de hasta 200m, sobre el que se pueden instalar, distribuidas aleatoriamente, un máximo de 10 rosetas en las que se permite tener conectados simultáneamente hasta 8 terminales. Existen dos modalidades de esta configuración: en la más habitual, la TR1 (Es el elemento que permite la interconexión entre la instalación interior del usuario a 4 hilos, y la red exterior, a 2 hilos) se ubicará en uno de los extremos del bus que se extenderá en la longitud mencionada hasta finalizar en una roseta que incluirá una resistencia de terminación. La otra posibilidad consiste en ubicar la TR1 en un punto intermedio del bus estableciendo de esta manera dos ramas, ninguna de las cuales podrá superar los 200m. En este caso, la distancia entre los extremos del bus podrá ser de hasta 400m y en ambos extremos habrá una resistencia de terminación. No se permiten configuraciones con más de dos ramas.

Bus Pasivo Extendido.

En el caso de que 200m no sean suficientes para llegar desde la TR1 hasta el emplazamiento donde se encuentran los terminales, se puede instalar este tipo de bus caracterizado por que con él se alcanzan hasta 500m. Sin embargo, en este caso solo se permite la conexión simultánea de un máximo de 4 terminales que, además, deberán de encontrarse agrupados en los últimos 50m del bus. Presenta una sola rama con resistencia de terminación en su extremo. En otras palabras, se gana alcance y se pierde flexibilidad.

Bus Largo

Si con el bus extendido no es suficiente, aún disponemos del bus largo, denominado así porque alcanza los 1000m. Presenta una sola rama con resistencia de terminación en su extremo. En este caso, solo se puede conectar un único terminal. Por razón de soportar un único terminal, se conoce también esta topología como bus punto a punto. No se debe confundir sin embargo esta terminología que hace referencia a una configuración de cableado, con otra que en los mismos términos se refiere al modo de funcionamiento de la capa de datos del protocolo de canal D.

4.5.4 Configuraciones de Acceso de la RDSI.

Existen dos configuraciones elementales de acceso a la RDSI conocidas como configuración de acceso básico y configuración de acceso primario, estas se pueden comercializar de forma individual o se pueden agrupar entre sí, o incluso de manera cruzada de tal forma que se obtengan funcionalidades que mejoran lo que ofrecería cada una de estas configuraciones de manera independiente.

Acceso Básico (BRI)

El Acceso Básico o BRI (BASIC RATE INTERFACE) está constituido por dos canales B (a 64 kb/s.) Para la transmisión de información, y un canal D (a 16 Kb/s.) Para la señalización de usuario. Permite conectar simultáneamente hasta 8 terminales. En el lado de instalaciones de usuario, (interfaz S/T), la velocidad de transmisión total es de 192 Kbps distribuidos de la siguiente manera: canales B, 1 canal D, y la información adicional necesaria para el mantenimiento del sincronismo, el mantenimiento de la estructura multitramas (actualmente no se utiliza), y el control de acceso al canal de señalización. Como ya se mencionó, está soportado por una configuración a cuatro hilos (dos para transmisión y dos para recepción). En el lado red, la velocidad en línea es de 160Kb/s. y la transmisión es full-dúplex con técnicas de cancelación de eco.

Acceso Primario (PRI)

El Acceso Primario o PRI (PRIMARY RATE INTERFACE) está constituido por 30 canales B (a 64 Kb/s) y un canal D (a 64 Kbit/s) con una velocidad total de 2 Mb/s. En el lado de las instalaciones de usuario se dispone de una trama de 2048 Kbit/s que, a través de una agrupación funcional TR2 (Es una agrupación funcional que realiza funciones de conmutación, concentración y control en el interior de las instalaciones del cliente) puede estructurarse en otras combinaciones de canales de entre las ya mencionadas. En el lado red, esto es, para enlazar las instalaciones de usuario con la central RDSI, el acceso está soportado por una sistema de transmisión MIC a 2 Mb/s.

Grupo Salto.

La funcionalidad del grupo de salto es una facilidad asociada exclusivamente a agrupaciones de accesos básicos mediante la cual, las llamadas dirigidas a un único número denominado número de cabecera ó número de salto, se ofrecerán por alguno de los posibles canales B libres disponibles dentro del conjunto de accesos que constituyen el grupo de salto. Esta funcionalidad de búsqueda de línea solo puede estar asociada a un único número para determinado grupo de salto, pero dicho número no será el único disponible en cada uno de los accesos. Al constituirse en grupo de salto, cada uno de los accesos básicos que lo integran no modifican sus comportamientos individualizados, ni en relación con el repertorio de servicios suplementarios asociados a cada uno de dichos números. Al constituir un grupo de salto a partir de accesos básicos (individuales) que ya estuvieran en servicio se deberá tener presente que como número de cabecera de dicho grupo se podrá configurar cualquiera de los números disponibles con anterioridad en cualquiera de los accesos, excepto los números principales de cada acceso. Es decir, un número principal de un acceso, nunca podrá constituirse como número de cabecera o de salto de un grupo de salto. Los servicios suplementarios ofertados para los accesos básicos con grupo de salto, serán los mismos que para el acceso básico. Sólo existen algunas restricciones para los servicios suplementarios que se aplican al número de salto. El grupo de salto solo podrá ofrecerse para accesos básicos dependientes de una misma central RDSI y bajo una misma titularidad. No es necesario que se encuentren en el mismo local.

Grupo ISPBX

El grupo ISPBX de accesos básicos constituye una estructura de acceso a RDSI caracterizada por tratarse de una agrupación de accesos básicos, a la que la red asocia todo el rango de numeración contratado, de tal manera que desaparece la relación biunívoca entre número y acceso, estableciéndose en su lugar otra asociación entre el conjunto de accesos considerado globalmente y el rango de numeración. Así, una llamada dirigida a un número de entre los contratados, se ofrece al terminal que el usuario conecta en el grupo ISPBX por cualquiera de los canales B libres de cualquiera de los accesos.
Existen distintas modalidades en cuanto a la manera en que podría distribuirse el tráfico entre los distintos accesos, (reparto cíclico, secuencial o aleatorio). La utilización de un grupo ISPBX implica la presencia de una agrupación funcional del tipo TR2.

4.5.5 Servicios de la RDSI

La RDSI puede ser la infraestructura soporte de los servicios de telecomunicación ya establecidos y de aquellos nuevos que, por su mayor capacidad, pueda ofrecer frente a las redes convencionales. Los servicios que en la RDSI se contemplan se dividen en dos categorías básicas:

Servicios Portadores

Estos servicios ofrecen al usuario RDSI, mediante una serie de interfaces normalizadas, una capacidad de transporte de información, independientemente de su contenido y aplicación, entre dos equipos terminales. Atendiendo a cómo se transmite esta información, podemos clasificarlos en:

Servicios Portadores en Modo Circuito.

Estos servicios se caracterizan porque toda la información de señalización (para el establecimiento, control y liberación de un canal digital entre dos equipos terminales) se efectúa por el canal D de señalización, viajando la información propiamente dicha por el circuito digital establecido por el/los canal/es B. Se clasifican según su categoría en: Servicio Portador a 64 Kb/s estructurado a 8 Khz sin restricciones(ofrece una capacidad de transferencia entre dos usuarios sin alterar la secuencia de bits transmitida), Servicio Portador a 64 Kb/s estructurado a 8 Khz para conversación (permite soportar comunicaciones vocales codificadas a 64 Kb/s), Servicio Portador a 64 Kb/s estructurado a 8 Khz para información de audio a 3,1 Khz (proporciona la transferencia de señales digitalizadas a partir de señales analógicas de 3,1 Khz de ancho de banda. Aunque este servicio transmite perfectamente señales de voz, está orientado a la transmisión de datos procedentes de módems que trabajan en dicha banda.

Servicios Portadores en Modo Paquete.

La RDSI puede proporcionar acceso a los servicios portadores en modo paquete en dos modalidades diferentes: Mediante conexión de Acceso a la Red Pública de datos por Conmutación de Paquetes (la RDSI se limita a proporcionar una conexión por conmutación de circuitos entre el usuario y la puerta de acceso a la RPDCP) y Mediante servicio de circuito virtual de la RDSI (la RDSI dispondría de los elementos necesarios para soportar la conmutación de paquetes).

Teleservicios.

Son servicios que, apoyándose en la RDSI, proporcionan servicios más sofisticados, aunque muchos de ellos están todavía en fase de desarrollo y habrá que esperar algún tiempo para ver su aplicación en la vida cotidiana. Así: La clave del desarrollo de la informática móvil está en los avances experimentados por la tecnología de las pantallas de las computadoras portátiles que actualmente compiten en calidad de imagen, aunque no en precio, con los monitores CTR. La creciente duración de las fuentes de alimentación de los ordenadores portátiles, gracias a sus subsistemas de gestión de consumo, prolongan su autonomía de forma que hoy resulta habitual desplazar fuera de las oficinas a muchos empleados que se mantienen en contacto con ésta a través de la comunicación por módem.

4.5.6 Transmisión de datos en la RDSI.

Canales de Transmisión y de Señalización.

Como ya se menciono la RDSI está formada por canales de comunicación digital a 64 Kbps (Kilo bits por segundo), pero para las comunicaciones se necesita algo mas, ya que es necesario controlar la comunicación. Es necesario poder llamar y colgar. Para estas funciones de control se utiliza un canal aparte, denominado canal de señalización; mediante este canal, con un protocolo de mensajes, se inician y terminan las llamadas y se realizan todas las funciones típicas disponibles en las líneas telefónicas modernas (y que las líneas RDSI conservan), funciones como retención de llamada, conferencia a tres, redirección de llamada, etc.

En la terminología de comunicaciones los canales de transmisión de datos se denominan canales B, y los canales de señalización se denominan canales D. Las compañías telefónicas ofrecen dos tipos fundamentales de líneas RDSI, las líneas básicas (BRI) y las líneas primarias (PRI). Una línea BRI consiste en un cable de dos o de cuatro hilos dos son para la transmisión, y los dos hilos opcionales se utilizan para proporcionar alimentación eléctrica al terminal NT1. Sobre este cable sé multiplexan dos canales B y un canal D a 16 Kbps, lo que da una velocidad total de 144 Kbps (64 * 2 canales B + 16 * 1 canal D = 144 Kbps.). Una línea PRI puede ser un cable coaxial o de fibra óptica sobre el que se multiplexan 30 canales B y un canal D a 64 Kbps, lo que da una velocidad total de 1984 Kbps. En el lado del abonado, la línea BRI finaliza en un terminal NT1, dispositivo que en esencia, es un módem; este aparato tiene un terminal de salida de 4 líneas llamado BUS S/T, al cual se puede conectar los equipos terminales (teléfono/fax, RDSI, ordenador) o un terminal NT2, que es un multiplexor que permite tener conectados varios equipos terminales a un mismo terminal NT1. Una línea PRI, en cambio, se conecta a una central (PBX) que dispone de interfaces para la conexión de terminales NT2.

Circuitos Virtuales

Existen múltiples técnicas para multiplexar varios canales sobre un mismo cable, y la elegida por el CCITT fue el de circuitos virtuales. Un circuito virtual es una técnica que se utiliza en protocolos de comunicaciones basados en paquetes (la unidad mínima de información es un paquete de bits o bytes). Cada paquete lleva una etiqueta que identifica un camino dentro de la red, camino que indica la ruta que deben seguir estos paquetes para ir desde la computadora origen hasta el destino. Los protocolos de circuitos virtuales disponen de un subprotocolo para abrir y cerrar dichas rutas, es decir, para "llamar" (crear una ruta que conecte nuestra máquina con otra máquina de red) y "colgar" (eliminar esa ruta).

4.5.7 Conexión a la RDSI desde una PC y el CAPI.

Conexión a la RDSI desde una PC

Cuando se contrata una línea RDSI la compañía telefónica instala una terminal NT-1, siendo responsabilidad del usuario instalar el equipo terminal de conexión en su ordenador. Existen múltiples formas de conectar dicho equipo a la computadora, aunque lo más común es que sea una placa que se enchufa en una ranura de expansión. El software necesario para hacer funcionar la placa es un driver para la misma, encima del cual se colocan los protocolos V110, HDLC, X.75 y Q.931, que se estructuran.
Encima de todos estos protocolos se sitúa la capa más importante: el CAPI. (Este software está formado por una serie de programas residentes en memoria, cada uno de los cuales implementa un protocolo).

El CAPI

Para manejar dispositivos RDSI desde los programas de aplicaciones se ha creado el CAPI, que es el acrónimo de "Common ISDN API", y define un protocolo que comunica el programa con el driver a través de dos colas de mensajes, una de envío, para los mensajes enviados por la aplicación al driver, y otra de recepción, para los mensajes enviados desde el driver a la aplicación. Si el sistema es multitarea, cada programa que esté en marcha dispondrá de una cola de recepción de mensajes propia, en cambio, la cola de envío es común a todas las aplicaciones. Cuando un programa envía un mensaje, la respuesta a ese mensaje se envía también como un mensaje.

Se ha elegido este sistema porque permite ignorar el mecanismo exacto utilizado para ejecutar las llamadas al driver, lo que lo hace independiente del sistema operativo, de hecho, existen implementaciones de CAPI para MS-DOS, OS/2, UNIX, etc. El CAPI solamente tiene definidas cuatro llamadas a función:

API_REGISTER
Registrar aplicación, esta función informa de que una aplicación va a hacer uso del dispositivo RDSI, al ejecutarla se crea una cola de recepción, se realizan las inicializaciones necesarias devuelve un identificador que deberá ser utilizado en los mensajes.

API_RELEASE
Librería aplicación, esta función informa de que la aplicación ya no necesita el dispositivo RDSI, al ejecutarla se liberan los recursos que se hayan podido ocupar y se elimina la cola de recepción.

API_PUT_MESSAGE
Envía un mensaje, esta función coloca un mensaje en la cola de envío.

API_GET_MESSAGE:
Recibe un mensaje, esta función lee el siguiente mensaje de la cola de recepción de la aplicación.

4.6 SONET/SDH CONFIGURACIÓN FÍSICA, NIVELES DE SONET.

El ancho de banda que ofrece el cable de fibra óptica es adecuado para las tecnologías que requieren las más altas tasas de datos de hoy en día (como la videoconferencia) y para transportar al mismo tiempo señales de un gran número de tecnologías de velocidades más bajas. Por esta razón la importancia de la fibra óptica crece junto con el desarrollo de tecnologías que requieren para transmitir altas tasa de datos o grandes anchos de banda. Dada su importancia se hace necesario su estandarización. Sin estándares, la interconexión entre sistemas propietarios existentes seria imposible. Los Estados Unidos (ANSI) y Europa (ITU-T) han respondido definiendo estándares que, aunque independientes, son fundamentalmente similares y en última instancia compatibles. El estándar ANSI se denomina Red Óptica Sincrónica (SONET, Synchronous Optical Netware). El estándar de la ITU-T se denomina Jerarquía Digital Sincrónica (SDH, Synchronous Digital Hierarchy). Estas dos normalizaciones son casi idénticas.

Entre los aspectos considerados por los diseñadores de SONET y SDH, hay tres de particular interés para nosotros. En primer lugar SONET/SDH es una red síncrona. Se utiliza un único reloj para gestionar la temporización de las transmisiones de los equipos a través de la red completa. Esta sincronización sobre toda la red añade una cierta capacidad de predicción al sistema. Esta capacidad de predicción, junto con un potente diseño de tramas, permite que los canales individuales sean multiplexados, mejorando por tanto la velocidad y reduciendo el costo.

En segundo lugar, SONET/SDH contiene recomendaciones para la normalización de los equipos de transmisión de fibra óptica (FOTS) vendidos por diferentes fabricantes. En tercer lugar, las especificaciones físicas de SONET/SDH y el diseño de las tramas incluyen mecanismos que permiten transportar señales de sistemas tributarios incompatibles (particularmente los servicios asíncronos como DS-0 y DS-1). Es esta flexibilidad la que da a SONET una buena reputación para la conectividad universal. Es importante hacer énfasis en que SONET es un mecanismo de transporte multiplexado y como tal puede ser portador de servicios de banda ancha, particularmente ATM y RDSI-BA.

4.6.1 Configuración Física

La figura 4.10 muestra los dispositivos utilizados en un sistema de transmisión SONET y algunas formas de organizar y enlazar estos dispositivos.

La transmisión con SONET depende de tres dispositivos básicos: multiplexores, STS, regeneradores y multiplexores de inserción/extracción (multiplexores add/drop).Los multiplexores STS marcan el comienzo y el final de un enlace SONET. Proporcionan la interfaz entre una red tributaria y la red SONET. Puede haber cualquier número de dispositivos entre ellos, y estos dispositivos pueden tener cualquier configuración requerida por el sistema. Los regeneradores extienden la longitud de los posibles enlaces entre el generador y el receptor. Los multiplexores de inserción/extracción permiten la inserción y extracción de caminos SONET.

a) Multiplexor/Demodulador STS.

Un Multiplexor/Demodulador STS o multiplexa las señales de varias fuentes en una señal STS o demultiplexa una señal STS en señales para diferentes destinos.

b) Regenerador.

Un regenerador STS es un repetidor que recibe una señal óptica y la regenera. Los regeneradores en este sistema, sin embargo, añaden una función a los repetidores de nivel físico. Un regenerador SONET reemplaza alguna información de sobrecarga existente (información de cabecera) con nueva información. Estos dispositivos funcionan en el nivel de enlace de datos.

c) Multiplexor de Inserción/Extracción.

Un Multiplexor de Inserción/Extracción puede añadir señales que vienen de fuentes diferentes en un camino o eliminar una señal deseada de un camino y redirigirla sin demultiplexarla señal entera. En lugar de depender de la temporización y las posiciones de los bits, los multiplexores de inserción/extracción utilizan la información de la cabecera, como direcciones y punteros para identificar los flujos individuales.

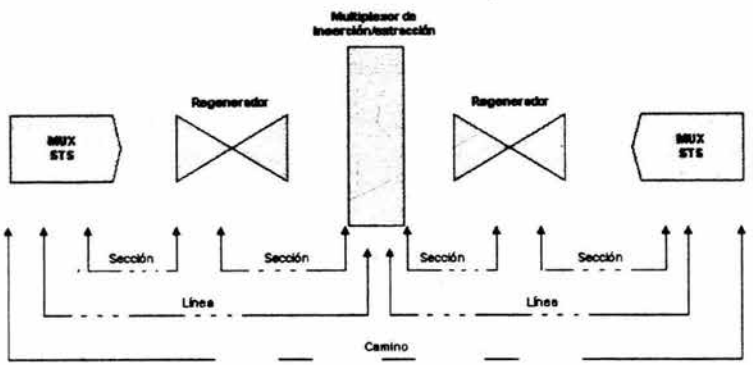


figura 4.10 Configuración básica de un sistema de transmisión SONET

En la sencilla configuración mostrada en la figura anterior varias señales electrónicas llegan a un mutiplexor STS, donde se combinan en una única señal óptica. La señal óptica se transmite a un regenerador, donde se regenera sin ruido y se mejora. Las señales regeneradas de varios orígenes son llevadas después de un multiplexor de inserción/extracción. El multiplexor de inserción/extracción reorganiza las estas señales, si es necesario, y las envía de acuerdo a la información de las tramas de datos. Estas señales remultiplexadas son enviadas a otro regenerador y de aquí al multiplexor STS de recepción, donde se convierten a un formato utilizable por los enlaces de recepción.

4.6.2 Niveles de conexión SONET

Como se puede ver en la siguiente figura los diversos niveles de las conexiones SONET se denominan secciones, líneas y caminos.

Una sección es el enlace óptico que conecta dos dispositivos vecinos: multiplexor a multiplexor, multiplexor a regenerador o regenerador a regenerador.

Una línea es la porción de red situada entre dos multiplexores: un multiplexor STS a un mutiplexor de inserción/extracción, dos multiplexores de inserción/extracción o dos multiplexores STS.

Un camino es la porción extremo a extremo de la red situada entre dos multiplexores STS. En una red SONET sencilla, compuesta de dos multiplexores STS enlazados directamente uno a uno, la sección, la línea y el camino son lo mismo.

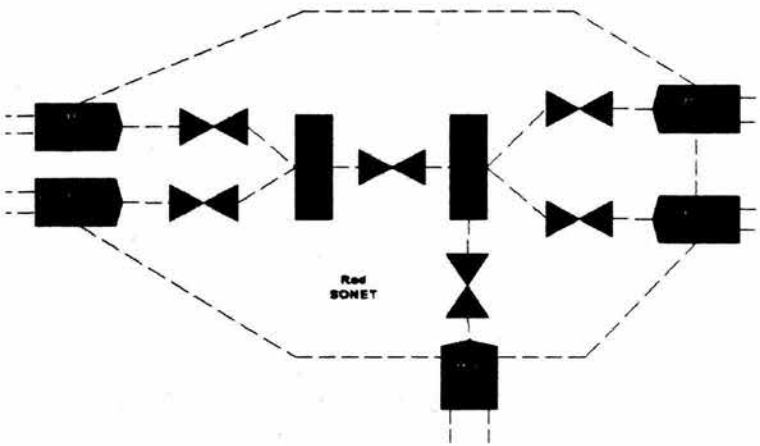


Figura 4.11 Niveles de conexión SONET

4.6.3 Niveles de Señalización (STS)

Como lo más importante es la flexibilidad, SONET define una jerarquía de niveles de señalización denominados señales de transporte síncronas (STS). Cada nivel STS (STS-1 a STS-192) soporta una cierta tasa de datos, especificada en megabits por segundo. Los enlaces físicos definidos para transportar cada nivel de STS se denominan portadoras ópticas (OC). Los niveles OC describen las especificaciones físicas y conceptuales de los enlaces requeridos para admitir cada nivel de señalización.

STS	OC	Velocidad (Mbps)	**STM**
STS-1	OC-1	51,840	
STS-3	OC-3	155,520	STM-1
STS-9	OC-9	466,560	STM-3
STS-12	OC-12		

622,080
STM-4

STS-18
OC-18
933,120
STM-6

STS-24
OC-24
1244,160
STM-8

STS-36
OC-36
1866,230
STM-12

STS-48
OC-48
2488,320
STM-16

STS-96
OC-96
4976,640
STM-32

STS-192
OC-192
9953,280
STM-64

Tabla 4.1 Niveles de Señalización

4.7 PROTOCOLOS DE ENLACE

Las redes proporcionan a las computadoras la habilidad básica de transferir bits de una a otra. Para poder usar las redes necesitamos un conjunto de reglas en las que todos los miembros de la red estén de acuerdo, esto es lo que conocemos como protocolo. Los protocolos de comunicaciones se diseñan para especificar cómo interactúan e intercambian mensajes.
El enlace es el conjunto de módems u otro equipo de interfaces y circuitos de comunicaciones que conectan a dos o más terminales que desean comunicarse entre sí, entonces el protocolo de enlace son las reglas que deben seguir estos equipos para lograr la transferencia de datos entre ellos. Generalmente, las computadoras no están capacitadas para transmitir y recibir datos de una red de larga distancia, y para esto existen los módems u otros circuitos de conexión, a las terminales o computadoras se les llama DTE y a los circuitos de conexión (por ejemplo los módems) con la red se les llama DCE. Los DCE se encargan de transmitir y recibir bits uno a uno. Los DTE y DCE están comunicados y se pasan tanto datos de información como de control. Para que se puedan comunicar dos DTE hace falta que ambos cooperen y se entiendan con sus respectivos DCE. También es necesario que los dos DCE se entiendan y usen los mismos protocolos.

4.7.1 Métodos de Comunicación en los Protocolos de Enlace

Comunicación Símplex

Una comunicación es símplex si están perfectamente definidas las funciones del emisor y del receptor y la transmisión de los datos siempre se efectúa en una dirección. La transmisión de señales por medio de la televisión es el ejemplo más claro de comunicación símplex.

Comunicación Semidúplex

En la transmisión semidúplex cada vez sólo una de las dos estaciones del enlace punto a punto puede transmitir. Este modo también se denomina "alterno en dos sentidos", ya que las dos estaciones deben transmitir alternativamente. Esto es comparable a un puente con un sólo carril con circulación en los dos sentidos. Este tipo de transmisión se usa a menudo en la interacción entre los terminales y el servidor central. Mientras que el usuario introduce y transmite datos, la computadora receptora esta impedida para enviar datos a la terminal emisora. Este tipo de comunicación puede ser bidireccional, esto quiere decir que el emisor y receptor pueden intercambiarse los papeles. Sin embargo, la bidireccionalidad no puede ser simultánea. Cuando el emisor transmite, el receptor necesariamente recibe y puede ocurrir lo contrario siempre y cuando el antiguo emisor se convierta en el nuevo receptor.

Comunicación Dúplex o Full-dúplex

En este tipo de comunicación es bidireccional y simultánea. En la transmisión full-duplex las dos estaciones pueden simultáneamente enviar y recibir datos. Este modo se denomina simultáneo en dos sentidos y es comparable a un puente con dos carriles con tráfico en ambos sentidos.
El Teléfono es un buen ejemplo de comunicación dúplex ya que en esta comunicación el emisor y el receptor no están perfectamente definidos. Ambos actúan como emisor y como receptor indistintamente. En una comunicación dúplex se dice que hay un canal físico y dos canales lógicos, y para el intercambio de datos entre computadoras, este tipo de transmisión es más eficiente que la transmisión semidúplex.
En las transmisiones de señales analógicas, para hacer la comunicación full-dúplex, es necesaria la utilización de dos frecuencias o dos cables de conexión en el caso de que se quiera usar la misma frecuencia para transmitir y recibir los datos.

4.7.2 Protocolo de Enlace IBM 3780

El protocolo de enlace IBM 3780 es un protocolo semidúplex de contención y este tipo de enlaces se utiliza generalmente en enlaces síncronos punto a punto para comunicar las siguientes configuraciones de dispositivos:

a) Computadora a computadora.

b) Computadora a servidor.

c) Servidor a servidor.

Con un protocolo de contención el enlace permanece activo solo cuando hay transferencia de datos a diferencia del protocolo tipo encuesta y selección, donde el enlace de comunicaciones siempre está activo debido al proceso continuo de encuesta de fondo. Cuando el enlace en el que funciona un protocolo de contención queda inactivo, el dispositivo de comunicación de cada uno de los extremos, puede realizar una petición de uso del enlace para enviar datos: SYN SYN SYN SYN ENQ y espera confirmación SYN SYN SYN SYN ACK por parte del otro extremo.

Ya puede comenzar la transferencia de datos. Si el dispositivo no recibe la confirmación durante un cierto tiempo, (llamado "time-out"), vuelve a realizar la petición. Si sucede que los dispositivos conectados al mismo enlace simultáneamente se realizan "peticiones", entonces ambos dispositivos ignorarán la petición del otro pues con un protocolo semidúplex un dispositivo está o enviando o recibiendo pero no ambas cosas a la vez. Para superar este problema, los dispositivos de cada lado del enlace de comunicaciones tienen diferentes periodos de "time-out", de manera que en el caso de dos "peticiones" simultáneas, uno de los dispositivos ganará eventualmente el enlace. Un dispositivo cuya "petición" haya sido confirmada comenzará a enviar sus datos en bloques, cada uno de los cuales será individualmente confirmado (positivamente con ACK) o confirmado negativamente (con NAK) por el dispositivo receptor. Los bloques confirmados negativamente serán retransmitidos por el extremo emisor.

El carácter de control utilizado para acabar la sección de datos de un bloque transmitido suele ser ETB excepto en el caso del bloque de datos final, donde normalmente se utiliza ETX. Una vez que un dispositivo emisor ha enviado todos sus bloques de datos envía una secuencia de "final de transmisión" (SYN,SYN,SYN,SYN,EOT). Entonces el enlace de comunicaciones pasa a inactivo, y si el dispositivo que previamente era receptor, dispone de datos para enviar, realiza una petición de uso del enlace.

4.6.3 Protocolo de Enlace BSC

El protocolo de enlace de comunicación síncrona binaria BSC por sus siglas en Inglés (Binary Synchronous Communications) fue desarrollado por IBM a mediados de la década de los 60's y fue utilizado en la mayoría de las transmisiones de datos de aquella época. El BSC define un conjunto de reglas para la transmisión síncrona de datos codificados en forma binaria, y aun actualmente este realiza la comunicación entre diversos medios y equipos de comunicación. El BSC transmite la información en block de datos y realiza estas comunicaciones en modo semidúplex. Aún y cuando el BSC fue originalmente diseñado para enlaces de punto a punto posteriormente este fue modificado para proveer una gran variedad de otras funciones. Estas alteraciones resultaron en un número de diferentes Releases de BSC.

En la transmisión síncrona binaria los datos, datos de control de caracteres y otros caracteres son transmitidos juntos en series continuas, y por lo mismo no son requeridos bits extra con cada carácter para sincronizar la transmisión, ya que la sincronización se logra mandando un carácter específico llamado patrón de sincronía (SYN). El BSC es capaz de proveer un rango mayor de velocidades que los protocolos de enlace asíncronos, trabaja una línea mayor de utilización, esta mucho mejor definido que los protocolos de enlace de transmisión asíncrona y provoca menos perdidas al realizar la transmisión. Al mismo tiempo este protocolo se puede utilizar con tres tipos diferentes de datos (SBT, EBCDIC, y ASCII) en los cuales los cuales los códigos se diferencian en el número de bits codificados por símbolo o carácter (6 en el SBT, 7 en el ASCII, y 8 en el EBCDIC) y el número de caracteres es también diferente en los juegos de información de los diferentes tipos de datos ((64 en SBT, 128 en ASCII y 144 en EBCDIC). En el BSC se utilizan varios tipos de caracteres de control de enlace para aumentar el control de enlace de datos y asegurar que ocurran las acciones apropiadas. Entre los caracteres de control de enlace están: SYN, SOH, STX, EBT, ETX, DEL, TTD, EOT, ENQ, ACKO o ACKI, WACK, NAK. Algunos de estos caracteres de control requieren una sucesión de dos caracteres normalizados, ASCII y EBCDIC. Actualmente debido a todas las ventajas que este representa, el BSC es uno de los protocolos de enlace más difundidos y populares para realizar las comunicaciones entre redes y/o computadoras.

4.7.4 Protocolo de Enlace HDLC

El protocolo de enlace "Control de alto nivel de Enlace de Datos" conocido como HDLC por sus siglas en Inglés (High Data Level Control) proviene de un protocolo creado por la IBM originalmente llamado SDLC y de una modificación de la ISO a este con el fin de hacerlo de uso internacionalmente. Este protocolo esta basado en el principio de la orientación a bit y utiliza la inserción de bits para la transparencia de datos.
Los protocolos orientados a bit utilizan la estructura de trama que se muestra en la siguiente figura.

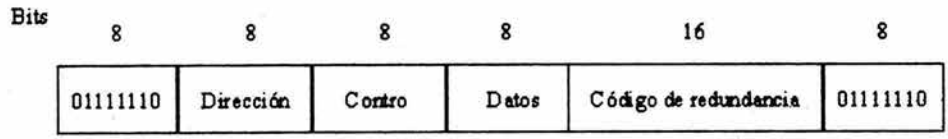


Figura 4.12 Formato de la trama para un protocolo HDLC

El Campo Dirección es fundamentalmente importante en las transferencias de datos tipo multipunto en donde se emplea para identificar cada una de las terminales. En las transferencias de datos punto a punto este campo algunas veces se utiliza para distinguir los comandos de las respuestas.

El Campo Control de utiliza para los números de secuencia asentamientos y otros propósitos que mencionaremos un poco más adelante.

El Campo Datos contiene la información principal a transmitir y puede ser arbitrariamente largo, aunque la eficiencia del código de redundancia decrecerá a medida que se aumenta la longitud de la trama, debido a la posibilidad de tener múltiples errores de grupo.

El Campo Código de redundancia es una variante mínima del código de redundancia cíclica, en donde el motivo de la variación consiste en permitir que se detecten los octetos de las banderas.
La trama esta delimitada con otra secuencia de bandera (01111110). En líneas punto a punto inactivas, las secuencias de bandera se transmiten continuamente tal y como sucede con los caracteres SYN que, por lo general se transmiten durante periodos de inactividad, cuando se utilizan BYSSYNC. La trama mínima esta formada por 3 campos y totaliza 32 bits, excluyendo las banderas localizada en ambos extremos.
En este protocolo existen 3 tipos de tramas: información, supervisoras y sin enumerar en la siguiente figura se muestra el contenido del campo control para estos tres tipos.
Este protocolo utiliza una ventana deslizante con un número de secuencia de 3 bits y en cualquier instante pueda haber hasta siete tramas pendientes de ser transmitidas el campo Sec (ver figura anterior) contiene él número de secuencia de la trama. El campo siguiente es un asentamiento superpuesto.

Generalmente este protocolo usa la convención, de la trama por recibir. Aún así, es conveniente mencionar que la elección de esta convención es arbitraria, es decir, no importa si se utiliza la convención de la trama por recibir o la de la última trama procesada, siempre y cuando se haga en forma consistente.

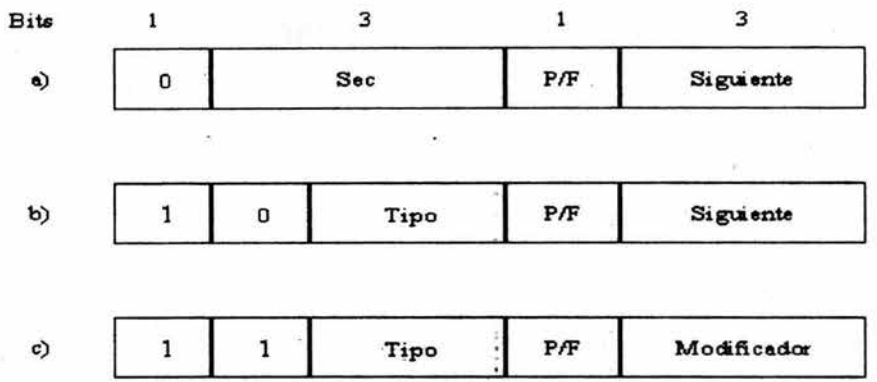


Figura 4.13 Campo de control a) trama de información, b) trama supervisora, c) trama sin enumerar.

Este protocolo utiliza una ventana deslizante con un número de secuencia de 3 bits y en cualquier instante pueda haber hasta siete tramas pendientes de ser transmitidas el campo Sec (ver figura anterior) contiene el número de secuencia de la trama. El campo siguiente es un asentamiento superpuesto.
Generalmente este protocolo usa la convención, de la trama por recibir. Aun así, es conveniente mencionar que la elección de esta convención es arbitraria, es decir, no importa si se utiliza la convención de la trama por recibir o la de la ultima trama procesada, siempre y cuando se haga en forma consistente.
Número, Cuando se usa P, se quiere indicar que la computadora esta invitando a la terminal para que le envíe datos. Todas las tramas que envía la terminal, con excepción de la última, tienen el bit P/F puesto en al valor P, y el de la última trama llevará un valor d.

4.8 CONJUNTOS DE PROTOCOLOS TCP/IP

El TCP/IP (Transfer Control Protocol / Internet Protocol) es un grupo de protocolos estándares de la industria diseñados para grandes redes que incluyen los enlaces de las redes de área amplia (wide area network, WAN). El TCP/IP fue desarrollado en 1969 por la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de los Estados Unidos (Department of Defense Advanced Research Projects Agency, DARPA), el resultado de un experimento para compartir recursos llamado la Red de la Agencia de Proyectos de Investigación Avanzada (Advanced Research Projects Agency Network, ARPANET). El propósito del TCP/IP fue proporcionar enlaces de redes para comunicación de alta velocidad.

4.8.1 Ventajas de los Protocolos TCP/IP

Algunas de las ventajas de este protocolo son:

a) Un protocolo de red empresarial enrutable, estándar que es uno de los protocolos más completos y aceptados disponible. Todos los sistemas operativos de redes modernos ofrecen soporte para el TCP/IP, y la mayoría de las grandes redes utilizan el TCP/IP para la mayoría de su tráfico de red.

b) Una tecnología para conectar sistemas disímiles. Muchas utilidades de conectividad estándar están disponibles para accesar y transferir datos entre sistemas diferentes, incluyendo el Protocolo de Transferencia de Archivos (File Transfer Protocol, FTP) y de Telnet, un protocolo de emulación de terminal.

c) Un marco cliente-servidor, multiplataforma, escalable y robusto. El TCP/IP ofrece interfases de sockets, las cuales son ideales para desarrollar aplicaciones cliente servidor que pueden ejecutarse sobre las pilas que sean compatibles inter - compañías.

d) Un método para tener acceso a Internet. Internet consiste de miles de redes mundiales que conectan instalaciones de investigación, universidades, bibliotecas y compañías privadas

4.8.2 Los Estándares TCP/IP

Los estándares para TCP/IP están publicados en una serie de documentos llamados Request for Comments (RFCs). Los RFCs describen el funcionamiento interno de Internet. Algunos RFCs describen los servicios de red o protocolos y su implementación, mientras otros resumen políticas. Los estándares TCP/IP son siempre publicados como RFCs, aunque no todos los RFCs especifican estándares. Los estándares TCP/IP no son desarrollados por un comité, sino por consenso. Cualquiera puede enviar un documento para su publicación como un RFCs. Los documentos son revisados por un experto técnico, una fuerza de trabajo, o un editor de RFCs y se les asigna un estado. El estado especifica si un documento está siendo considerado como un estándar.

Existen cinco estados asignables para los RFCs tal como se describe en la siguiente tabla.

Estado	Descripción
Requerido	Debe estar implementado en todos los servidores y pasarelas TCP/IP.
Recomendado	Se recomienda que se implemente el RFC en todos los servidores y pasarelas TCP/IP. Los RFCs recomendados generalmente son implementados.
Electivo	La implementación es opcional. Su aplicación ha sido aceptada pero no es un requerimiento.
Uso limitado	No va dirigido al uso general.
No recomendado	No se recomienda su implementación.

Tabla 4.2 Asignaciones de estado para los RFCs

Sí un documento está siendo considerado como un estándar, pasa a través de fases de desarrollo, prueba y aceptación conocidas como el Proceso de Estándares de Internet. Estas fases son formalmente etiquetadas como niveles de madurez. La tabla 4.3 lista los tres niveles de madurez para los Estándares de Internet.

Niveles de madurez	Descripción
Propuesta de estándar	Una especificación de propuesta de estándar es generalmente estable, ha resuelto decisiones de diseño conocidas, y se cree que está bien comprendida, ha recibido revisión importante de la comunidad y parece disfrutar suficiente interés de la comunidad para ser considerada valiosa.
Borrador de Estándar	Un borrador de estándar debe estar bien comprendido y se debe conocer que es muy estable, tanto en su semántica como en que pueda ser una base para el desarrollo de una implementación.
Estándar de Internet	La especificación de estándar de Internet (que puede simplemente ser referida como un Estándar) está caracterizada por un alto grado de madurez técnica y por la creencia generalizada de que el servicio o protocolo especificado proporciona algún beneficio importante a la comunidad de Internet.

Tabla 4.3 Niveles de madurez para los Estándares de Internet.

Cuando un documento es publicado se le asigna un número de RFC. El RFC original nunca es actualizado. Si se requieren cambios, se publica un nuevo RFC con un nuevo número. Por lo tanto es importante verificar constantemente el RFC más reciente de un tema en particular.
Los RFCs pueden ser obtenidos de varias formas. La manera más simple de obtener un RFC o un listado indexado completo y actualizado de todos los RFCs publicados es revisar http://www.rfc-editor.org/rfc.html en la Web

4.8.3 La arquitectura del protocolo TCP/IP.

Los protocolos TCP/IP mapean un modelo conceptual de cuatro capas conocido como el modelo DARPA, denominado así por la agencia del gobierno de los Estados Unidos que inicialmente desarrolló TCP/IP. Las cuatro capas en el modelo DARPA corresponden a una o más capas del modelo de siete capas del modelo OSI.

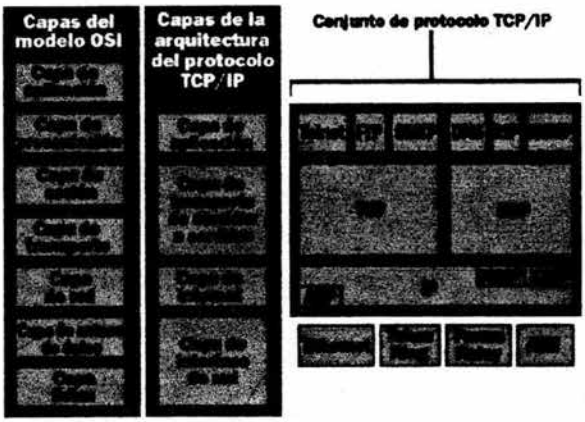


Figura 4.14 Arquitectura del protocolo TCP/IP.

Capa de Interfase de Red.

La capa de interfase de red (también llamada la capa de acceso de red) es responsable de colocar los paquetes TCP/IP en el medio de la red y de recibir los paquetes TCP/IP del medio de la red. El TCP/IP fue diseñado para ser independiente del método de acceso a la red, del formato del cuadro (frame) y del medio. De este modo, el TCP/IP puede ser utilizado para conectar diferentes tipos de red. Esto incluye tecnologías de LAN, tales como Ethernet o Token Ring y tecnologías de WAN tales como X.25 o Frame Relay. La independencia de cualquier tecnología de red específica le da al TCP/IP la habilidad de ser adaptado a las nuevas tecnologías tales como Asynchronous Transfer Mode (ATM). La capa de interfase de red comprende a las capas de enlace datos y física del modelo OSI. Hay que notar que la capa de Internet no aprovecha los servicios de secuenciación y la confirmación que pudieran estar presentes en la capa de enlace de datos. Se asume una capa de interfase de red no confiable, y la comunicación confiable es responsabilidad de la capa de transporte, a través del establecimiento de la sesión y la confirmación de paquetes.

Capa de Internet.

La capa de Internet es responsable de las funciones de direccionamiento, empaque y enrutamiento. Los protocolos base de la capa de Internet son el IP, ICMP y IGMP.

a) El Protocolo de Internet (Internet Protocol, IP) es un protocolo enrutable responsable del direccionamiento IP y de la fragmentación y ensamble de los paquetes.

b) El Protocolo de Conversión de Dirección (Address Resolution Protocol, ARP) es responsable de la conversión de las direcciones de la capa de Internet a las direcciones de la capa de la interfase de red, tales como las direcciones de hardware.

c) El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol, ICMP) es responsable de proporcionar funciones de diagnóstico y de reporte de errores o de condiciones referentes a la entrega de los paquetes IP.

d) El Protocolo de Administración de Grupo de internet (Internet Group Management Protocol, IGMP) es responsable de la administración de los grupos IP multicast.

La capa de Internet es análoga a la capa de red del modelo OSI.

Capa de Transporte.

La capa de transporte (también conocida como la capa de transporte de servidor a servidor) es responsable de proporcional a la capa de aplicación los servicios de comunicación de sesión y datagrama. Los protocolos base de la capa de transporte son el TCP y el Protocolo de Datagramas de Usuario (User Datagram Protocol, UDP).

a) El TCP proporciona un servicio de comunicación confiable, orientado a conexión, uno a uno. El TCP es responsable del establecimiento de una conexión TCP, la secuenciación y la confirmación de los paquetes enviados, y de la recuperación de los paquetes perdidos durante la transmisión.

b) El UDP proporciona servicios de comunicación no confiables, uno a uno o de uno a muchos, sin conexión. El UDP es utilizado cuando la cantidad de datos a ser transferidos es pequeña (tales como datos que pueden caber dentro de un paquete único), cuando la carga de establecer la conexión no es deseable o cuando la aplicación o los protocolos de capas superiores proporcionan una entrega confiable.
La capa de transporte comprende las responsabilidades de la capa de transporte OSI y algunas de las responsabilidades de la capa de sesión OSI.

Capa de Aplicación.

La capa de aplicación proporciona la habilidad de accesar los servicios de otras capas y define los protocolos que las aplicaciones utilizan para intercambiar datos. Hay varios protocolos para la capa de aplicación y constantemente se están desarrollando nuevos protocolos.
Los protocolos de la capa de aplicación más ampliamente conocidos son aquellos usados para el intercambio de información del usuario:

a) El Protocolo de Transferencia de Hipertexto (HyperText Transfer Protocol, HTTP) es utilizado para transferir los archivos que componen las páginas de la Web.

b) El Protocolo de Transferencia de Archivos (File Transfer Protocol, FTP) es utilizado para la transferencia interactiva de archivos.

c) El Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol, SMTP) es utilizado para la transferencia de mensajes de correo y anexos.

d) El Telnet, un protocolo de emulación de terminal, es utilizado para el inicio de sesiones remotas en servidores de red.

Adicionalmente, los siguientes protocolos ayudan a facilitar el uso y la administración de redes TCP/IP:

a) El Sistema de Nombre de Dominio (Domain Name System, DNS) es utilizado para convertir un nombre de servidor en una dirección IP.

b) El Protocolo de Información de Enrutamiento (Routing Information Protocol, RIP) es un protocolo de enrutamiento que los ruteadores utilizan para intercambiar información de enrutamiento en una red IP.

c) El Protocolo Simple de Administración de Red (Simple Network Management Protocol, SNMP) es utilizado entre la consola de administración de red y los dispositivos de la red (ruteadores, puentes y concentradores inteligentes) para colectar e intercambiar información de administración de la red.

Ejemplos de interfases de la capa de aplicación para aplicaciones TCP/IP son Windows Sockets y NetBIOS. Windows Sockets proporciona una interfase de programación para aplicaciones (API) estándar bajo el sistema operativo Microsoft Windows.

4.8.4 Los Protocolos Bases del TCP/IP

El componente del protocolo TCP/IP que está instalado en su sistema operativo es una serie de protocolos interconectados llamados los protocolos base del TCP/IP. Todas las demás aplicaciones y demás protocolos en el grupo de protocolos TCP/IP se apoyan en los servicios básicos proporcionados por los siguientes protocolos: IP, ARP, ICMP, IGMP, TCP, y UDP.

El IP

El IP es un protocolo de datagramas no confiable, sin conexión y principalmente responsable del direccionamiento y enrutamiento de los paquetes entre servidores. Sin conexión significa que una sesión no se establece antes de intercambiar los datos. No confiable significa que la entrega no está garantizada. Un paquete IP podría perderse, entregarse fuera de secuencia, duplicado o retrasado. El IP no intenta recuperarse de este tipo de errores. La confirmación de la entrega de los paquetes y la recuperación de paquetes perdidos es responsabilidad de un protocolo de alguna capa superior, tal como el TCP.

Campos de la cabecera IP	Función
Dirección IP origen	La dirección IP de la fuente original del datagrama IP.
Dirección IP destino	La dirección IP del destino final del datagrama IP.
Identificación	Utilizado para identificar a un datagrama IP específico y para identificar todos los fragmentos de un datagrama IP específico si ocurriera la fragmentación.
Protocolo	Informa al IP en el servidor destino si tiene que pasar el paquete al TCP, UDP, ICMP u otros protocolos.
Suma de verificación	Un simple cálculo matemático utilizado para verificar la integridad de la cabecera IP.
Tiempo de vida (Time to Live, TTL)	Contiene el número de redes en las cuales el datagrama es permitido viajar antes de ser descartado por un ruteador. El TTL es establecido por el servidor que envía y es utilizado para prevenir que los paquetes circulen infinitamente en una red IP. Cuando se redirecciona un paquete IP, a los ruteadores se les requiere que disminuyan el TTL o al menos uno.

Tabla 4.4 Campos clave en la cabecera IP.

Sí un ruteador recibe un paquete IP que es demasiado grande para la red a la cual el paquete será redireccionado, el IP fragmentará el paquete original en paquetes más pequeños que cabrán en la red. Cuando los paquetes lleguen a su destino final, el IP en el servidor destino ensamblará los fragmentos a su carga original. Este proceso es denominado fragmentación y ensamblado.

La fragmentación puede ocurrir en ambientes que tienen una mezcla de tecnologías de red, tales como Ethernet y Token Ring.

La fragmentación y ensamblado funcionan como sigue:

a). Cuando un paquete IP es enviado por el origen, pone un valor único en el campo Identificación.

b). El paquete IP es recibido en el ruteador. El ruteador IP nota que la unidad de transmisión máxima (maximum transmission unit, MTU) de la red a la cual el paquete será redireccionado es más pequeña que el tamaño del paquete IP.

c). El IP fragmenta la carga original en fragmentos que cabrán en la siguiente red. Cada fragmento es enviado por su propia cabecera IP la cual contiene:

- El campo Identificación original que identifica todos los fragmentos que van juntos.
- La bandera Más Fragmentos (More Fragments) indica que otros fragmentos siguen. La bandera Más Fragmentos no es establecido en el último fragmento, porque no le siguen otros fragmentos.
- El campo Desplazamiento de Fragmento (Fragment Offset) indica la posición del fragmento relativa a la carga IP original.

d). Cuando los fragmentos son recibidos por el IP en el servidor remoto, son identificados por el campo Identificación como pertenecientes a uno mismo. Entonces el Desplazamiento de Fragmento es utilizado para ensamblar los fragmentos en la carga IP original.

El ARP

Cuando los paquetes IP son enviados sobre tecnologías de redes de acceso compartido, de transmisión amplia (broadcast-based), tales como Ethernet o Token Ring, la dirección de Control de Acceso de Medios (Media Access Control, MAC) correspondiente a una dirección IP de redireccionamiento debe ser convertida. El ARP utiliza las transmisiones a nivel de MAC para convertir una dirección IP de redireccionamiento conocida a su dirección MAC. El ARP está definido en el RFC 826.

El ICMP

El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol, ICMP) proporciona servicios de resolución de problemas y de reporte de errores para los paquetes que no son entregables. Por ejemplo, si el IP es incapaz de entregar un paquete al servidor destino, el ICMP enviará un mensaje de Destino Inalcanzable (Destination Unreachable) al servidor origen

La siguiente tabla nos muestra los mensajes ICMP más comunes.

Mensaje ICMP	Función
Echo Request	Mensaje simple para resolución de problemas utilizado para revisar la conectividad IP hacia un servidor deseado.
Echo Reply	Respuesta a un Echo Request del ICMP.
Redirect	Enviado por un ruteador para informar a un servidor que envía de una mejor ruta hacia la dirección IP destino.
Source Quench	Enviada por un ruteador para informar a un servidor que envía que sus datagramas IP están siendo descartadas debido a la congestión en el ruteador. El servidor que envía, entonces disminuye su velocidad de transmisión. Source Quench es un mensaje ICMP electivo y frecuentemente no es implementado.
Destination Unreachable	Enviado por un ruteador o por el servidor destino para informar al servidor que envía que el datagrama no puede ser entregado.

Tabla 4.5. Mensajes ICMP comunes.

Para enviar mensajes Echo Request del ICMP y ver las estadísticas de las respuestas en una computadora es necesario utilizar la utilidad ping en la interfase de comandos de la PC.
Hay una serie de mensajes Destination Unreachable del ICMP. La siguiente tabla describe los mensajes Destination Unreachable del ICMP más comunes.

Mensajes Destination Unreachable	Descripción
Network Unreachable	Enviado por un ruteador IP cuando una ruta a la red destino no pudo ser encontrada.
Host Unreachable	Enviado por un ruteador IP cuando un servidor destino en la red destino no puede ser encontrado. Este mensaje solamente es utilizado con tecnologías de red orientadas a conexiones (enlaces WAN). Los ruteadores IP con tecnologías de red sin conexión (tales como Ethernet y Token Ring) no envían mensajes Host Unreachable.
Protocol Unreachable	Enviado por el nodo IP destino cuando el campo Protocolo en la cabecera IP no pude ser apareado con un protocolo del cliente IP a actualmente cargado.
Port Unreachable	Enviado por un nodo IP destino cuando el Puerto Destino (Destination Port) en la cabecera IP no puede ser apareado con un proceso que utilice ese puerto.
Fragmentation Needed and DF Set	Enviado por un ruteador IP cuando la fragmentación debe de ocurrir pero no es permitida debido a que el valor de la bandera No Fragmentar (Don't Fragment, DF) en la cabecera IP fue activada por el nodo origen.

Tabla 4.6 Mensajes Destination Unreachable del ICMP comunes.

El ICMP no hace al IP un protocolo confiable. El ICMP intenta reportar los errores y proporcionar retroalimentación sobre condiciones específicas. Los mensajes ICMP son llevados como datagramas IP no confirmados y son por sí mismos no confiables. El ICMP está definido en el RFC 792.

El IGMP.

El Protocolo de Administración de Grupos de Internet (Internet Group Management Protocol, IGMP) es un protocolo que administra la membresía de los servidores en los grupos IP multicast. Un grupo IP multicast, también conocido como un grupo de servidores (host group), es un conjunto de servidores que escuchan el tráfico IP destinado a una dirección IP multicast específica. El tráfico IP multicast es enviado a una sola dirección MAC pero es procesado por múltiples servidores IP. Un servidor dado escucha en una dirección IP multicast específica y recibe todos los paquetes de esa dirección IP. Algunos aspectos adicionales de la transmisión IP multicast (IP multicasting):

a). La membresía del grupo de servidores es dinámica, los servidores pueden unirse y abandonar al grupo en cualquier momento.

b). Un grupo de servidores puede ser de cualquier tamaño.

c). Los miembros de un grupo de servidores pueden SPAN ruteadores IP a lo largo de múltiples redes. Esta situación requiere el soporte de IP multicast en los ruteadores IP y la habilidad de los servidores para registrar su membresía de grupo con los ruteadores locales. El registro del servidor se logra usando el IGMP.

d). Un servidor puede enviar tráfico a una dirección IP multicast sin pertenecer al grupo de servidores correspondientes.
Para que un servidor reciba transmisiones IP multicast, una aplicación debe informar al IP que estará recibiendo transmisiones multicast en una dirección IP multicast destino. Si la tecnología de red soporta la transmisión multicast basada en el hardware, entonces a la interfase de red se le indica que pase los paquetes para una dirección multicast específica. En el caso de Ethernet, la tarjeta de interfase de red es programada para responder a una dirección MAC multicast correspondiente a la dirección IP multicast deseada.
Un servidor soporta IP multicast en uno de los siguientes niveles:

a). Nivel 0. Sin soporte para enviar o recibir tráfico IP multicast.

b). Nivel 1.Con soporte para enviar pero no para recibir tráfico IP multicast.

c). Nivel 2. Con soporte para enviar y recibir tráfico IP multicast.
El TCP/IP soporta el nivel 2 de transmisión de IP multicast.
El protocolo para registrar la información del grupo de servidores es IGMP. El IGMP es requerido en todos los servidores que soportan el nivel 2 de la transmisión IP multicast. Los paquetes IGMP son enviados utilizando una cabecera IP.

Los mensajes IGMP toman dos formas:
Cuando un servidor se une a un grupo de servidores, envía un mensaje de Reporte de Membresía de Servidor (Host Membership Report) a la dirección IP multicast para todos los servidores (224.0.0.1) o a la dirección multicast deseada declarando su membresía en un grupo de servidores específico haciendo referencia a la dirección IP multicast. Cuando un ruteador revisa la red para asegurarse de que hay miembros de un grupo de servidores específico, envía un mensaje de Petición de Membresía de Servidor (Host Membership Query) a la dirección IP multicast para todos los servidores. Si no se reciben respuestas a la petición después de varios intentos, el ruteador supone que no hay membresías en ese grupo para esa red y deja de anunciar la información de red de ese grupo a los otros ruteadores.

Para que la transmisión de IP multicast incluya ruteadores a lo largo de una red los ruteadores utilizan protocolos de enrutamiento multicast para comunicar la información del grupo de servidores de tal manera que cada ruteador que soporte el redireccionamiento multicast se de cuenta de qué redes contienen miembros para cuál grupo de servidores.

El TCP.

El TCP es un servicio de entrega confiable, orientado a conexiones. Los datos son transmitidos en segmentos. Orientado a conexiones significa que una conexión debe establecerse antes de que el servidor intercambie datos. La confiabilidad es lograda asignando un número de secuencia a cada segmento transmitido. Se utiliza una confirmación para verificar que los datos fueron recibidos por el otro servidor. Para cada segmento enviado, el servidor que recibe debe regresar una confirmación (acknowledgment, ACK) dentro de un periodo específico de bytes recibidos. Si una ACK no es recibida, los datos son retransmitidos.

El TCP utiliza comunicaciones de flujo de bytes (byte-stream), donde los datos dentro del segmento TCP son tratados como una secuencia de bytes sin límites de registro o de campo. La tabla 4.7 describe los campos claves en la cabecera TCP.

Campo	Función
Puerto origen	El puerto TCP del servidor que envía.
Puerto destino	El puerto TCP del servidor destino.
Número de secuencia	El número de secuencia del primer byte de datos en el segmento TCP.
Número de confirmación	El número de secuencia del byte que el que envía espera recibir del otro lado de la conexión.
Ventana	El tamaño actual de la memoria intermedia TCP en el servidor que envía este segmento TCP para almacenar segmentos que llegan.
Suma de verificación TCP	Verifica la integridad de la cabecera TCP y de los datos TCP.

Tabla 4.7 Campos clave en la cabecera TCP

4.8.5 Puertos TCP

Un puerto TCP proporciona una localización específica para entregar los segmentos TCP. Los números de puertos por debajo de 1024 son puertos bien conocidos y están asignados por la Autoridad de Número Asignados de Internet (Internet Assigned Numbers Authority, IANA).

Número de puerto TCP	Descripción
20	FTP (Canal de datos).
21	FTP (Canal de control).
23	Telnet.
80	Protocolo de Transferencia de Hipertexto (HyperText Transfer Protocol, HTTP) utilizado para la Web.
139	Servicios de sesión NetBIOS.

Tabla 4.8 Puertos TCP bien conocidos

4.8.6 La negociación de tres vías (Three-Way Handshake)

Una conexión TCP es inicializada a través de un intercambio de tres vías. El propósito del intercambio de tres vías es sincronizar el número de secuencia y los números de confirmación de ambos lados de la conexión, intercambiar los tamaños de ventana TCP e intercambiar otras opciones TCP tales como el tamaño máximo de segmento. Los siguientes pasos delinean el proceso:

a). El cliente envía un segmento TCP al servidor con un número de secuencia inicial para la conexión y un tamaño de ventana indicando el tamaño de la memoria intermedia en el cliente para almacenar los segmentos que lleguen del servidor.

b). El servidor envía de regreso un segmento TCP conteniendo su número de secuencia inicial elegido; una confirmación del número de secuencia del cliente y un tamaño de ventana indicando el tamaño de la memoria intermedia en el servidor para almacenar los segmentos que lleguen del cliente.

c). El cliente envía un segmento TCP al servidor conteniendo una confirmación del Número de Secuencia del servidor.
El TCP utiliza un proceso de intercambio similar para terminar una conexión. Esto garantiza que ambos servidores hayan terminado de transmitir que todos los datos hayan sido recibidos.

4.8.7 El UDP.

El UDP proporciona un servicio de datagrama sin conexión que ofrece entrega no confiable, de mejor esfuerzo de los datos transmitidos en los mensajes. Esto significa que la llegada de los datagramas no está garantizada; ni que la entrega de los paquetes esté en la secuencia correcta. El UDP no se recupera de la pérdida de datos utilizando retransmisión.
El UDP es utilizado por aplicaciones que no requieren confirmación de la recepción de los datos y que típicamente transmiten pequeñas cantidades de datos en un momento dado. El servicio de nombres de NetBIOS, el servicio de datagramas de NetBIOS y el Protocolo Simple de Administración de Redes (Simple Network Management Protocolo, SNMP) son ejemplos de servicios y aplicaciones que utilizan el UDP. La tabla 4.9 describe los campos clave en la cabecera UDP.

Campo	Función
Puerto origen	Puerto UDP del servidor que envía.
Puerto destino	Puerto UDP del servidor destino.
Suma de verificación UDP	Verifica la integridad de la cabecera UDP y de los datos UDP.
Número de confirmación	El número de secuencia del byte que el que envía espera recibir del otro lado de la conexión.

Tabla 4.9 Campos claves en la cabecera UDP.

Puertos UDP

Para usar el UDP, una aplicación debe proporcionar la dirección IP y el número de puerto UDP de la aplicación destino. Un puerto proporciona una localización para los mensajes que se envían. Un puerto funciona como una cola de mensajes multiplexada, significando que puede recibir múltiples mensajes a la vez. Cada puerto está identificado por un número único.

Es importante notar que los puertos UDP son distintos y separados de los puertos TCP, incluso aunque algunos de ellos usen el mismo número. La tabla 4.10 lista algunos puertos UDP mas conocidos.

Número de puerto UDP	Descripción
53	Petición de nombre para el Sistema de Nombres de Dominio (Domain Name System, DNS).
69	Protocolo Trivial de Transferencia de Archivos (File Transfer Protocol, TFTP).
137	Servicios de nombres NetBIOS.
138	Servicio de datagrama NetBIOS.
161	Protocolo Simple de Administración de Redes (Simple Network Management Protocol, SNMP).

Tabla 4.10 Puertos UDP más conocidos.

4.8.8 Interfaces de programación de aplicación (APIs)

Para permitir a las aplicaciones accesar a los servicios ofrecidos por los protocolos bases del TCP/IP de una manera estándar, los sistemas operativos de redes como Windows NT hacen disponible interfases de programación de aplicaciones (application programming interfaces, APIs) estándares de la industria. Las interfases de programación de aplicaciones son conjuntos de funciones y comandos que son llamados programáticamente por el código de la aplicación para ejecutar funciones de red. Por ejemplo, una aplicación navegadora de Web que se conecta a un sitio Web necesita acceso al servicio de establecimiento de conexión del TCP.
La siguiente nos muestra dos interfases de conexión TCP/IP comunes, Windows Sockets y NetBIOS, y su relación con los protocolos bases.

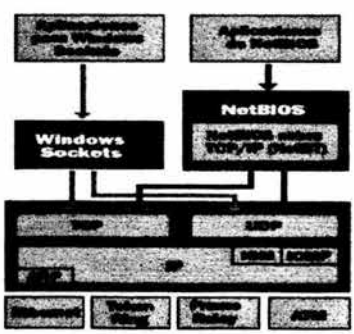


Figura 4.15 Interfases de Aplicación para TCP/IP.

4.9 DIRECCIONAMIENTO IP

Cada servidor TCP/IP está identificado por una dirección IP lógica. La dirección IP es una dirección de la capa de red y no tiene dependencia sobre la dirección de la capa de enlace de datos (tal como una dirección MAC de una tarjeta de interfase de red). Una dirección IP única es necesaria para cada servidor y componente de red que se comunique usando TCP/IP.
La dirección IP identifica una localización del sistema en la red de la misma manera en que una dirección de postal identifica una casa en la cuadra de una ciudad. Tal como una dirección postal identifica una residencia única, una dirección IP globalmente única y debe tener un formato uniforme.

4.9.1 Direcciones IP

Cada dirección IP incluye un identificador de red y un identificador de servidor.

Identificador de Red

El identificador de red (también conocido como dirección de red) identifica los sistemas que están localizados en la misma red física rodeados por ruteadores IP. Todos los sistemas en la misma red física deben tener el mismo identificador de red. El identificador de red debe ser único en la red global.

Identificador de Servidor

El identificador de servidor (también conocido como dirección de servidor) identifica una estación de trabajo, servidor, ruteador u otro dispositivo TCP/IP dentro de una red. La dirección de cada servidor debe ser única al identificador de red.
Una dirección IP tiene 32 bits de longitud. En lugar de trabajar con 32 bits a la vez, es una práctica común segmentar los 32 bits de la dirección IP en cuatro campos de 8 bits llamados octetos. Cada octeto es convertido a un número decimal (al sistema de numeración de base 10) en el rango de 0 a 255 y separados por un punto. Este formato es llamado notación decimal punteada.

Formato Binario	Formato decimal punteado
11000000 10101000 00000011 00011000	192.168.3.24

Tabla 4.11 Ejemplo de una dirección IP en formato binario y decimal punteado.

La anotación w.x.y.z es utilizada cuando se hace referencia a una dirección IP como se muestra en la siguiente figura.

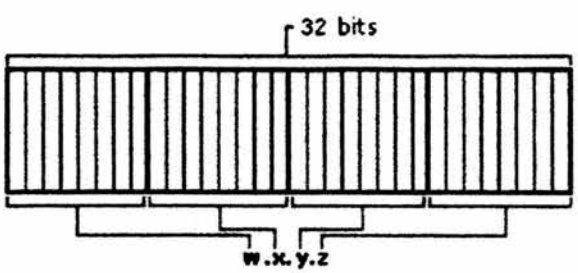


Figura 4.16 La dirección IP.

4.9.2 Clases de Direcciones

La comunidad de Internet originalmente definió cinco clases de direcciones para acomodar redes de diferentes tamaños. El TCP/IP de Microsoft soporta las direcciones de clase A, B y C asignadas a servidores. La clase de direcciones define cuales bits son usados para el identificador de red y que bits son usados para el identificador de servidor. También define el número posible de redes y el número de servidores por red.

Clase A.

Las direcciones de clase A son asignadas a redes con un número muy grande de servidores. El bit de orden alto en una dirección de clase A siempre es igual a cero. Los siguientes siete bits (completando el primer octeto) completan el identificador de la red. Los restantes 24 bits (los últimos tres octetos) representan el identificador del servidor. Esto permite 126 redes y 16,777,214 de servidores por red. La siguiente ilustra la estructura de las direcciones de clase A.

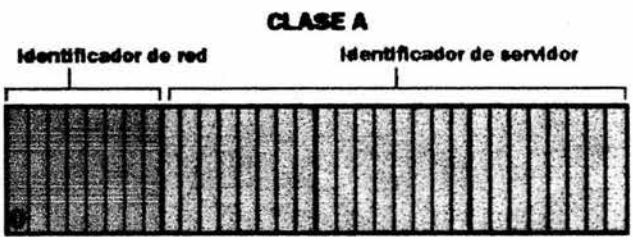


Figura 4.17 Direcciones IP de clase A.

Clase B.

Las direcciones de clase B son asignadas a redes de mediano a gran tamaño. Los dos bit de orden más alto en una dirección de clase B son siempre iguales al binario 10. Los siguientes 14 bits (completando los primeros dos octetos) completan el identificador de red. Los restantes 16 bits (los últimos dos octetos) representan el identificador del servidor. Esto permite 16,384 redes y 65,534 servidores por red. La siguiente figura ilustra la estructura de las direcciones de clase B.

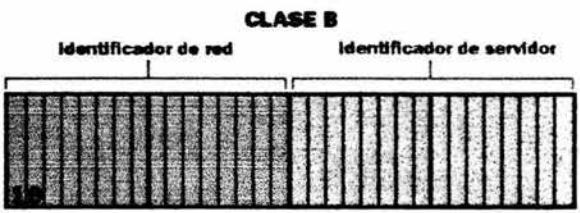


Figura 4.18 Direcciones IP de clase B.

Clase C.

Las direcciones de clase C son utilizadas para pequeñas redes. Los tres bits de orden más alto en una dirección de clase C son siempre iguales al binario 110. Los siguientes 21 bits (completando los primeros tres octetos) completan el identificador de red. Esto permite 2,097,157 redes y 254 servidores por red. La siguiente figura ilustra la estructura de las direcciones de clase C.

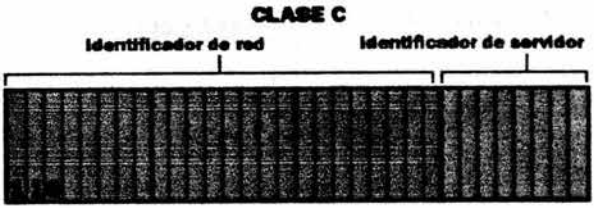


Figura 4.19 Direcciones IP de clase C.

Clase D.

Las direcciones de clase D están reservadas para direcciones IP multicast. Los cuatro bits de orden más alto en una dirección de clase D son siempre iguales al binario 1110. Los bits restantes son para la dirección que los servidores interesados reconocerán. Microsoft soporta direcciones de clase D para que las aplicaciones transmitan por multicast datos a servidores con capacidad multicast en una red.

Clase E.

Las direcciones de clase E son direcciones experimentales reservadas para uso futuro. Los bits de orden más alto en la dirección de clase E son iguales a 1111.
La tabla 4.12 es un resumen de las clases de direcciones A, B y C que pueden ser utilizados para direcciones de servidores IP.

Clase	Valor para w	Porción del identificador de red	Porción del identificador de servidor	Redes disponibles	Servidores por red
A	1-126	w	x.y.z	126	16,777,214
B	128-191	w.x	y.z	16,384	65,534
C	192-223	w.x.y	z	2,097,152	254

Tabla 4.12 Resumen de las direcciones de clases IP

Guías para el Identificador de Red

El identificador de red identifica a los servidores TCP/IP que están localizados en la misma red física. Todos los servidores en la misma red física deben tener asignado el mismo identificador de red para comunicarse unos con otros. A continuación las guías recomendadas a seguir cuando se debe asignar el identificador de red:

a) La dirección de red debe ser única dentro de la red IP. Sí se planea tener una conexión enrutada directa a Internet, el identificador de red debe ser único en Internet. Sí no se planea conectarse a internet, el identificador de red debe ser único en la red privada.

b) El identificador de red no puede empezar con el número 127. El número 127 es una dirección de clase A reservada para funciones loopback internas.

c) Todos los bits dentro del identificador de red no pueden ser iguales a 1. Todos los 1's en el identificador de red son reservados para una dirección de transmisión IP.

d) Todos los bits dentro del identificador de red no pueden ser iguales a 0. Todos los 0's en identificador de red son utilizados para denotar un servidor específico en la red local y no serán enrutados.
La siguiente tabla lista los rangos válidos de identificadores de red basados en las clases de direcciones IP. Para denotar identificadores de red IP, los bits del servidor son todos iguales a 0. Hay que notar que aunque esté expresado en notación decimal punteada el identificador de red no es una dirección IP.

Clase de dirección	Primer identificador de red	Ultimo identificador de red
Clase A	1.0.0.0	126.0.0.0
Clase B	128.0.0.0	191.255.0.0
Clase C	192.0.0.0	223.255.255.0

Tabla 4.13. Rangos de las clases de identificadores de red.

Guías para el Identificador de Servidor

Los identificadores de servidor identifican un servidor TCP/IP dentro de una red. La combinación del identificador de red y del identificador de red IP es una dirección IP.

A continuación las guías que se sugieren para asignar un identificador de servidor:

a) El identificador de servidor debe ser único para el identificador de red.

b) Todos los bits dentro del identificador del servidor no pueden ser iguales a 1, porque este identificador está reservado como una dirección de transmisión para enviar un paquete a todos los servidores de una red.

c) Todos los bits en el identificador de red no pueden ser iguales a 0 porque este identificador de servidor está reservado para denominar el identificador de red IP.
La tabla 4.14 lista los rangos válidos de identificador de servidor basados en las clases de direcciones IP.

Clase de dirección	Primer identificador del servidor	Ultimo identificador del servidor
Clase A	w.0.0.1	w.255.255.254
Clase B	w.x.0.1	w.x.255.254
Clase C	w.x.y.1	w.x.y.254

Tabla 4.14. Rangos de clase de los Identificadores de Servidor.

4.9.3 Creación de Subredes IP

Las clases de direcciones de Internet fueron diseñadas para acomodar tres diferentes escalas de redes IP, donde los 32 bits de la dirección IP son repartidos entre identificadores de red e identificadores de servidor dependiendo de cuantas redes y servidores por red son necesarios. Sin embargo, es importante considerar los identificadores de red de clase A, quienes tiene la posibilidad de más de 16 millones de servidores en la misma red.

Todos los servidores en la misma red física limitados por ruteadores IP comparten el mismo tráfico de transmisión; están en el mismo dominio de transmisión (broadcast domain). No es práctico tener 16 millones de nodos en el mismo dominio de transmisión. El resultado es que la mayoría de las 16 millones de direcciones de servidor no son asignables y son desperdiciadas. Incluso una red de clase B con 65 mil servidores es impráctica. En un esfuerzo para crear dominio de transmisión más pequeños y para utilizar mejor los bits del identificador de servidor, una red IP puede ser subdividida en redes más pequeñas, cada una limitada por un ruteador IP y a las que se le asigna un nuevo identificador de subred, el cual es un subconjunto de identificador de red basado en clases originales. Esto crea subredes, subdivisiones de una red IP cada una con su identificador de subred único. Los identificadores de subred son creados usando bits de la porción del identificador de servidor del identificador de red original basado en clases.

Considerando el ejemplo en la siguiente figura. La red de clase B de 139.12.0.0 puede tener hasta 65,534 nodos. Estos son demasiados nodos, y de hecho, la red actual se está saturando con tráfico de transmisión. La conversión de la red 139.12.0.0 en subredes debe ser hecha de tal manera que no impacte, ni requiera la reconfiguración del resto de la red IP.

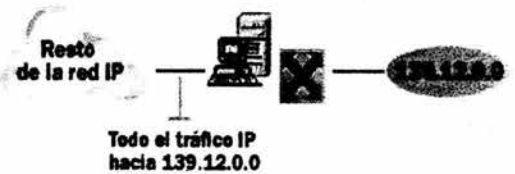


Figura 4.20 La red 139.12.0.0 antes de hacer las subredes.

La red 139.12.0.0 fue convertida en subredes utilizando los primeros ocho bits del servidor (el tercer octeto) para el nuevo identificador de subred. Cuando la 139.12.0.0 es convertida a subredes, como se muestra en la figura 4.21, redes separadas con sus propios identificadores de subred (139.12.1.0, 139.12.2.0, 139.12.3.0) son creadas. El ruteador se da cuenta de los identificadores de subred separados y enrutará los paquetes IP a su subred apropiada.
Es importante notar que el resto de la red IP aún considera a todos los nodos de las tres subredes como parte de la red 139.12.0.0. Los otros ruteadores en la red IP no se dan cuenta de que se han creado subredes en la red 139.12.0.0 y por lo tanto no requieren reconfiguración.

Figura 4.21 La red 139.12.0.0 después de crear subredes.

Un elemento clave de las subredes falta todavía. ¿Cómo sabe el ruteador que subdivide a la red 139.12.0.0 cómo está siendo subdividida la red y cuáles subredes están disponibles en cuáles interfases del ruteador? Para darle a los nuevos IP este nuevo nivel de conocimiento, se les debe decir exactamente cómo discernir el nuevo identificador de subred sin importar las Clases de Direcciones de Internet. Para decirle a un nodo IP exactamente cómo extraer un identificador de red, ya sea basado en clases o en subredes, se utiliza una máscara de subred.

4.9.3.1 Máscaras de Subred

Con el advenimiento de las subredes, ya no se puede apoyar en la definición de las clases de direcciones IP para determinar el identificador de red en la dirección IP. Se necesita un nuevo valor para definir que parte de la dirección IP es el identificador de red y que parte es el identificador de servidor, sin importar si se utilicen identificadores de red basados en clase o en subredes.
El RFC 950 define el uso de una máscara de subred (referida como una máscara de dirección), como un valor de 32 bits el cual es utilizado para distinguir el identificador de la red del identificador del servidor en una dirección IP arbitraria. Los bits de la máscara de subred se definen como:

a) Todos los bits que correspondan al identificador de red son puestos a 1.

b) Todos los bits que correspondan al identificador del servidor son puestos a 0.
Cada servidor en una red TCP/IP requiere una máscara de subred incluso en una red de un segmento único. En cada nodo TCP/IP se configura ya sea una máscara de subred por defecto, la cual es utilizada cuando se usan identificadores de red basados en clases, o una máscara de subred personalizada, la cual es utilizada cuando se hacen subredes o superredes.

Tipos de Máscaras de Subred.

Las máscaras de subred son frecuentemente expresadas en notación decimal punteada. Una vez que los bits son establecidos para las porciones de identificador de red e identificador de servidor, el número de 32 bits resultante es convertido a notación decimal punteada. Note que aunque esté expresado en notación decimal punteada, una máscara de subred no es una dirección IP.

a) Máscara de Subred por Defecto

Una máscara de subred por defecto está basada en las clases de direcciones IP y es utilizada en redes TCP/IP que no estén divididas en subredes. La siguiente lista las máscaras de subred por defecto utilizando notación decimal punteada para la máscara de subred.

Clase de dirección	Bits para la máscara de subred	Máscara de subred
Clase A	11111111 00000000 00000000 00000000	255.0.0.0
Clase B	11111111 11111111 00000000 00000000	255.255.0.0
Clase C	11111111 11111111 11111111 00000000	255.255.255.0

Tabla 4.15 Máscaras de subred por defecto en notación decimal punteada.

b) Máscaras de Subred Personalizadas

Las máscaras de subred personalizadas son aquellas que difieren de las máscaras de subred por defecto anteriores cuando se hacen subredes o superredes. Por ejemplo, el 138.96.58.0 en un identificador de red de clase B para subredes. Ocho bits del identificador del servidor basado en clases están siendo utilizados para expresar los identificadores de subredes. La máscara de subred utiliza un total de 24 bits (255.255.255.0) para definir èl identificador de subred. El identificador de subred y su máscara de subred correspondiente son entonces expresadas en notación decimal punteada como:
138.96.58.0, 255.255.255.0

Representación de la Máscara de Subred.

Debido a que los bits del identificador de red deben siempre ser elegidos de una manera contigua a los bits de orden alto, una manera compacta de expresar una máscara de subred es denotar el número de bits de definen al identificador de la red, como un prefijo de red utilizando la notación de prefijo de red: /<# de bits>. La siguiente tabla lista las máscaras de subred utilizando la notación de prefijo de red para la máscara de subred.

Clase de dirección	Bits para la máscara de subred	Prefijo de red
Clase A	11111111 00000000 00000000 00000000	/8
Clase B	11111111 11111111 00000000 00000000	/16
Clase C	11111111 11111111 11111111 00000000	/24

Tabla 4.16. Máscaras de subred por defecto utilizando la notación de prefijo de red para la máscara de subred.

Por ejemplo, el identificador de red de clase B 138.96.0.0 con la máscara de subred 255.255.0.0 sería expresado en notación de prefijo de red como 138.96.0.0/16.
Como un ejemplo de una máscara de subred personalizada, el 138.96.58.0 es un identificador de red clase B con subredes de 8 bits. La máscara de subred utiliza un total de 24 bits para definir el identificador de subred. El identificador de subred y su máscara de subred correspondiente son entonces expresados en notación de prefijo de red, como:
138.96.58.0/24

Determinando el Identificador de Red.

Para extraer el identificador de red de una dirección IP arbitraria, utilizando una máscara de subred, el IP utiliza una operación matemática llamada una comparación lógica AND. En una comparación AND, el resultado de los dos elementos que están siendo comparados es verdadero solamente cuando ambos elementos son verdaderos, de otro modo el resultado es falso. Aplicando este principio a los bits, el resultado es uno cuando ambos bits comparados son iguales a 1; de otro modo el resultado es 0.
El IP toma la direcciones IP de 32 bits y ejecuta un AND lógico con una máscara de subred de 32 bits. Esta operación es conocida como un AND lógico sobre bits (bit-wise). El resultado del AND lógico de la dirección IP y la máscara de subred es el identificador de red.

4.10 PROTOCOLOS DE COMUNICACIÓN MÁS CONOCIDOS

En la actualidad se cuenta con muchos protocolos de comunicación comerciales con los cuales muchas veces aún sin darnos cuenta, los utilizamos y nos ayudan a hacer tareas como lo son el Internet, una transferencia por módem o una simple comunicación a un servicio en línea inteligente. A continuación se describiremos algunos de los protocolos más importantes y/ o comerciales hoy en día.

4.10.1 Protocolo de Transferencia de Archivos (FTP)

El objetivo principal de este protocolo son varios puntos, promover el compartir archivos entre computadoras (programas y/ o datos), alentar al uso remoto de las computadoras, y transferir datos de una forma segura y óptima por computadora. FTP (File Transfer Protocol; FTP) más que para ser usado por un usuario directamente es para que los programas lo usen entre ellos para comunicarse.
Con este tipo de forma de hacer las cosas se le ayuda al usuario a despreocuparse si él tiene contacto con macro computadoras, micro, mini o simples PC's, gracias a un protocolo como este, no se necesita saber mucho y se logra lo que se quiere.
FTP ha ido evolucionando demasiado en todos estos años desde que se creo, este empezó en 1971 con un modelo de transferencia llamado RFC 141 en M.I.T. Fue hasta después de muchas revisiones que llegó a RFC 265 cuando ya se le considero un protocolo de transferencia de archivos completa entre HOST's (servidores de archivos) de ARPHANET. Finalmente un documento declarando un FTP oficial se publico cuando se llego a RFC 454.

Algunos de los comandos más utilizados en este protocolo en la actualidad son:

CDUP	Change to Parent Directory
SMNT	Structure Mount
STOU	Store Unique
RMD	Remove Directory
MKD	Make Directory
PWD	Print Directory
SIST.	System

Terminología de este protocolo.

Alguna de la terminología usada en este protocolo son las siguientes definiciones:

ASCII: Solo se usan todos los caracteres dentro de los 8 bits en su valor bajo

Access Controls: Este sirve para hablar a cerca de los privilegios (derechos en la red) de cada usuario tanto en archivos como en dispositivos.

Data Connection: Habla de cuando hay una comunicación Full Duplex entre dos computadoras.

DTP: Proceso de la transferencia.

Error Recovery: Este es un procedimiento que le permite al usuario en algunos casos recuperar información perdida en el proceso de transferencia.

Tipos de datos:

Existen tres tipos de datos en la transferencia por FTP, tipo ASCII, EBCDIC e IMAGEN.

a) El tipo ASCII, es el más común en el protocolo FTP, este se usa cuando se transfieren archivos de texto, la computadora que envía (sender), debe convertir cualquiera que sea su estructura de archivos interna, debe convertir sus datos al formato genérico de 8 bits, y el que recibe (receiver) lo debe convertir de nuevo a su formato propio.

b) El tipo EBCDIC es el más eficiente cuando ambos el que recibe y el que envía lo usan como formato propio, este tipo se representa también en 8 bits pero de forma EBCDIC. Lo único en lo que cambian es en la forma de reconocer los códigos de los caracteres.

c) El formato de IMAGEN es cuando se empaca todo lo que se quiere enviar en cadenas seguidas de paquetes de 8 bits, esto es no importa el formato en que internamente se maneje la información, cuando se va a enviar se tiene que hacer una conversión de 8 bits en 8 bits y cuando el que recibe tiene todo el paquete, el mismo debe codificarlos de nuevo para que la transmisión sea completada.

Tipos de Archivos:

En la estructura de datos en FTP se consideran tres tipos diferentes de archivos:

a) File – Structure: donde no hay estructuras internas y el archivo es considerado una secuencia continua de bytes

b) Record – Structure: donde los archivos contienen puros registros igualitos en estructura

c) Page – Structure: donde los archivos contienen paginas enteras indexadas separadas.

Al establecer una conexión por FTP se debe tomar en cuenta que el mecanismo de transferencia consiste en colocar bien la transferencia de datos en los puertos adecuados y al concluir la conexión estos puertos deben ser cerrados adecuadamente. El tamaño de transferencia es de 8 bits, en ambos. El que va a transferir, debe escuchar desde el puerto hasta que el comando enviado sea recibido y este será el que de la dirección de la transferencia. Una vez recibido el comando y establecido una transferencia del servidor al que solicita, sé inicializa la comunicación de la transferencia para verificar la conexión, esta es una cabecera con un formato específico, después de esto se comienza a enviar las tramas de 8 bits sin importar el tipo de datos que sea (antes mencionado), y al finalizar se envía otra trama cabecera ya establecida confirmando la transferencia completada.

Modos de Transferencia:

Existen tres modos de transferencia en FTP

STREAM MODE

BLOCK MODE

COMPRESSED MODE

4.10.2 Protocolo para la Transferencia de Hipertextos (HTTP)

El protocolo para la transferencia de hipertextos HTTP (Hyper Text Transfer Protocol;HTTP) es para todos los sistemas de información distribuidos que tengan la necesidad de mostrar la información y pasarla por una comunicación normal haciendo uso de las ligas de este lenguaje. La primera versión de este lenguaje (HTTP 0.9) se uso desde 1990. El Protocolo fue implementado inicialmente para WWW en 1991 como una iniciativa de software y se denominó HTTP 0.9. El protocolo completo fue definido en 1992 e implementado en marzo de 1993.

HTTP 1.0: Esta especificación prevé las características básicas del protocolo. Fue desarrollado por Tim Berners-Lee, Roy T. Fielding, y Henrik Frystyk Nielsen.

HTTP 1.1: La primera versión no está aún habilitada, pero las especificaciones son muy similares a la anterior.

HTTP-NG Next Generation of HTTP: propuesta por Simón Spero. Es un protocolo binario con nuevas características para un acceso más rápido usando TCP. Este es el último HTTP en la actualidad.

Terminología:

Este protocolo como todos tiene una propia terminología, a continuación la terminología más importante usada en este protocolo.

a) Conexión: Es el circuito virtual establecido entre dos programas en una red de comunicación con el proceso de una simple comunicación.

b) Mensaje: Esta es la unidad básica de un protocolo HTTP, estos consisten en una secuencia estructurada que es transmitida siempre entre los programas.

c) Cliente: Es el programa que hace la llamada al servidor y es el que atiende en toda la transmisión la trama de los mensajes.

d) Servidor: El que presta el servicio en la Red.

e) Proxy: Un programa intermedio que actúa sobre los dos, el servidor y el cliente.

4.10.3 Sistema de Archivos de Red (NFS)

NFS (Network File System; NFS) es un sistema distribuido para archivos, este es para las redes heterogéneas, con este protocolo, el usuario solo ve un directorio cuando esta dentro de la red, claro que tiene ramas dentro pero no puede ver mas arriba de el nivel en el que se entra, tal vez los archivos dentro de esta estructura del directorio ni siquiera están en la misma computadora.

4.10.4 Protocolo de Oficina Postal Versión 3 (POP3)

POP3 (Post Office Protocol Version 3) es netamente un protocolo para la administración de correo en Internet. En algunos nodos menores de Internet normalmente es poco práctico mantener un sistema de transporte de mensajes (MTS). Por ejemplo, es posible que una estación de trabajo no tenga recursos suficientes (espacio en disco, entre otros) para permitir que un servidor y un sistema local asociado de entrega de correo estén residentes y continuamente en ejecución. De forma similar, puede ser caro (o incluso imposible) mantener una computadora personal interconectada a una red tipo IP durante grandes cantidades de tiempo (el nodo carece el recurso conocido como "connectivity"). A pesar de esto, a menudo es muy útil poder administrar correo sobre estos nodos y frecuentemente soportan un user agent (UA) (agente de usuario) para ayudar en las tareas de manejo de correo. Para resolver el problema, un nodo que si sea capaz de soportar un MTS ofrecerá a estos nodos menos dotados un servicio de maildrop. Se entiende por maildrop, el "lugar" en el sistema con el MTS donde el correo es almacenado para que los otros nodos puedan trabajar con él sin necesidad de mantener su propio MTS.

El Protocolo de oficina de correos - Versión 3 (POP3) está destinado a permitir que una estación de trabajo acceda dinámicamente a un maildrop en un host servidor de forma útil y eficiente. Esto significa que el protocolo POP3 se usa para permitir a una estación de trabajo recobrar correo que el servidor tiene almacenado.

Una sesión POP3 progresa a través de una serie de estados a lo largo de su vida. Una vez la conexión TCP ha sido abierta y el servidor de POP3 ha enviado el "saludo" (línea especial que se utiliza cuando se establece la conexión), la sesión entra en el estado de autorización (AUTHORIZATION). En este estado, el cliente debe identificarse al servidor de POP3. Una vez el cliente ha hecho esto satisfactoriamente, el servidor adquiere los recursos asociados al maildrop del cliente, y la sesión entra en el estado de transacción (TRANSACTION). En este estado, el cliente realiza una serie de solicitudes al servidor de POP3. Cuando el cliente ha emitido el comando de finalización (QUIT), la sesión entra en el estado de actualización (UPDATE). En este estado, el servidor de POP3 libera cualesquiera recursos adquiridos durante el estado de transición, "dice adiós" y la conexión TCP se cierra.

Un servidor debe responder a comandos no reconocidos, no implementados, o sintácticamente incorrectos con un indicador negativo de estado (respuesta negativa). También debe responder con un indicador negativo de estado cuando la sesión se encuentra en un estado incorrecto. No hay un método general para que el cliente distinga entre un servidor que no implementa un comando opcional y un servidor que no esta dispuesto o es incapaz de procesar el comando.

Un servidor de POP3 puede disponer de un temporizador o cronómetro de inactividad (autologout inactivity timer). Tal cronómetro debe ser de por lo menos 10 minutos de duración. La recepción de cualquier comando desde el cliente durante este intervalo reinicia la cuenta de este cronómetro. Cuando el cronómetro llega a los diez minutos, la sesión no entra en el estado de actualización. Entonces, el servidor debería cerrar la conexión TCP sin eliminar ningún mensaje y sin enviar ninguna respuesta al cliente.

Una vez que ya describimos los conceptos básicos de redes que consideramos más importantes en el desarrollo de este trabajo de investigación, en el próximo capítulo describiremos los conceptos más importantes sobre conectividad y seguridad a tomar en cuenta en el diseño o armado de una red de cómputo.

CAPÍTULO 5
CONECTIVIDAD Y SEGURIDAD

5.1 EQUIPOS DE CONECTIVIDAD

Los equipos de conectividad son todos aquellos dispositivos que ayudaran a que se realice la comunicación remota entre las bases de datos corporativas y los empleados que por alguna u otra razón se encuentren trabajando remotamente, a continuación realizaremos un estudio detallado de equipos de conectividad necesarios el objetivo de TESYS, como son: ruteadores, conmutadores y concentradores, modems, pasarelas y puentes.

5.1.1 Ruteadores (Routers)

Son dispositivos inteligentes que trabajan en el nivel de red del modelo de referencia OSI, por lo que son dependientes del protocolo particular de cada red. Envían paquetes de datos de un protocolo común, desde una red a otra. Convierten los paquetes de información de la red de área local (LAN), en paquetes capaces de ser enviados mediante redes de área extensa (WAN). Durante el envío, el ruteador examina el paquete buscando la dirección de destino consultando su propia tabla de direcciones, la cual mantiene actualizada intercambiando direcciones con los demás ruteadores para establecer rutas de enlace a través de las redes que los interconectan. Este intercambio de información entre ruteadores se realiza mediante protocolos de gestión propietarios.

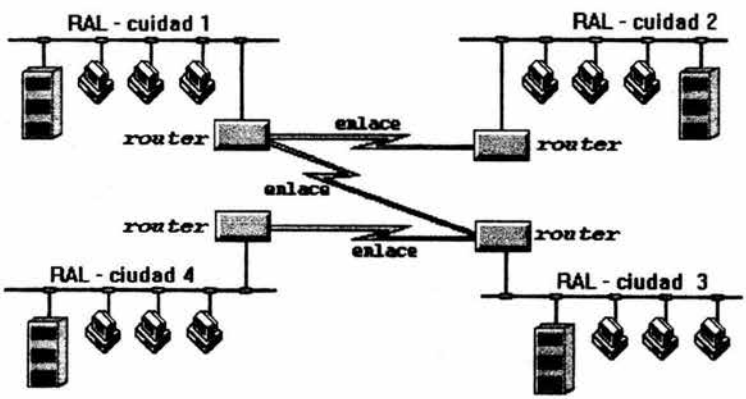


Figura 5.1 Envió de datos a través de los ruteadores

Los ruteadores se pueden clasificar dependiendo de varios criterios:

En función del área:

a). Locales: Sirven para interconectar dos redes por conexión directa de los medios físicos de ambas al ruteador.

b) De área extensa: Enlazan redes distantes.
En función de la forma de actualizar las tablas de ruteamiento:

c) Estáticos: La actualización de las tablas es manual.

d) Dinámicos: La actualización de las tablas las realiza el propio ruteador automáticamente.

En función de los protocolos que soportan:

IPX
TCP/IP
DECnet
AppleTalk
XNS
OSI
X.25
etc.

En función del protocolo de ruteamiento que utilicen:

a) Routing Information Protocol (RIP)

Permite comunicar diferentes sistemas que pertenezcan a la misma red lógica. Tienen tablas de ruteamiento dinámicas y se intercambian información según la necesitan. Las tablas contienen por dónde ir hacia los diferentes destinos y el número de saltos que se tienen que realizar. Esta técnica permite 14 saltos como máximo.

b) Exterior Gateway Protocol (EGP)

Este protocolo permite conectar dos sistemas autónomos que intercambien mensajes de actualización. Se realiza un sondeo entre los diferentes ruteadores para encontrar el destino solicitado. Este protocolo sólo se utiliza para establecer un camino origen-destino; no funciona como el RIP determinando el número de saltos.

c) Open Shortest Path First Routing (OSPF)

Está diseñado para minimizar el tráfico de ruteamiento, permitiendo una total autentificación de los mensajes que se envían. Cada ruteador tiene una copia de la topología de la red y todas las copias son idénticas. Cada ruteador distribuye la información a su ruteador adyacente. Cada equipo construye un árbol de ruteamiento independientemente.

d) IS-IS

Ruteamiento OSI según las normativas: ISO 9575, ISO 9542 e ISO 10589. El concepto fundamental es la definición de ruteamiento en un dominio y entre diferentes dominios. Dentro de un mismo dominio el ruteamiento se realiza aplicando la técnica de menor coste. Entre diferentes dominios se consideran otros aspectos como puede ser la seguridad.

Otras variantes de los ruteadores son:

a) Ruteador Multiprotocolo

Tienen la posibilidad de soportar tramas con diferentes protocolos de Nivel de Red de forma simultánea, encaminándolas dinámicamente al destino especificado, a través de la ruta de menor coste o más rápida. Son los ruteadores de segunda generación. No es necesario, por tanto, tener un ruteador por cada protocolo de alto nivel existente en el conjunto de redes interconectadas.

Esto supone una reducción de gastos de equipamiento cuando son varios los protocolos en la red global.

b) Brouter (bridging router)

Son ruteadores multiprotocolo con facilidad de puente. Funcionan como ruteador para protocolos ruteables y, para aquellos que no lo son se comportan como puente, transfiriendo los paquetes de forma transparente según las tablas de asignación de direcciones. Operan tanto en el nivel de enlace como en el nivel de red del modelo de referencia OSI. Por ejemplo, un Brouter puede soportar protocolos de ruteamiento además de source routing y spanning tree bridging. El Brouter funciona como un ruteador multiprotocolo, pero si encuentra un protocolo para el que no puede encaminar, entonces simplemente opera como puente.
Las características y costos de los Brouter, hacen de estos la solución más apropiada para el problema de interconexión de redes complejas. Ofrecen la mayor flexibilidad en entornos de interconexión complejos, que requieran soporte multiprotocolo, source routing y spanning tree e incluso de protocolos no encaminables. Son aconsejables en situaciones mixtas bridge/router. Ofrecen la mayor flexibilidad en entornos de interconexión complejos, que requieran soporte multiprotocolo.

c) Trouter

Es una combinación entre un ruteador y servidor de terminales. Permite a pequeños grupos de trabajo la posibilidad de conectarse a RALs, WANs, modems, impresoras, y otras computadoras sin tener que comprar un servidor de terminales y un ruteador. El problema que presenta este dispositivo es que al integrar las funcionalidades de ruteador y de servidor de terminales puede ocasionar una degradación en el tiempo de respuesta.

Ventajas de los ruteadores:

a) Seguridad. Permiten el aislamiento de tráfico, y los mecanismos de ruteamiento facilitan el proceso de localización de fallos en la red.

b) Flexibilidad. Las redes interconectadas con ruteador no están limitadas en su topología, siendo estas redes de mayor extensión y más complejas que las redes enlazadas con puente.

c) Soporte de Protocolos. Son dependientes de los protocolos utilizados, aprovechando de una forma eficiente la información de cabecera de los paquetes de red.

d) Relación Precio / Eficiencia. El coste es superior al de otros dispositivos, en términos de precio de compra, pero no en términos de explotación y mantenimiento para redes de una complejidad mayor.

e) Control de Flujo y Ruteamiento. Utilizan algoritmos de ruteamiento adaptativo (RIP, OSPF, etc), que gestionan la congestión del tráfico con un control de flujo que redirige hacia rutas alternativas menos congestionadas.

Desventajas de los ruteadores:

a) Lentitud de proceso de paquetes respecto a los puentes.
b) Necesidad de gestionar el subdireccionamiento en el Nivel de Enlace.
c) Precio superior a los puentes.

En resumen, por su posibilidad de segregar tráfico administrativo y determinar las rutas más eficientes para evitar congestión de red, los ruteadores son una excelente solución para una gran interconexión de redes con múltiples tipos de LANs, MANs, WANs y diferentes protocolos. Es una buena solución en redes de complejidad media, para separar diferentes redes lógicas, por razones de seguridad y optimización de las rutas

5.1.2 Conmutadores y Concentradores (Switchs y Hubs)

5.1.2.2 Conmutadores (Switchs)

Los conmutadores tienen la funcionalidad de los concentradores a los que añaden la capacidad principal de dedicar todo el ancho de banda de forma exclusiva a cualquier comunicación entre sus puertos. Esto se consigue debido a que el conmutador no actúa como repetidor multipuerto, sino que únicamente envía paquetes de datos hacia aquella puerta a la que van dirigidos. Esto es posible debido a que los equipos configuran unas tablas de ruteamiento con las direcciones MAC (nivel 2 de OSI) asociadas a cada una de sus puertas.
Esta tecnología hace posible que cada una de las puertas disponga de la totalidad del ancho de banda para su utilización. Estos equipos habitualmente trabajan con anchos de banda de 10 y 100 Mbps, pudiendo coexistir puertas con diferentes anchos de banda en el mismo equipo. Las puertas de un conmutador pueden dar servicio tanto a puestos de trabajo personales como a segmentos de red (concentradores), siendo por este motivo ampliamente utilizados como elementos de segmentación de redes y de ruteamiento de tráfico. De esta forma se consigue que el tráfico interno en los distintos segmentos de red conectados al conmutador no afecte al resto de la red aumentando de esta manera la eficiencia de uso del ancho de banda.

Tipos de conmutadores o técnicas de conmutación:

a) Almacenar - Transmitir. Almacenan las tramas recibidas y una vez chequeadas se envían a su destinatario. La ventaja de este sistema es que previene del malgasto de ancho de banda sobre la red destinataria al no enviar tramas inválidas o incorrectas. La desventaja es que incrementa ligeramente el tiempo de respuesta del conmutador.

b) Contar.- Continuar. En este caso el envío de las tramas es inmediato una vez recibida la dirección de destino. Las ventajas y desventajas son cruzadas respecto a almacenar-transmitir. Este tipo de conmutadores es indicado para redes con poca latencia de errores.

c) Híbridos. Este conmutador normalmente opera como cortar-continuar, pero constantemente monitoriza la frecuencia a la que tramas inválidas o dañadas son enviadas. Si este valor supera un umbral prefijado el conmutador se comporta como un almacenar-transmitir. Si desciende este nivel se pasa al modo inicial. En caso de diferencia de velocidades entre las subredes interconectadas el conmutador necesariamente ha de operar como almacenar -transmitir.

5.1.2.3 Concentradores (Hubs)

Son equipos que permiten estructurar el cableado de las redes. La variedad de tipos y características de estos equipos es muy grande. En un principio eran solo concentradores de cableado, pero cada vez disponen de mayor número de capacidades, como aislamiento de tramos de red, capacidad de conmutación de las salidas para aumentar la capacidad de la red, gestión remota, etc. La tendencia es seguir incorporando más funciones en el concentrador.
Existen concentradores para todo tipo de medios físicos. El término concentrador o hub describe la manera en que las conexiones de cableado de cada nodo de una red se centralizan y conectan en

un único dispositivo. Se suele aplicar a concentradores Ethernet, TokenRing y FDDI (Fiber Distributed Data Interfase) soportando módulos individuales que concentran múltiples tipos de funciones en un solo dispositivo. Normalmente los concentradores incluyen ranuras para aceptar varios módulos y un panel trasero común para funciones de ruteamiento, filtrado y conexión a diferentes medios de transmisión (por ejemplo Ethernet y TokenRing).

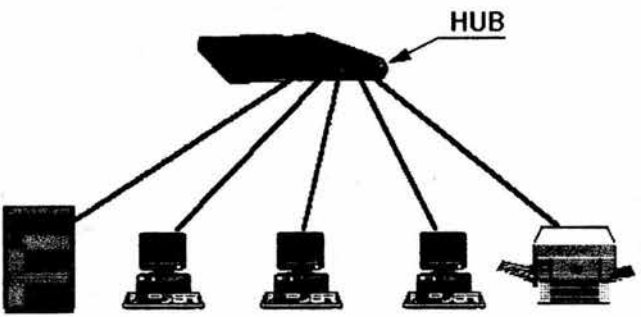


Figura 5.2 Ejemplo de conexión de un concentrador (HUB)

Concentradores de primera generación.

Los primeros concentradores o de "primera generación" son cajas de cableado avanzadas que ofrecen un punto central de conexión conectado a varios puntos. Sus principales beneficios son la conversión de medio (por ejemplo de coaxial a fibra óptica), y algunas funciones de gestión bastante primitivas como particionamiento automático cuando se detecta un problema en un segmento determinado.

Concentradores de segunda generación.

Los concentradores inteligentes de "segunda generación" basan su potencial en las posibilidades de gestión ofrecidas por las topologías radiales (TokenRing y Ethernet). Tiene la capacidad de gestión, supervisión y control remoto, dando a los gestores de la red la oportunidad de ofrecer un periodo mayor de funcionamiento de la red gracias a la aceleración del diagnóstico y solución de problemas. Sin embargo tienen limitaciones cuando se intentan emplear como herramienta universal de configuración y gestión de arquitecturas complejas y heterogéneas.

Concentradores de tercera generación.

Los nuevos concentradores de "tercera generación" ofrecen proceso basado en arquitectura RISC (Reduced Instructions Set Computer) junto con múltiples placas de alta velocidad. Estas placas están formadas por varios buses independientes Ethernet, TokenRing, FDDI y de gestión, lo que elimina la saturación de tráfico de los actuales productos de segunda generación. A un concentrador Ethernet se le denomina "repetidor multipuerta". El dispositivo repite simultáneamente la señal a múltiples cables conectados en cada uno de los puertos del concentrador. En el otro extremo de cada cable está un nodo de la red, por ejemplo una computadora personal.

Concentradores Ethernet.

Un concentrador Ethernet se convierte en un concentrador inteligente (smart hub) cuando puede soportar inteligencia añadida para realizar monitorización y funciones de control. Los concentradores inteligentes (smart hub) permiten a los usuarios dividir la red en segmentos de fácil detección de errores a la vez que proporcionan una estructura de crecimiento ordenado de la red. La capacidad de gestión remota de los concentradores inteligentes hace posible el diagnóstico remoto de un problema y aísla un punto con problemas del resto de la RAL, con lo que otros usuarios no se ven afectados.
El tipo de concentrador Ethernet más popular es el concentrador 10BaseT. En este sistema la señal llega a través de cables de par trenzado a una de las puertas, siendo regenerada eléctricamente y enviada a las demás salidas. Este elemento también se encarga de desconectar las salidas cuando se produce una situación de error. A un concentrador TokenRing se le denomina Unidad de Acceso Multiestación (MAU, Multiestation Access Unit). Las MAUs se diferencian de los concentradores Ethernet porque las primeras repiten la señal de datos únicamente a la siguiente estación en el anillo y no a todos los nodos conectados a ella como hace un concentrador Ethernet. Las MAUs pasivas no tienen inteligencia, son simplemente retransmisores. Las MAUs activas no sólo repiten la señal, además la amplifican y regeneran. Las MAUs inteligentes detectan errores y activan procedimientos para recuperarse de ellos.

5.1.3 Módem

El módem es un dispositivo que permite conectar dos computadoras utilizando la línea telefónica de forma que puedan intercambiar información entre sí. El módem es uno de los métodos mas extendidos para este tipo de interconexión de computadoras por su sencillez y bajo costo. La gran cobertura de la red telefónica convencional posibilita la casi inmediata conexión de dos computadoras si se utiliza módem. Por todas estas razones el módem es considerado el método más popular de acceso a la Internet por parte de los usuarios privados y muchas de las empresas.

La información que maneja la computadora es digital, es decir esta compuesta por un conjunto discreto de dos valores el 1 y el 0. Sin embargo, por las limitaciones físicas de las líneas de transmisión no es posible enviar información digital a través de un circuito telefónico. Para poder utilizar las líneas de teléfono (y en general cualquier línea de transmisión) para el envío de información entre computadoras digitales, es necesario un proceso de transformación de la información. Durante este proceso la información sé adecua para ser transportada por el canal de comunicación. Este proceso se conoce como modulación-demodulación y es el que se encargue de realizar el módem.

5.1.3.1 Modulación de la información

Existen distintos sistemas de modular una señal analógica para que transporte información digital. En la siguiente figura se muestran los dos métodos más sencillos la modulación de amplitud y la modulación de frecuencia.

Otros mecanismos como la modulación de fase o los métodos combinados permiten transportar más información por el mismo canal.

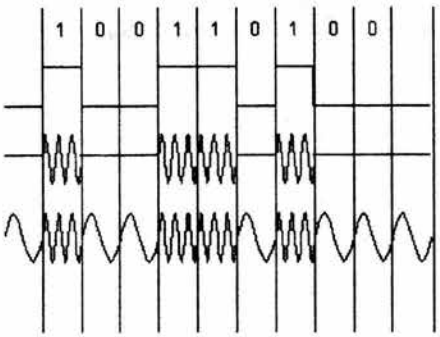


Figura 5.3 Ejemplo de la modulación en frecuencia

A continuación describiremos algunas de las definiciones principales y necesarias para lograr la modulación de la información.

Baudios.

Número de veces de cambio en el voltaje de la señal por segundo en la línea de transmisión. Los módem envían datos como una serie de tonos a través de la línea telefónica. Los tonos se "encienden"(ON) o "apagan"(OFF) para indicar un 1 o un 0 digital. El baudio es él número de veces que esos tonos se ponen a ON o a OFF. El módem moderno puede enviar 4 o más bits por baudio.

Bits por segundo (BPS).

Es el número efectivo de bits/seg que se transmiten en una línea por segundo. Como hemos visto un módem de 600 baudios puede transmitir a 1200, 2400 o, incluso a 9600 BPS. La señal esta formada por diferentes tonos que viajan hasta el otro extremo de la línea telefónica, donde se vuelven a convertir a datos digitales. Las leyes físicas establecen un límite para la velocidad de transmisión en un canal ruidoso, con un ancho de banda determinado. Por ejemplo, un canal de banda 3000Hz, y una señal de ruido 30dB (que son parámetros típicos del sistema telefónico), nunca podrán transmitir a más de 30.000 BPS.

Tasa efectiva de Transmisión (Throughput).

Define la cantidad de datos que pueden enviarse a través de un módem en un cierto período de tiempo. Un módem de 9600 baudios puede tener un Throughput distinto de 9600 BPS debido al ruido de la línea o a la compresión de datos (que puede incrementar la velocidad hasta 4 veces el valor de los baudios). Para mejorar la tasa efectiva de transmisión o Throughput se utilizan técnica de compresión de datos y corrección de errores.

a) Compresión de datos.

Describe el proceso de tomar un bloque de datos y reducir su tamaño. Se emplea para eliminar información redundante y para empaquetar caracteres empleados frecuentemente y representarlos con sólo uno o dos bits.

b) Control de errores.

La ineludible presencia de ruido en las líneas de transmisión provoca errores en el intercambio de información que se debe detectar introduciendo información de control. Así mismo puede incluirse información redundante que permita además corregir los errores cuando se presenten.

5.1.3.2 Estándares de modulación

Dos módems para comunicarse necesitan emplear la misma técnica de modulación. La mayoría de los módem son full-duplex, lo cual significa que pueden transferir datos en ambas direcciones. Hay otros módem que son half-duplex y pueden transmitir en una sola dirección al mismo tiempo. Algunos estándares permiten sólo operaciones asíncronas y otros síncronas o asíncronas con el mismo módem. Veamos los tipos de modulación mas frecuentes:

Tipos y Características

a) Bell 103. Especificación del sistema Bell para un módem de 300 baudios, asíncrono y full-duplex

b) Bell 201. Especificación del sistema Bell para un módem de 2400 BPS, síncrono, y full-duplex.

c) Bell 212. Especificación del sistema Bell para un módem de 2400 BPS, asíncrono, y full-duplex.

d) Hayes Express. Módem de 4800/9600 BPS, síncrono/asíncrono y half-duplex. Sólo compatibles consigo mismo aunque los más modernos soportan V.32
USR-HST. Módem de USRobotics de 9600/14400 BPS. Sólo compatibles consigo mismo aunque los más modernos soportan V.32 y V.32bis.

e) Vfast Vfast. Es una recomendación de la industria de fabricantes de módem. La norma Vfast permite velocidades de transferencia de hasta 28.800 bps V34 estándar del CCITT para comunicaciones de módem en velocidades de hasta 28.800 bps

5.1.3.3 Codificación de la información

La información de la computadora se codifica siempre en unos y ceros, que como se ha visto, son los valores elementales que la computadora es capaz de reconocer. La combinación de 1 y 0 permite componer números enteros y números reales. Los caracteres se representan utilizando una tabla de conversión. La más común de estas tablas es el código ASCII que utilizan las computadoras personales. Sin embargo existen otras y por ejemplo las grandes computadoras de IBM utilizan el código EBCDIC. La información codificada en binario se transmite entre las computadoras. En las conexiones por módem los bits se transmiten de uno en uno siguiendo el proceso descrito en el apartado modulación de la información. Pero además de los códigos originales de la información, los equipos de comunicación de datos añaden bits de control que permiten detectar si ha habido algún error en la transmisión. Los errores se deben principalmente a ruido en el canal de transmisión que provoca que algunos bits se malinterpreten. La forma más común de evitar estos errores es añadir a cada palabra (conjunto de bits) un bit que indica si el número de 1 en la palabra es par o impar. Según sea lo primero o lo segundo se dice que el control de paridad es par o impar. Este simple mecanismo permite detectar la mayor parte de errores que aparecen durante la transmisión de la información. La información sobre longitud de la palabra (7 u 8 bits) y tipo de paridad (par o impar) es básica en la configuración de los programas de comunicaciones. Otro de los parámetros necesarios son los bits de paro. Los bits de paro indican al equipo que recibe que la transmisión se ha completado. (Los bits de paro pueden ser uno o dos).

Estándares De Control De Errores

El problema de ruido puede causar perdidas importantes de información en módem a velocidades altas, existen para ello diversas técnicas para el control de errores. Cuando se detecta un ruido en un módem con control de errores, todo lo que se aprecia es un momento de inactividad o pausa en el enlace de la comunicación, mientras que si el módem no tiene control de errores lo que ocurre ante un ruido es la posible aparición en la pantalla de caracteres "basura" o, si se esta transfiriendo un fichero en ese momento, esa parte del fichero tuviese que retransmitirse otra vez. En algunos casos el método de control de errores está ligado a la técnica de modulación, como se muestra en los siguientes ejemplos:

a) Módem Hayes V-Serie emplea modulación Hayes Express y un esquema de control errores llamado Link Access Procedure-Modem (LAP-M).

b) Modem US Robotics con protocolo HTS emplea una modulación y control de errores propios de US Robotics

Estándares de Compresión de Datos

La compresión de datos observa bloques repetitivos de datos y los envía al módem remoto en forma de palabras codificadas. Cuando el otro módem recibe el paquete lo decodifica y forma el bloque de datos original. Hay dos técnicas para la compresión muy extendidas:

a) Microcom Network Protocol (MNP-5, 7).

Este protocolo permite compresiones de dos a uno, es decir podemos enviar el doble de información utilizando la misma velocidad de modulación.

b) Norma V.42 bis (procedente del CCITT).

Con esta norma de compresión se consiguen ratios de 4:1. Estas tasas son las máximas que se pueden conseguir. Las mejores tasas se consiguen con ficheros de tipo texto o gráficos generados por computadora. Sí la información esta ya comprimida con alguna utilidad tipo arj o zip, estos protocolos no pueden comprimir más la información y en estos casos incluso se pierde capacidad. Sí se envía información ya comprimida en la computadora, el módem ya no podrá comprimirla más, y en estos casos los protocolos de compresión perjudican el rendimiento del módem.

Control de flujo

El control de flujo es un mecanismo por el cual módem y computadora gestionan los intercambios de información. Estos mecanismos permiten detener el flujo cuando uno de los elementos no puede procesar más información y reanudar el proceso en cuanto vuelve a estar disponible. Los métodos más comunes de control de flujo son:

a) Control de flujo hardware RTS y CTS permiten al PC y al módem parar el flujo de datos que se establece entre ellos de forma temporal.

Este sistema es el más seguro y el que soporta una operación adecuada a altas velocidades. Control de flujo software: XON/XOFF Aquí se utilizan para el control dos caracteres especiales XON y XOFF (en vez de las líneas hardware RTS y CTS) que controlan el flujo. Cuando el PC quiere que el módem pare su envío de datos, envía XOFF. Cuando el PC quiere que el módem le envíe más datos, envía XON. Los mismos caracteres utilizan el módem para controlar los envíos del Pc. Este sistema no es adecuado para altas velocidades.
b) Comandos de control del módem.

La mayoría de los módem se controlan y responden a caracteres enviados a través del puerto serie. El lenguaje de comandos para módem más extendido es de los comandos Hayes que fue inicialmente incorporado a los modems de este fabricante.

5.1.3.4 Modos de operación del módem

Modo de comandos.

En este modo el módem responde a los comandos que envía la computadora y es posible configurar el módem o realizar las operaciones de marcado y conexión. Antes de que se puedan enviar un comando al módem este debe estar en el "estado de comandos".

Modo en línea.

Este modo se alcanza cuando el módem se conecta con otro módem. En este modo cualquier información que reciba de la computadora será enviada al módem distante. En este modo el módem no procesa la información y simplemente la trasmite a través de la línea de comunicación. Para salir del modo en línea y pasar de nuevo al modo comandos se envía al módem +++ (petición de atención) precedidos por un segundo de inactividad.

Comandos de Hayes más simples:

ATH dice al módem que cuelgue el teléfono
ATDT dice al módem que marque un número de teléfono determinado empleando la marcación por tonos
ATDP lo mismo que ATDT pero la marcación es por pulsos
Los comandos comienzan con las letras AT y siguen con las letras del alfabeto (A...Z). A medida que los módem se hicieron más complicados, surgió la necesidad de incluir mas comandos, son los comandos extendidos y tienen la forma AT&X (por ejemplo), donde el "&" marca la "X" como carácter extendido.

Códigos de resultados

Cuando envía un comando al módem, este responde con un código de resultado: "CONNECT", "OK" o "ERROR".
ATV determina el tipo de código de resultado que aparecerá:
ATV0 respuesta numérica
ATV1 respuesta de palabras
ATQ1 inhibe los códigos de resultado, pone el módem en "estado silencioso"
ATQ0 habilita los códigos de resultado, desconecta el modo silencioso

Desarrollo de una conexión a través de Módem

En la conexión participan dos computadoras con sus respectivos módem que se encuentran conectados a la red telefónica. En la computadora que origina la conexión, el usuario trabaja sobre un programa de comunicaciones que le permite actuar sobre el módem. Cuando un módem llama a otro este comienza la secuencia de acontecimientos que se describe a continuación.

1. Selecciona "dial" en el menú del programa o teclea en la línea de comandos. Pone a ON la señal DTR y envía al módem el comando de marcación ATDT 055El módem conecta el altavoz, descuelga la línea, espera el tono de llamada y marca el número de teléfono.

2. Comienza observando los códigos de resultados del módem. Espera una respuesta durante tiempo según configuración del registro S7.

3. La línea de teléfono suena.

4. El módem detecta la llamada, y contesta situando el tono de respuesta en línea.

5. El módem detecta el modo de respuesta y sitúa la portadora de comienzo en línea.

6. Los módems se ponen de acuerdo en la modulación y velocidad a utilizar.

7. Los módems determinan la técnica de compresión y control de errores a utilizar Los módems determinan la técnica de compresión y control de errores a utilizar.

8. Envía el código de rtdo. "connet" al PC, apaga el altavoz, y pone a ON la señal CD.

9. Detecta el código de rtdo. y/o la señal CD; Informa al usuario que la conexión está establecida.

10. Comienza la comunicación con el host. Gestiona la sesión de comunicaciones; vigila la pérdida de portadora monitorizando la señal CD. Envía y recibe datos.

11. Completa la sesión de comunicaciones y selecciona el comando "disconnect". Pone a OFF la señal DTR, o envía +++ seguidos por ATH.

12. Cuelga el teléfono. Detecta la pérdida de portadora y cuelga.

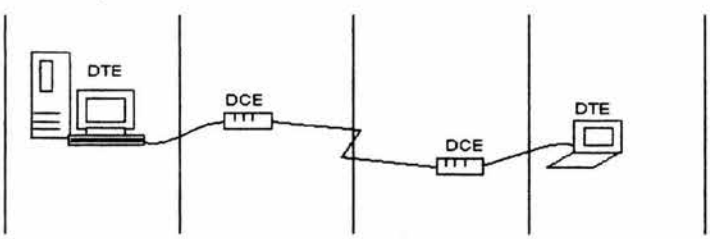


Figura 5.4 Conexión entre dos computadoras por medio del uso de módems

5.1.4 Pasarela (Gateway)

Estos dispositivos están pensados para facilitar el acceso entre sistemas o entornos soportando diferentes protocolos. Operan en los niveles más altos del modelo de referencia OSI (nivel de transporte, sesión, presentación y aplicación) y realizan conversión de protocolos para la interconexión de redes con protocolos de alto nivel diferentes. Las pasarelas incluyen los 7 niveles del modelo de referencia OSI, y aunque son más caros que un puente o un ruteador, se pueden utilizar como dispositivos universales en una red corporativa compuesta por un gran número de redes de diferentes tipos. Las pasarelas tienen mayores capacidades que los ruteadores y los puentes porque no sólo conectan redes de diferentes tipos, sino que también aseguran que los datos de una red que transportan son compatibles con los de la otra red.

Conectan redes de diferentes arquitecturas procesando sus protocolos y permitiendo que los dispositivos de un tipo de red puedan comunicarse con otros dispositivos de otro tipo de red.

Tipos de pasarelas.

A continuación se describen algunos tipos de pasarelas:

a) Pasarela asíncrona.

Sistema que permite a los usuarios de computadoras personales acceder a grandes computadoras (mainframes) asíncronos a través de un servidor de comunicaciones, utilizando líneas telefónicas conmutadas o punto a punto. Generalmente están diseñados para una infraestructura de transporte muy concreta, por lo que son dependientes de la red.

b) Pasarela SNA.

Permite la conexión a grandes computadoras con arquitectura de comunicaciones SNA (System Network Architecture, Arquitectura de Sistemas de Red), actuando como terminales y pudiendo transferir ficheros o listados de impresión.

c) Pasarela TCP/IP.

Estos gateways proporcionan servicios de comunicaciones con el exterior vía RAL o WAN y también funcionan como interfaz de cliente proporcionando los servicios de aplicación estándares de TCP/IP.

d) Pasarela PAD X.25

Son similares a los asíncronos; la diferencia está en que se accede a los servicios a través de redes de conmutación de paquetes X.25.

e) Pasarela FAX

Los servidores de Fax proporcionan la posibilidad de enviar y recibir documentos de fax.

5.1.5 Puente (Bridge)

Son elementos inteligentes, constituidos como nodos de la red, que conectan entre sí dos subredes, transmitiendo de una a otra el tráfico generado no local. Al distinguir los tráficos locales y no locales, estos elementos disminuyen el mínimo total de paquetes circulando por la red por lo que, en general, habrá menos colisiones y resultará más difícil llegar a la congestión de la red. Operan en el nivel de enlace del modelo de referencia OSI, en el nivel de trama MAC (Medium Access Control, Control de Acceso al Medio) y se utilizan para conectar o extender redes similares, es decir redes que tienen protocolos idénticos en los dos niveles inferiores OSI, (como es TokenRing con TokenRing, Ethernet con Ethernet, etc) y conexiones a redes de área extensa. Se encargan de filtrar el tráfico que pasa de una a otra red según la dirección de destino y una tabla que relaciona las direcciones y la red en que se encuentran las estaciones asignadas. Las redes conectadas a través de un puente aparentan ser una única red, ya que realizan su función transparentemente; es decir, las estaciones no necesitan conocer la existencia de estos dispositivos, ni siquiera si una estación pertenece a uno u otro segmento.

Figura 5.5 Puente Aironet 350 Series de Cisco

Un puente ejecuta tres tareas básicas:

a) Aprendizaje de las direcciones de nodos en cada red.
b) Filtrado de las tramas destinadas a la red local.
c) Envío de las tramas destinadas a la red remota.

Tipos de Puentes.

Los puentes se dividen según el tipo de enlace a realizar en:

a) Locales: sirven para enlazar directamente dos redes físicamente cercanas.

b) De área extensa: se conectan en parejas, enlazando dos o más redes locales, formando una red de área extensa, a través de líneas telefónicas.

Además de esta se puede realizar otra división de los bridges en función de la técnica de filtrado y envío (bridging), la cual se describe a continuación:

a) Spanning Tree Protocol Bridge o Transparent Protocol Bridge (Protocolo de Arbol en Expansión o Transparente, STP).

Estos puentes deciden qué paquetes se filtran en función de un conjunto de tablas de direcciones almacenadas internamente. Su objetivo es evitar la formación de lazos entre las redes que interconecta. Se emplea normalmente en entornos Ethernet.

b) Source Routing Protocol Bridge (Bridge de Protocolo de Ruteamiento por Emisor, SRP).

El emisor ha de indicar al puente cuál es el camino a recorrer por el paquete que quiere enviar. Se utiliza normalmente en entornos TokenRing.
Source Routing Transparent Protocol Bridge (Puente de Protocolo de Ruteamiento por Emisor Transparente, SRTP).
Este tipo de puentes pueden funcionar en cualquiera de las técnicas anteriores.

Ventajas de la utilización de puentes:

a) Fiabilidad. Utilizando puentes se segmentan las redes de forma que un fallo sólo imposibilita las comunicaciones en un segmento.

b) Eficiencia. Segmentando una red se limita el tráfico por segmento, no influyendo el tráfico de un segmento en el de otro.

c) Seguridad. Creando diferentes segmentos de red se pueden definir distintos niveles de seguridad para acceder a cada uno de ellos, siendo no visible por un segmento la información que circula por otro.

d) Dispersión. Cuando la conexión mediante repetidores no es posible debido a la excesiva distancia de separación, los puentes permiten romper esa barrera de distancias.

Desventajas de los puentes:

a) Son ineficientes en grandes interconexiones de redes, debido a la gran cantidad de tráfico administrativo que se genera.
b) Pueden surgir problemas de temporización cuando se encadenan varios puentes.
c) Pueden aparecer problemas de saturación de las redes por tráfico de difusión.

5.2 MECANISMOS DE SEGURIDAD

Los modernos sistemas de seguridad en transacciones a través de redes están basados en el uso de Infraestructuras de clave pública, basadas en un conjunto de elementos como certificados digitales, criptografía simétrica y de clave pública, firmas digitales, listas de certificados revocados, muros de fuego etc, que garantizan el cumplimiento de los 4 pilares de las comunicaciones seguras.

5.2.1 Requisitos para una comunicación segura.

Para que una comunicación entre dos entidades sea segura se deben cumplir los cuatro requisitos principales:

Autenticidad

Todas las entidades participantes en la transacción deben estar perfecta y debidamente identificadas antes de comenzar la misma. Debemos estar seguros de que la persona con la que nos comunicamos es realmente quién dice ser, ya que si no podemos estar facilitando datos íntimos y/o sensibles a una persona o entidad no deseada, que puede hacer con ellos luego lo que le venga en gana.

En las comunicaciones "normales" entre dos personas casi siempre se dispone alguna forma de comprobación de la Autenticidad. Si hablamos en directo con alguien, sabemos quién es, y si no lo sabemos podemos poner límites a la información que le facilitamos. En una conversación telefónica podemos oír la voz de nuestro interlocutor, y si lo conocemos bien es muy difícil que otra persona se pueda hacer pasar por él.

La Autenticidad se consigue mediante el uso de los certificados y firmas digitales.

Confidencialidad:

Debemos estar seguros de que los datos que enviamos no pueden ser leídos por otra persona distinta del destinatario final deseado, o que si ocurre esto, el espía no pueda conocer el mensaje enviado. O en su defecto, que cuando consiga obtener los datos éstos ya no le sirvan para nada. Es decir, debemos estar seguros de que ninguna persona ajena a la transacción puede tener acceso a los datos de la misma. Imaginemos ahora que trabajamos en una empresa y deseamos enviar un correo al director general explicándole el fabuloso contrato que estamos a punto de firmar con un cliente.

Si nuestro pirata de turno está a la escucha, puede conocer al momento todos los detalles del trato que vamos a realizar, pudiendo vender esa información a la competencia, lo que nos puede arruinar el negocio antes de hacerse realidad (¿qué impresión le causaría a nuestro cliente si recibiera información detallada de sus actividades con nosotros por medio de un correo anónimo?). Lo ideal en este aspecto sería que las entidades implicadas en la transacción no llegaran a conocer más que los datos imprescindibles para realizar su función. La confidencialidad se consigue en las transacciones electrónicas con el uso de la Criptografía.

Integridad:

Es necesario estar seguro de que los datos que enviamos llegan íntegros, sin modificaciones, a su destino final. En este caso estamos realizando el pedido de una computadora a una tienda virtual, introducimos nuestro número de tarjeta de crédito y nuestra dirección de entrega del equipo. Pero nuestro simpático pirata está a la escucha, intercepta el envío, cambia los datos de la dirección por otros a su gusto y deja que continúe el envío. El resultado será que nuestro amigo disfrutará de una computadora que hemos pagado nosotros. La integridad se consigue combinando Criptografía, funciones hash y firmas digitales.

No repudio:

Debemos estar seguros de que una vez enviado un mensaje con datos importantes o sensibles el destinatario de los mismos no pueda negar el haberlos recibido. Y en una compra on-line debe garantizarse que una vez finalizada la misma ninguna de las partes que intervienen pueda negar haber participado en ella. Vamos entonces a imaginar que nuestra empresa tiene que enviar un presupuesto antes de una fecha determinada, presupuesto que debe ser recogido por un empleado de otra empresa, y que éste olvida comunicar a sus superiores la recepción del presupuesto. Pasa el plazo y el contrato que esperábamos se lo dan a otra empresa, alegando que no han recibido a tiempo el presupuesto nuestro. Si no disponemos de un medio para atestiguar que el mensaje fue entregado en plazo, nos quedaremos sin contrato y sin poder reclamar. Lo ideal sería que al finalizar la transacción quedara algo equivalente a un recibo de compra o factura firmado por todas las partes implicadas. El no repudio se consigue mediante los certificados y la firma digital.

5.2.2 Certificados digitales.

Para solucionar el problema de la autentificación en las transacciones por Internet se buscó algún sistema identificación única de una entidad o persona. Ya existían los sistemas criptográficos de clave asimétrica, mediante los cuales una persona disponía de dos claves, una pública, al alcance de todos, y otra privada, sólo conocida por el propietario. Cuando deseamos enviar un mensaje confidencial a otra persona, debemos cifrarlo con su clave pública, y así estaremos seguros de que sólo el destinatario correcto podrá leer el mensaje en claro, el problema era estar seguro de que efectivamente la clave pública que nos envían sea de la persona correcta, y no de un suplantador. Entonces se pensó en implementar una especie de documento de identidad electrónica que identificara sin dudas a su emisor. La solución a este problema la trajo la aparición de los certificados digitales o certificados electrónicos, documentos electrónicos basados en la criptografía de clave pública y en el sistema de firmas digitales. La misión principal de un certificado Digital es garantizar con toda confianza el vínculo existente entre una persona, entidad o servidor web con una pareja de claves correspondientes a un sistema criptográfico de clave pública. Un certificado digital es un documento electrónico que contiene datos identificativos de una persona o entidad (empresa, servidor web, etc.) y la llave pública de la misma, haciéndose responsable de la autenticidad de los datos que figuran en el certificado otra persona o entidad de confianza, denominada autoridad certificadora. Las principales Autoridades certificadoras actuales son Verisign (filial de RSA Data Security Inc.) y Thawte.

El formato de los certificados digitales es estándar, siendo X.509 v3 el recomendado por la Unión Internacional de Comunicaciones (ITU) y el que está en vigor en la actualidad. El aspecto de los certificados X.509 v3 es el siguiente:

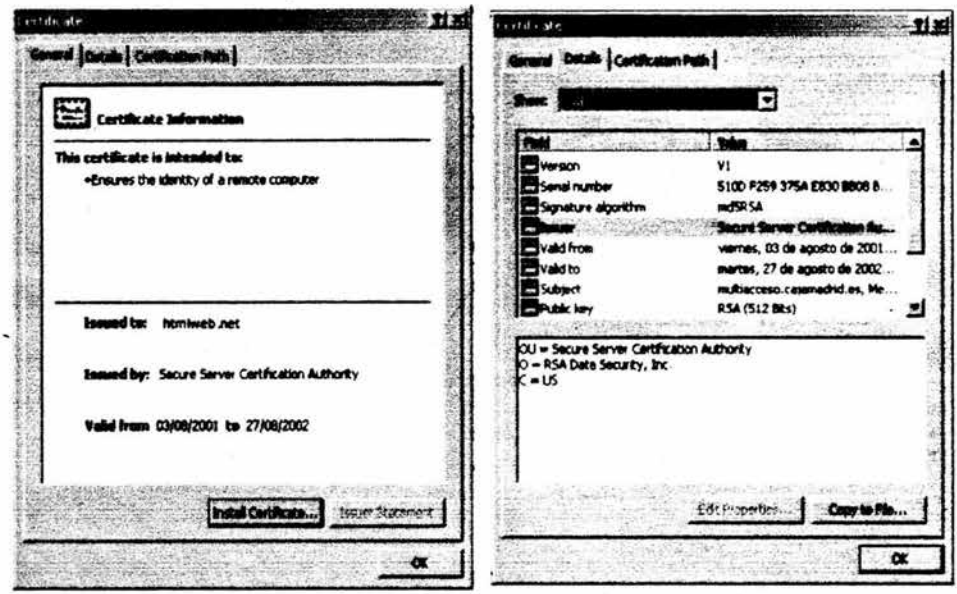


Figura 5.6 Ejemplo de un certificado X.509 v3

Los datos que figuran generalmente en un certificado son:

1. Versión: versión del estándar X.509, generalmente la 3, que es la más actual.

2. Número de serie: número identificador del certificado, único para cada certificado expedido por una AC determinada.

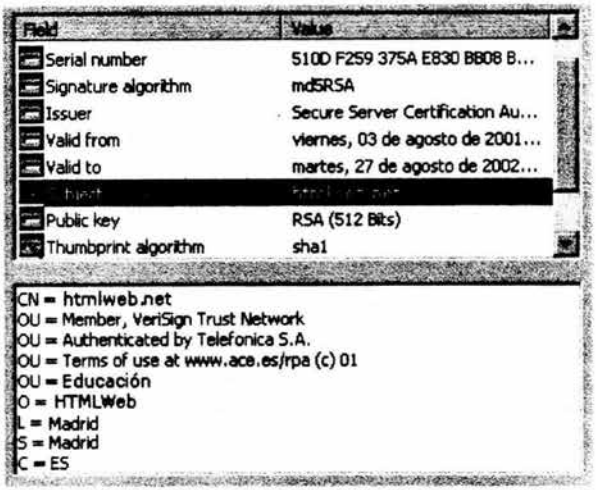
3. Algoritmo de firma: algoritmo criptográfico usado para la firma digital.

4. Autoridad certificadora: datos sobre la autoridad que expide el certificado.

5. Fechas de inicio y de fin de validez del certificado. Definen el periodo de validez del mismo, que generalmente es de un año.

6. Propietario: persona o entidad vinculada al certificado. Dentro de este apartado se usan una serie de abreviaturas para establecer datos de identidad.

Un ejemplo sería:



CN	nombre común del usuario
OU	información varia
O	Organización
L	Ciudad
S	estado (provincia)
C	País
E	correo electrónico
UID	ID de usuario

Figura 5.7 Datos de identidad

7. Llave pública: representación de la llave pública vinculada a la persona o entidad (en hexadecimal), junto con el algoritmo criptográfico para el que es aplicable.

8. Algoritmo usado para la misma para obtener la firma digital de la autoridad certificadora.

9. Firma de la autoridad certificadora, que asegura la autenticidad del mismo.

10. Información adicional, como tipo de certificado, etc.

El problema que se plantea ahora es: si la autoridad certificadora avala los datos del certificado ¿Quién avala a la autoridad certificadora? Para solventar esto se han creado una serie de entidades autorizadas a emitir certificados, de tal forma que éstas a su vez son avaladas por otras entidades de mayor confianza, hasta llegar a la cabeza de la jerarquía, en la que figuran unas pocas entidades de reconocido prestigio y confianza, como Verisign, que se auto firman su certificado. Cada certificado emitido por una AC debe estar firmado por una AC de mayor grado en el esquema jerárquico de autoridades certificadoras, formándose así una cadena de certificados, en los que unas AC se avalan a otras hasta llegar a la AC superior, que se avala a sí misma. La jerarquía de firmas y la cadena con ella formada están contempladas en el estándar X.509 v3, que indica la forma correcta de realizar estas cadenas de certificaciones.

El certificado Digital vincula pues indisolublemente a una persona o entidad con una llave pública, y mediante el sistema de firma digital se asegura que el certificado que recibimos es realmente de la persona que consta en el mismo. El sistema de firma digital liga un documento digital con una clave de cifrado.

Tipos de certificados

Dependiendo del uso que se vaya a dar al certificado y de qué persona o entidad lo solicita, las autoridades certificadoras han dividido los certificados en varios tipos. Del tipo de certificado a emitir van a depender las medidas de comprobación de los datos y el precio del mismo.

Los certificados, según las comprobaciones de los datos que se realizan, se dividen en cuatro clases:

a) Certificados de Clase 1:

Corresponde a los certificados más fáciles de obtener e involucran pocas verificaciones de los datos que figuran en él: sólo el nombre y la dirección de correo electrónico del titular.

b) Certificados de Clase 2:

En los que la autoridad certificadora comprueba además el permiso de conducir, el número de la Seguridad Social y la fecha de nacimiento.

c) Certificados de Clase 3:

En la que se añaden a las comprobaciones de la clase 2 la verificación de crédito de la persona o empresa mediante un servicio como Equifax.

d) Certificados de Clase 4:

Que a todas las comprobaciones anteriores suma la verificación del cargo o la posición de una persona dentro de una organización (todavía no formalizados los requerimientos; está en estudio).

Desde el punto de vista de la finalidad, los certificados electrónicos se dividen en:

a) Certificados SSL para cliente.

Usados para identificar y autenticar a clientes ante servidores en comunicaciones mediante el protocolo Secure Socket Layer (SSL), y se expiden normalmente a una persona física, bien un particular, bien un empleado de una empresa.

b) Certificados SSL para servidor:

Usados para identificar a un servidor ante un cliente en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden generalmente a nombre de la empresa propietaria del servidor seguro o del servicio que éste va a ofrecer, vinculando también el dominio por el que se debe acceder al servidor. La presencia de éste certificado es condición imprescindible para establecer comunicaciones seguras SSL.

c) Certificados S/MIME:

Usados para servicios de correo electrónico firmado y cifrado, que se expiden generalmente a una persona física. El mensaje lo firma digitalmente el remitente, lo que proporciona autenticación, integridad y no rechazo. También se puede cifrar el mensaje con la llave pública del destinatario, lo que proporciona Confidencialidad al envío.

d) Certificados de firma de objetos:

Usados para identificar al autor de ficheros o porciones de código en cualquier lenguaje de programación que se deba ejecutar en red (Java, JavaScript, CGI, etc.). Cuando un código de éste tipo puede resultar peligroso para el sistema del usuario, el navegador lanza un aviso de alerta, en el que figurará si existe certificado que avale al código, con lo que el usuario puede elegir si confía en el autor, dejando que se ejecute el código, o si por el contrario no confía en él, con lo que el código será rechazado.

e) Certificados para AC:

Que identifican a las propias autoridades certificadoras, y es usado por el software cliente para determinar si pueden confiar en un certificado cualquiera, accediendo al certificado de la AC y comprobando que ésta es de confianza.

Toda persona o entidad que deseé obtener un certificado debe pagar una cuota a las autoridades de certificación, cuota que irá en función de la clase del certificado y del uso que se le vaya a dar al mismo (ambas están relacionadas). A mayor nivel de comprobación de datos (clase mayor), más costará el certificado.

5.2.3 Listas de Certificados Revocados. (CRL)

Para llevar un control de los certificados revocados (no válidos) las autoridades de certificación han implementado unos servidores especiales que contienen bases de datos en las que figuran los certificados anulados, que se conocen con el nombre de lista de certificados revocados, (CRL; Certificate Revoked List). Un CRL es pues un archivo, firmado por la autoridad certificadora, que contiene la fecha de emisión del mismo y una lista de certificados revocados, figurando para cada uno de ellos su número de identificación y la fecha en que ha sido revocado. Cuando nuestro software de seguridad recibe un certificado digital de otra persona o entidad comprueba antes de darlo por bueno si dicho certificado se encuentra en la lista más actualizada de certificados revocados. Si está en la lista, el certificado será rechazado. Ahora bien, imaginemos que recibimos un certificado como medio de autentificación en una transacción, nuestro software comprueba que no está revocado en la última CRL y lo da por válido, pero resulta que al día siguiente aparece como revocado en la CRL nueva. En estos casos deberemos poder demostrar de algún modo que hemos recibido el certificado antes de que se produjera la actualización. Para solucionar este tipo de situaciones existen los documentos digitales denominados recibos. Un recibo es un documento firmado digitalmente por una persona o entidad de confianza, llamada autoridad de oficialía de partes, que añade la fecha actual a los documentos que recibe para su certificación, firmando luego el resultado con su llave privada. De esta forma los usuarios disponen de un documento que atestigua la hora y fecha exacta en la que envía o recibe un certificado digital u otro documento electrónico cualquiera. Resumiendo, mediante la consulta a una lista de certificados revocados y un recibo de una autoridad de oficialía de partes disponemos de pruebas suficientes para considerar cualquier transacción realizada sobre la base de certificados digitales como segura (por lo menos en el sentido de autenticación). El uso de un CRL en un proceso de Autentificación presenta varios problemas adicionales. En primer lugar sólo podemos considerarlo válido cuando la fecha del mismo es igual o posterior a la que queremos usar como referencia en la validez del documento, y en segundo lugar, también puede resultar inadecuado en aquellas operaciones que exijan una velocidad alta en la transacción, sobre todo si el CRL a consultar tiene un tamaño muy grande

5.2.4 Firmas digitales

El procedimiento de firma digital lo que hace es obtener un resumen de un documento o de un texto aleatorio y cifrarlo con llave privada del propietario del certificado. Cuando nos llega un certificado, y su firma digital asociada, tan sólo debemos obtener nosotros el resumen el mismo, descifrar la firma con la llave pública del remitente y comprobar que ambos resúmenes coinciden, lo que nos hace estar totalmente seguros de la autenticidad del certificado. Se firma un resumen del documento y no el documento mismo para evitar ataques contra el sistema de cifrado RSA (por ejemplo, encriptar un documento especialmente concebido por un pirata, con lo que éste podría llegar a obtener la llave privada) y para no hacer el proceso demasiado lento.

Figura 5.8 Firma Digital con resumen hash

Para obtener el resumen del documento se utilizan las funciones hash o de resumen, algoritmos criptográficos muy rápidos, de uso público e irreversibles (de un sólo sentido). Son funciones de dispersión que no usan ninguna clave, y que transforman el mensaje original en una cadena de dígitos de longitud fija (generalmente de entre 16 y 128 bits).

5.2.5 Capa de Seguridad (Secure Socket Layer)

Como vimos al principio del tema, toda transacción segura por la red debe contemplar los aspectos de autenticidad, integridad, confidencialidad y no repudio. Son varios los sistemas y tecnologías que se han desarrollado para intentar implementar estos aspectos en las transacciones electrónicas, siendo sin duda SSL el más conocido y usado en la actualidad. SSL permite la confidencialidad y la autentificación en las transacciones por Internet, siendo usado principalmente en aquellas transacciones en la que se intercambian datos sensibles, como números de tarjetas de crédito o contraseñas de acceso a sistemas privados. SSL es una de las formas base para la implementación de soluciones PKI (Infraestructuras de Clave Pública).

Secure Socket Layer es un sistema de protocolos de carácter general diseñado en 1994 por la empresa Nestcape Communcations Corporation, y está basado en la aplicación conjunta de criptografía simétrica, criptografía asimétrica (de llave pública), certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet. De los sistemas criptográficos simétricos, motor principal de la encriptación de datos transferidos en la comunicación, se aprovecha la rapidez de operación, mientras que los sistemas asimétricos se usan para el intercambio seguro de las claves simétricas, consiguiendo con ello resolver el problema de la Confidencialidad en la transmisión de datos.

SSL implementa un protocolo de negociación para establecer una comunicación segura a nivel de socked (nombre de máquina más puerto), de forma transparente al usuario y a las aplicaciones que lo usan.

Actualmente es el estándar de comunicación segura en los navegadores web más importantes (protocolo HTTP), como Nestcape Navigator e Internet Explorer, y se espera que pronto se saquen versiones para otros protocolos de la capa de aplicación (correo, FTP, etc.).

La identidad del servidor web seguro (y a veces también del usuario cliente) se consigue mediante el certificado digital correspondiente, del que se comprueba su validez antes de iniciar el intercambio de datos sensibles (Autenticación), mientras que de la seguridad de Integridad de los datos intercambiados se encarga la firma digital mediante funciones hash y la comprobación de resúmenes de todos los datos enviados y recibidos.

Desde el punto de vista de su implementación en los modelos de referencia OSI y TCP/IP, SSL se introduce como una especie de nivel o capa adicional, situada entre la capa de aplicación y la capa de transporte, sustituyendo los sockets del sistema operativo, lo que hace que sea independiente de la aplicación que lo utilice, y se implementa generalmente en el puerto 443. (NOTA: Los puertos son las interfases que hay entre las aplicaciones y la pila de protocolos TCP/IP del sistema operativo).

Figura 5.9 Implementación del SSL.

SSL proporciona servicios de seguridad a la pila de protocolos, encriptando los datos salientes de la capa de Aplicación antes de que estos sean segmentados en la capa de Transporte y encapsulados y enviados por las capas inferiores. Es más, también puede aplicar algoritmos de compresión a los datos a enviar y fragmentar los bloques de tamaño mayor a 2^{14} bytes, volviéndolos a reensamblarlos en el receptor. La versión más actual de SSL es la 3.0. que usa los algoritmos simétricos de encriptación DES, triple DES, RC2, RC4 e IDEA, el asimétrico RSA, la función hash MD5 y el algoritmo de firma SHA-1.

Protocolos de Capa de Seguridad (Secure Socket Layer).-

Para establecer una comunicación SSL es necesario que previamente el cliente y el servidor realicen un proceso de reconocimiento mutuo y de petición de conexión que, al igual que en otros tipos de comunicaciones, recibe el nombre de apretón de manos o Handshake, que en este caso está controlado por el protocolo SSL Handshake, que se encarga de establecer, mantener y finalizar las conexiones SSL. Durante el mismo se negocian los parámetros generales de la sesión y los particulares de cada conexión. Concretamente, y de forma general, el protocolo comienza con el saludo del cliente al servidor, conocido como Client Hello, por el que se informa al servidor de que se desea establecer una comunicación segura con él. SSL soporta solicitudes de conexión por puertos diferentes al utilizado normalmente para este servicio. Junto con este saludo inicial, el cliente envía al servidor información de la versión de SSL que tiene implementada, de los algoritmos de encriptación que soporta, las longitudes de clave máximas que admite para cada uno de ellos y las funciones hash que puede utilizar. También se le solicita al servidor el envío de su certificado digital X.509 v3, con objeto de verificar el cliente la identidad del mismo y recoger su clave pública. En este momento se asigna un identificador a la sesión y se hace constar la hora y fecha de la misma. Como medida adicional, el cliente envía asimismo una clave numérica aleatoria, para que se pueda establecer una comunicación segura mediante otros protocolos o algoritmos en el caso de que el servidor web no posea un certificado digital. En este paso no se intercambia en ningún momento información sensible, tan sólo información necesaria para establecer la comunicación segura. A continuación, el servidor SSL responde al cliente en el proceso que se conoce con el nombre de Server Hello, enviándole su certificado digital (con su llave pública) e informándole de su versión de SSL, de los algoritmos y longitudes de clave que soporta. Generalmente se obtiene el conjunto de algoritmos, longitudes de clave y funciones hash soportados por ambos, eligiéndose entonces los más fuertes. Si no hay acuerdo con los algoritmos a usar se envía un mensaje de error. A veces, y si la comunicación posterior así lo exige, el servidor solicita al cliente su certificado digital, en el mensaje llamado CertificateRequest. Esto sólo suele ocurrir en SSL cuando los datos a transferir sean especialmente sensibles y precisen la previa autenticación del cliente. Si es el caso, el cliente debe contestar al servidor mediante el mensaje CertificateVerify, enviándole entonces su certificado. En este momento el cliente verifica la validez del certificado Digital del servidor, desencriptando el resumen del mismo y comprobando su corrección, verificando que ha sido emitido por una autoridad certificadora de confianza, que esté correctamente firmado por ella y que el certificado no esté revocado. También se comprueba que la fecha actual está dentro del rango de fechas válidas para el certificado y que el dominio (URL) que aparece en el certificado se corresponde con el que se está intentando establecer la comunicación segura. Si alguna de estas validaciones falla, el navegador cliente rechazará la comunicación, dándola por finalizada e informando al usuario del motivo del rechazo.

En caso de que el servidor no tenga un certificado X.509 v3 se puede utilizar un mensaje ServerKeyExchange para enviar la clave pública sin certificado, en cuyo caso queda en manos del cliente la elección de si acepta la llave o no, lo que finalizaría el proceso. Como medida adicional de seguridad, el cliente genera una clave aleatoria temporal y se la envía al servidor, que debe devolvérsela cifrada con su clave privada. El cliente la descifra con la llave pública y comprueba la coincidencia, con lo que está totalmente seguro de que el servidor es quién dice ser. Y un proceso análogo a éste, pero en sentido inverso, se requiere si es necesaria la autenticación del usuario ante el servidor. Si todo está correcto el cliente genera un número aleatorio que va a servir para calcular una clave de sesión correspondiente al algoritmo de encriptación simétrico negociado antes, conocida con el nombre de clave maestra, que es enviada al servidor de forma segura encriptándola asimétricamente con la llave pública del mismo que aparece en el certificado Digital. Esta clave maestra se usará para generar todas las claves y números secretos utilizados en SSL. Con esto servidor y cliente se han identificado y tienen en su poder todos los componentes necesarios para empezar a transmitir información cifrada simétricamente. Se pasa entonces el control al subprotocolo Change Cipher Spec iniciándose la conexión segura. Así y todo, para que empiecen las transmisiones de datos protegidos se requiere otra verificación previa, denominada Finished, consistente en que cliente y servidor se envían uno al otro una copia de todas las

transacciones llevadas a cabo hasta el momento, encriptándola con la llave simétrica común. Al recibir esta copia, cada host la desencripta y la compara con el registro propio de las transacciones. Si las transacciones de los dos host coinciden significa que los datos enviados y recibidos durante todo el proceso no han sido modificados por un tercero. Se termina entonces la fase Handshake.

Para empezar a transmitir datos cifrados es necesario que cliente y servidor se pongan de acuerdo respecto a la forma común de encapsular los datos que se van a intercambiar, es decir, qué formato de datos se va a usar en la transmisión cifrada. Esto se realiza mediante el Protocolo SSL Record (Protocolo de Registro SSL), que establece tres componentes para la porción de datos del protocolo:

1. MAC-DATA: código de autenticación del mensaje.

2. ACTUAL-DATA: datos de aplicación a transmitir.

3. PADDING-DATA: datos requeridos para rellenar el mensaje cuando se usa un sistema de cifrado en bloque.

El Protocolo de Registro es el encargado de la seguridad en el intercambio los datos que le llegan desde las aplicaciones superiores, usando para ello los parámetros de encriptación y resumen negociados previamente mediante el protocolo SSL Handshake. Sus principales misiones son:

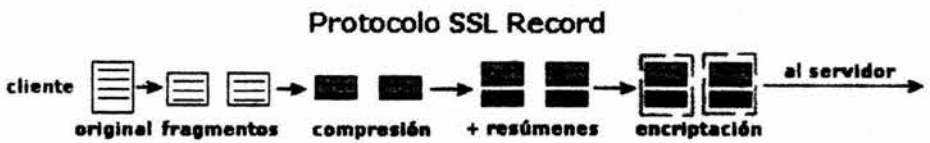


Figura 5.10 Funcionamiento del protocolo de registro.

- La fragmentación de los mensajes mayores de 2^{14} bytes en bloques más pequeños.

- La compresión de los bloques obtenidos mediante el algoritmo de compresión negociado anteriormente.

- La autenticación y la integridad de los datos recibidos mediante el resumen de cada mensaje recibido concatenado con un número de secuencia y un número secreto establecido en el estado de conexión. El resultado de esta concatenación se denomina MAC, y se añade al mensaje. Con esta base, la autenticación se comprueba mediante el número secreto, compartido por el cliente y el servidor, y mediante el número de secuencia, que viaja siempre encriptado. La integridad se comprueba mediante la función hash negociada.

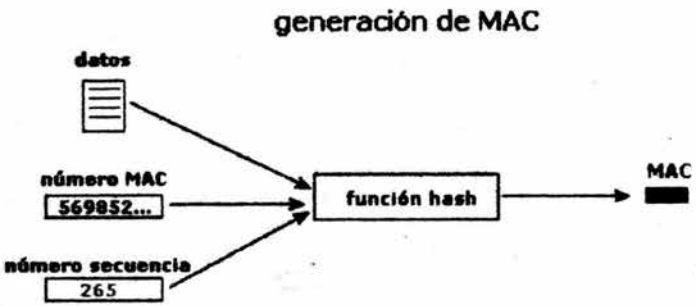


Figura 5.11 Concatenación MAC

La confidencialidad se asegura encriptando los bloques y sus resúmenes mediante el algoritmo simétrico y la clave correspondiente negociadas en la fase Handshake. Existen dos tipos posibles de encriptación:

a). Cifrado en bloque:

Se cifran los datos en bloques de 64 bits. Si el mensaje no es múltiplo de 64 bits se le añaden los bits de relleno necesarios para obtener un número entero de bloques completos, indicándose la adición en el formato del mensaje. Este método de cifrado se conoce con el nombre de Cipher Block Chainning, CBC, y precisa un vector inicial, que habrá sido negociado previamente en la fase Handshake. Como algoritmos de cifrado se usan RC2 y DES.

b). Cifrado Stream:

O de flujo, en el que se encriptan los datos realizando una operación lógica OR-Exclusiva entre los bytes y un generador seudo aleatorio usando el algoritmo RC4.

Tras todos estos requisitos, el canal seguro está listo para empezar la transmisión de datos de forma segura. Cuando el cliente o el servidor desean transmitir algún mensaje al otro se genera automáticamente un resumen del mismo mediante la función hash acordada, se encriptan mensaje y resumen con la clave simétrica acordada y se envían los datos. Cuando el destinatario los recibe, desencripta todo, vuelve a obtener el resumen a partir del original y lo compara con el recibido. Si coinciden hay seguridad de que la comunicación segura se ha producido satisfactoriamente, sin intromisiones externas. Si no coinciden, se pone en conocimiento del otro host, y si es preciso se suspende la conexión SSL. Cada uno de los mensajes enviados por cliente o servidor sufre este proceso de verificación. Por último, cuando la transferencia de mensajes ha finalizado y se desea cerrar la comunicación segura, generalmente porque el cliente así lo desea, la aplicación cliente (el navegador web, p.e.) lanza una ventana de aviso de que se va a cerrar la comunicación SSL, y si es aceptada por el usuario, se sale de la misma y se regresa a una comunicación normal, finalizando el proceso SSL.

5.2.6 Muro de Fuego (Firewall)

Un Muro de Fuego es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El Muro de fuego determina cual de los servicios de red puede ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un muro de fuego sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. Este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

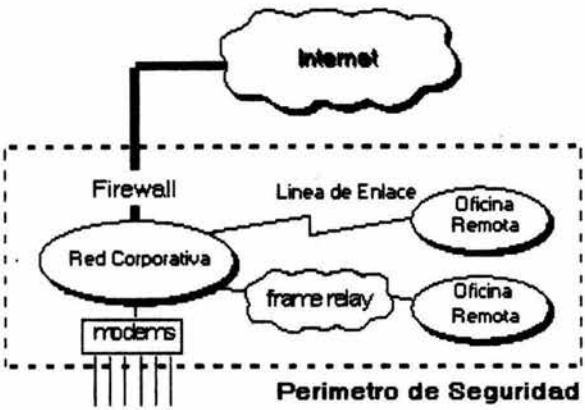


Figura 5.12 Perímetro De Defensa creado por el firewall

Esto es importante, ya que debemos de notar que un muro de fuego no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El muro de fuego es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. 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, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un muro de fuego sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

5.2.6.1 Componentes del sistema Muro de Fuego

Un muro de fuego típico se compone de uno, o una combinación, de los siguientes obstáculos:

a) Ruteador Filtra-paquetes.

b) Pasarela a Nivel-aplicación.

c) Pasarela a Nivel-circuito.

A continuación describiremos 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 muro de fuego de Internet.

Ruteador filtra-paquetes

Este ruteador toma las decisiones de rehusar/permitir el paso de cada uno de los paquetes que son recibidos. El ruteador examina cada diagrama de datos para determinar si este corresponde 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 (TCP, UDP, ICMP, o IP tunnel), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interfase de entrada del paquete, y la interfase 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.

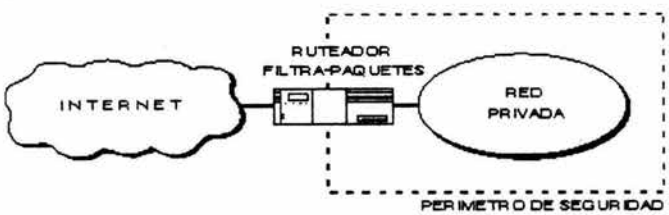


Figura 5.13 Ruteador Filtra-Paquetes.

Algunas características típicas de filtrado que un administrador de redes podría solicitar en un ruteador filtra-paquetes para perfeccionar su funcionamiento serian:

a) Permitir la entrada de sesiones Telnet únicamente a una lista especifica de servidores internos.
b) Permitir la entrada de sesiones FTP únicamente a los servidores internos especificados.
c) Permitir todas las salidas para sesiones Telnet.
d) Permitir todas las salidas para sesiones FTP.
e) Rehusar todo el trafico UDP.

Beneficios del ruteador filtra-paquetes

La mayoría de sistemas firewall son desplegados usando únicamente ruteadores filtra-paquetes. Otros que tienen tiempo planean los filtros y configuran el ruteador, sea este pequeño o no, es costoso para implementar la filtración de paquetes no es cara; desde que los componentes básicos de los ruteadores incluyen revisiones estándar de software para dicho efecto. Desde entonces el acceso a Internet es generalmente provisto a través de interfaces WAN, optimando la operación del ruteador moderando el tráfico y definiendo menos filtros. Finalmente, el ruteador de filtrado es por lo general transparente a los usuarios finales y a las aplicaciones por lo que no se requiere de entrenamiento especializado o software especifico que tenga que ser instalado en cada uno de los servidores. Generalmente, los paquetes entorno al ruteador disminuyen conforme el número de filtros utilizados se incrementa. Los ruteadores son optimizados para extraer la dirección destino IP de cada paquete, haciendo relativamente simple la consulta a la tabla de ruteo, y el desplazamiento de paquetes para la interfase apropiada de la transmisión. Si esta autorizado el filtro, no únicamente podrá el ruteador tomar la decisión de desplazar cada paquete, pero también sucede aun aplicando todas las reglas de filtrado. Esto puede consumir ciclos de CPU e impactar el perfecto funcionamiento del sistema.

Pasarelas a nivel-aplicación

Las Pasarelas a nivel-aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador 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 muro de fuego, se instala en la pasarela 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 muro de fuego. Aún cuando, el código proxy puede ser configurado para soportar únicamente las características especificas 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 pasarela seleccionado, los servicios de aplicaciones del proxy, el tiempo y los conocimientos requeridos para configurar la pasarela 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 la pasarela a nivel-aplicación. Si se permite a los usuarios seccionar en el sistema de muro de fuego, la seguridad es amenazada desde el momento en que un intruso puede potencialmente ejecutar muchas actividades que comprometen la efectividad del sistema. Por ejemplo, el intruso podría obtener el acceso de root, instalar un caballo de troya para colectar las contraseñas, y modificar la configuración de los archivos de seguridad en el muro de fuego. Un ruteador filtra-paquetes permite la circulación directa de los paquetes dentro y fuera del sistema, diferente a esto la pasarela 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. Una pasarela 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.

Características de diseño del servidor de defensa:

a) La plataforma de hardware del servidor de defensa ejecuta una versión "segura" de su sistema operativo. Por ejemplo, si el servidor de defensa es una plataforma UNIX, se ejecutará una versión segura del sistema operativo UNIX que es diseñado específicamente para proteger los sistemas operativos vulnerables y garantizar la integridad del muro de fuego.

b) Únicamente los servicios que el administrador de redes considera esenciales son instalados en el servidor de defensa. La lógica de operación es que si el servicio no esta instalado, este puede ser atacado. Generalmente, un conjunto limitado de aplicaciones proxy tales como Telnet, DNS, FTP, SMTP, y autenticación de usuarios son instalados en este servidor.

c) El servidor de defensa podrá requerir de una autenticación adicional para que el usuario acceda a los servicios proxy. Por ejemplo, el servidor de defensa es ideal para colocar un sistema fuerte de supervisión de autorización (tal como la tecnología "una-sola vez" de contraseña donde una tarjeta inteligente generaba un código de acceso único por medios criptográficos). Adicionalmente, cada servicio proxy podrá requerir de autorización propia después que el usuario tenga acceso a su sesión.

d) Cada proxy es configurado para soportar únicamente un subconjunto de aplicaciones estándar de un conjunto de comandos. Si un comando estándar no es soportado por la aplicación proxy, es porque simplemente no esta disponible para el usuario.

e) Cada proxy esta configurado para dejar acceder únicamente a los servidores especificados en el sistema. Esto significa que existe un conjunto de características/comandos que podrán ser aplicados para un subconjunto de sistemas en la red protegida.

f) Cada proxy mantiene la información detallada y auditada de todos los registros del tráfico, cada conexión, y la duración de cada conexión. El registro de audición es una herramienta esencial para descubrir y finalizar el ataque de un intruso.

g) Cada proxy es un programa pequeño y sencillo específicamente diseñado para la seguridad de redes. Este permite que el código fuente de la aplicación pueda revisar y analizar posibles intrusos y fugas de seguridad. Por ejemplo, una típica aplicación - UNIX mail - puede tener alrededor de 20,000 líneas de código cuando un correo proxy puede contener menos de mil.

h) Cada proxy es independiente de todas las demás aplicaciones proxy en el servidor de defensa. Si se presentara un problema con la operación de cualquier proxy, o si se descubriera un sistema vulnerable, este puede desinstalarse sin afectar la operación de las demás aplicaciones. Aún, si la población de usuarios requiere el soporte de un nuevo servicio, el administrador de redes puede fácilmente instalar el servicio proxy requerido en el servidor de defensa.

i) Un proxy generalmente funciona sin acceso al disco lo único que hace es leer su archivo de configuración inicial. Desde que la aplicación proxy no ejecuta su acceso al disco para soporte, un intruso podrá encontrar más dificultades para instalar caballos de Troya perjudiciales y otro tipo de archivos peligrosos en el servidor de defensa.

j) Cada proxy corre como un usuario no-previlegiado en un directorio privado y seguro del servidor de defensa.

La siguiente figura muestra la operación de un Telnet proxy en un servidor de defensa.

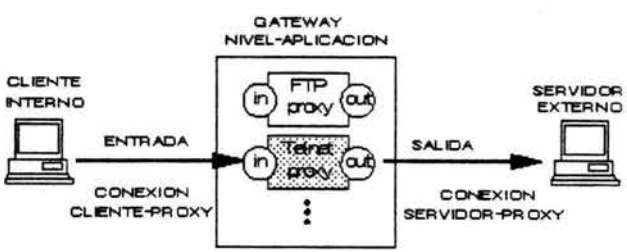


Figura 5.14 Telnet proxy.

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.

Beneficios de la pasarela a nivel-aplicación

Son muchos los beneficios desplegados en una pasarela a nivel-aplicación. Ellos dan a la administración de red un completo control de cada servicio desde aplicaciones proxy limitadas por un conjunto de comandos y la determinación del servidor interno donde se puede acceder a los servicios. Aun cuando, el administrador de la red tenga el completo control acerca de que servicios son permitidos, cuando se carece de un servicio proxy para uno en particular significa que el servicio esta completamente bloqueado.

Las pasarelas a nivel-aplicación tienen la habilidad de soportar autenticaciones forzando al usuario para proveer información detallada de registro. Finalmente, las reglas de filtrado para una pasarela de este tipo son mucho más fáciles de configurar y probar que en un ruteador filtra-paquetes.

Limitaciones de la pasarela a nivel-aplicación

Probablemente una de las grandes limitaciones de una pasarela a nivel-aplicación es que requiere de modificar la conducta del usuario o requiere de la instalación de software especializado en cada sistema que accede a los servicios proxy Por ejemplo, el acceso de Telnet vía pasarela a nivel-aplicación demanda modificar la conducta del usuario desde el momento en que se requiere de dos pasos para hacer una conexión mejor que un paso. Como siempre, el software especializado podrá ser instalado en un sistema terminado para hacer las aplicaciones de la pasarela transparentes al permitir a los usuarios especificar el servidor de destino, mejor que el propio, en un comando de telnet.

Pasarela a nivel-circuito

Una pasarela a nivel-circuito es en si una función que puede ser perfeccionada en una pasarela a nivel-aplicación. A nivel-circuito simplemente trasmite las conexiones TCP sin cumplir cualquier proceso adicional en filtrado de paquetes.

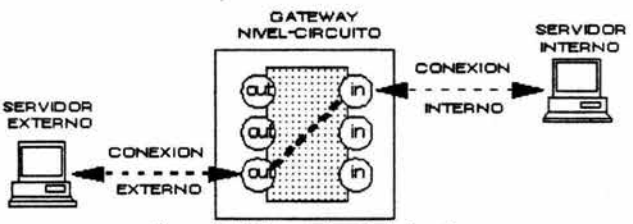


Figura 5.15 Pasarela nivel-circuito.

La figura anterior muestra la operación de una conexión típica Telnet a través de un gateway a nivel-circuito.Tal como se menciono anteriormente, esta pasarela simplemente trasmite la conexión a través del muro de fuego sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de Telnet. La pasarela a nivel-circuito trabaja como un 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 del muro de fuego tratando de beneficiar el encubrir la información sobre la protección de la red. La pasarela 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 una pasarela "híbrida" soportando nivel-aplicación o servicios proxy para conexiones de venida y funciones de nivel-circuito para conexiones de ida. Esto hace que el sistema del muro de fuego sea fácil de usar para los usuarios internos quienes desean tener acceso directo a los servicios de Internet mientras se proveen las funciones del muro de fuego necesarias para proteger la organización de los ataques externos.

5.2.6.2 Limitaciones de un sistema de muro de fuego.

a) Un muro de fuego no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación. Por ejemplo, si existe una conexión dial-out sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una conexión SLIP o PPP al Internet. Los usuarios con sentido común suelen "irritarse" cuando se requiere una autenticación adicional requerida por un Firewall Proxy server (FPS; Servidor Apoderado del muro de fuego). Lo cual se puede ser provocado por un sistema de seguridad circunvecino que esta incluido en una conexión directa SLIP o PPP del ISP.

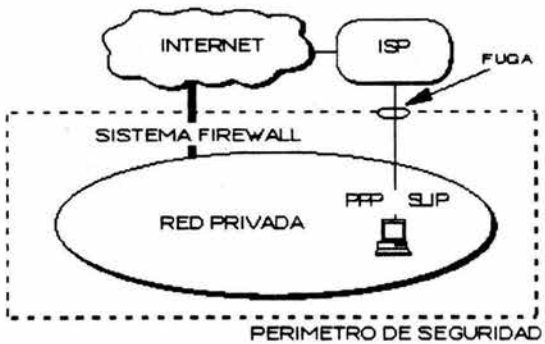


Figura 5.16 Conexión circunvecina al muro de fuego.

b) El muro de fuego no puede protegerse de las amenazas a la que esta sometido por traidores o usuarios inconscientes. El muro de fuego no puede prohibir que los traidores o espías corporativos copien datos sensitivos en disquetes o tarjetas PCMCIA y substraigan estas del edificio. El muro de fuego no puede proteger contra los ataques de la "Ingeniería Social", 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.

c) El muro de fuego 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 muro de fuego de Internet no puede contar con un sistema preciso de SCAN (SCAN; System Control Antivirus Network) para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él. La solución real esta en que la organización debe ser consciente en instalar software anti-viral en cada despacho para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.

d) El muro de fuego no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparentemente 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 más 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.

5.2.7 Servidores Seguros

Se entiende por Servidor Seguro un servidor de páginas web que establece una conexión cifrada con el cliente que ha solicitado la conexión, de manera que nadie, salvo el servidor y el cliente, puedan tener acceso a la información transmitida de forma útil. El uso de servidores seguros es un elemento imprescindible en todos aquellos servicios que utilicen información confidencial, como operaciones bancarias on-line, compras por Internet, acceso a servidores de datos sensibles, etc. Para conseguir la confidencialidad e integridad de datos perseguida los servidores seguros se basan en el uso de sistemas criptográficos mixtos, que combinan la criptografía de clave pública con la de clave simétrica. Pero esta protección que debiera darnos la Criptografía es, en la práctica, difícil de encontrar, debido a las severas leyes de exportación de software de cifrado que impone el gobierno de EEUU, sobre todo en lo que respecta a la longitud de las claves que usan. Para garantizar al usuario su autenticidad, los servidores seguros hacen uso de los certificados digitales ya estudiados. Cuando accedemos a un servidos seguro normalmente nos aparece una ventana indicándonos que vamos a iniciar una conexión segura, y el candado situado en la parte inferior de la ventana del navegador aparecerá cerrado cuando entremos a la página segura (Atención: la presencia del candado cerrado no garantiza una comunicación segura; hace falta comprobar el certificado del servidor). Además, si miramos en la barra de direcciones veremos que ahora estamos usando el protocolo HTTPS, que corresponde al protocolo HTTP con privacidad.

Podemos acudir al menú "Archivo" > "Propiedades" para obtener información más detallada sobre el documento seguro, entre la que destaca:

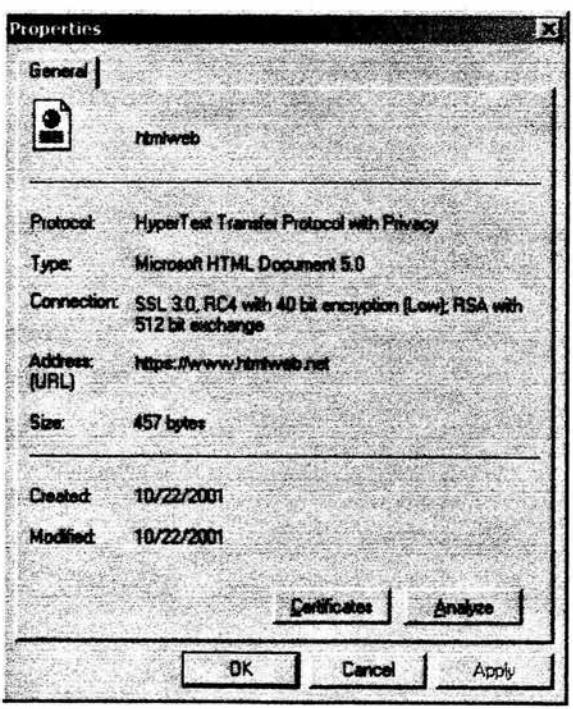


Figura 5.17 Información de un documento seguro.

a) Protocolo: HTTP Seguro (con privacidad).

b) Conexiones: Protocolo Secure Socket Layer versión 3.0, algoritmo simétrico de cifrado RC4 con longitud de claves de 40 bits, algoritmo de cifrado de clave pública RSA de 512 bits de longitud de clave.

c) URL del servidor seguro. Como vemos, tenemos una longitud de clave RC4 de 40 bits, limitación impuesta por el gobierno de EEUU al sistema de cifrado para su exportación. Esta longitud de clave no es toda lo segura que debiera para ser usada en transacciones delicadas; ya ha sido violentada anteriormente, y aunque esto no significa que pueda serlo en el tiempo de duración de la conexión segura, si es un indicio de la debilidad del sistema con esas longitudes de clave. También podemos acceder desde una página segura al certificado digital del servidor de forma rápida. Para ello basta hacer seleccionar el botón "Certificates" de la ventana anterior o hacer doble click sobre el candado cerrado. Otro aspecto importante a considerar son los fallos a la hora de implementar los protocolos criptográficos, sobre todo en lo que respecta a la configuración propia del servidor web seguro y a los fallos de implementación que de los protocolos hacen los navegadores cliente. Uno de estos fallos es la relativa falta de seguridad de los números seudo aleatorios generados para el proceso de creación de claves durante la fase Handshake. A pesar de todas estas consideraciones no hay que ser alarmista en cuanto al uso de los servidores y protocolos seguros, ya que generalmente el tiempo de duración de la conexión segura es lo suficientemente pequeño como para resultar imposible, con los medios actuales, descifrar las claves en un tiempo útil. Y a esto hay que añadir las innumerables ventajas que obtenemos de este tipo de aplicaciones, que permiten realizar transacciones seguras por Internet.

Condiciones mínimas necesarias.

Para minimizar los riesgos posibles, a la hora de implementar o aceptar un servicio de servidor seguro podemos exigir que se cumplan una serie de condiciones, entre las que podemos destacar:

a). Que el certificado de servidor seguro se corresponda con los de máximas garantías de verificación y que haya sido expedido por una Autoridad certificadora de toda confianza. Generalmente los navegadores cliente reconocen como tales a VeriSign/RSA Secure Server Certification Authority, EuroSign y Thawte Server.

b). Que el navegador usado en la comunicación tenga implementada la última versión de SSL, es decir, el protocolo SSL 3.0. Versiones anteriores son válidas, pero no recomendadas.

c). El uso de un sistema de cifrado simétrico robusto (RC4 RC5 o similar) con longitudes de clave largas (de entre 64 y 128 bits). A pesar de la limitación clásica del gobierno USA para la exportación de sistemas con claves largas, actualmente las principales compañías fabricantes de navegadores tienen permiso para exportar las actualizaciones a cifrado de 128 bits, por lo que es conveniente la actualización de nuestros navegadores. Estas actualizaciones a veces son también suministradas por bancos y entidades financieras a sus clientes.

5.3 ORGANISMOS DE ESTANDARIZACION.

En los últimos años las necesidades de comunicación entre las compañías, países y personas se han incrementado considerablemente y con el objetivo de satisfacer estas necesidades se han creado nuevas compañías de telecomunicaciones que brindan servicios de comunicación de datos especializados, que por o general compiten con las compañías telefónicas de antaño. (ATT&T, MCA, BELL). Algunas de estas compañías ofrecen servicios de larga distancia con un rendimiento muy alto (por ejemplo mediante el empleo de satélites), en tanto que otras ofrecen tiempo compartido, redes u otros servicios usando facilidades comunicación que ellas mismas rentan a otros proveedores de servicios portadores comunes.

Por otro lado existen países en los que el gobierno nacional tiene el monopolio de completo de todas las comunicaciones, incluyendo el correo, telégrafo, teléfono y frecuentemente también la radio y televisión. La mayoría de los países del mundo caen dentro de esta categoría. En algunos casos, la máxima autoridad en las telecomunicaciones resulta ser una compañía nacionalizada, en. tanto que en otros es solo una rama derivada de la estructura gubernamental comúnmente conocida como PTT (Administradora de Correo, Telégrafo y Teléfonos).

Con todos estos distintos proveedores de servicios, es clara la necesidad de que dicho servicio sea compatible a una escala mundial, para asegurar que la gente (y las computadoras), en un determinado país, se puedan comunicar con otras personas en otro país. Esta coordinación la ofrece una agencia de las naciones Unidas llamada ITU.

5.3.1 Unión Internacional de Telecomunicaciones (UIT)

La Unión Internacional de Telecomunicaciones conocida en inglés como ITU (International Telecomunication Union; ITU)) Es una agencia especializada del Sistema de las Naciones Unidas dedicada al sector de las Telecomunicaciones y cuya sede esta en Ginebra Suiza; Esta unión esta compuesta por gobiernos, compañías privadas, instituciones industriales y científicas que cooperan para un uso racional de las telecomunicaciones.

La oficina regional para Latino América se encuentra en Brasilia Brasil, pero la UIT cuenta además con oficinas de área en Barbados, Chile y Honduras.

La oficina de Honduras es la que atiende a los países del área centroamericana a México, Panamá, Cuba y a la República Dominicana.

La UIT esta formada principalmente por 3 órganos, donde dos de ellos se ocupan sobre todo de la difusión internacional de radio y el otro esta fundamentalmente relacionado con sistemas telefónicos y de comunicación de datos.

A este último grupo se le conoce como CCITT (Comité Consultivo Internacional Telegráfica y Telefónico por sus siglas en francés).

5.3.2 El Comité Consultivo (CCITT)

El CCITT tiene como propósito mantener y extender la cooperación internacional para el mejoramiento y el uso racional de las telecomunicaciones de todos los tiempos; promover el desarrollo de facilidades técnicas y sus operaciones más eficientes con una visión para mejorar la eficiencia de los servicios de telecomunicaciones, mejorar su completa utilización y hacer de ellos, en lo posible disponible para todo público; armonizar las acciones de las naciones en el logro de estos fines comunes.

El CCITT tiene 5 clases de miembros: miembros A, que son las PTT nacionales; miembros B, que son los reconocidos como administraciones privadas (por ejemplo, AT&T); miembros C que son las organizaciones científicas e industriales; miembros D, que corresponden a otras organizaciones internacionales; y miembros E, que corresponden a aquellas organizaciones cuya misión fundamental esta en otro campo pero que están interesadas en el trabajo del CCITT.

De esta clasificación solo los miembros tipo A tienen derecho a voto. La tarea del CCITT consiste en promover las recomendaciones técnicas sobre aspectos telefónicos, telegráficos e interfaces de comunicación de datos. Esta labor ha producido normas que tienen un reconocimiento internacional.

5.3.3 Comisión Federal de Telecomunicaciones (COFETEL)

La Comisión Federal de Telecomunicaciones, es un órgano administrativo desconcentrado de la Secretaría de Comunicaciones y Transportes, con autonomía técnica y operativa, el cual tendrá las atribuciones que le confiere el Decreto de Creación y el Reglamento Interior de la Secretaría de Comunicaciones y Transportes, con el objeto de regular y promover el desarrollo eficiente de las telecomunicaciones.

La COFETEL es la PTT que representa a México en la CCITT y se encarga de traducir, promover y aplicar las Normas acordadas por el pleno del CCITT y al mismo tiempo de acordar y generar, promover y aplicar algunas normas propias de la COFETEL y para aplicarse solo en nuestro país.

Para el desempeño de sus atribuciones y el despacho de los asuntos que le competen, la Comisión Federal de Telecomunicaciones esta formada por:

I. El Pleno;

II. La Presidencia;

III. Las Áreas Generales:

a) De Asuntos Jurídicos;
b) De Planeación y Análisis Económico, y
c) De Ingeniería y Tecnología.

IV. Las Coordinaciones Generales:

a) Ejecutiva;
b) De Asuntos Internacionales, y
c) De Servicios de Telecomunicaciones.

V. Las Coordinaciones:

a) De Comunicación Social;
b) De Administración, y
c) De Asesores.

VI. Las Direcciones Generales de:

a) Asuntos Contenciosos;
b) Consulta Jurídica y Normatividad;
c) Aspectos Regulatorios e Instrumentación Legal;
d) Tarifas e Integración Estadística;
e) Estudios Económicos y Regulatorios;
f) Análisis Financiero;
g) Estudios Técnicos, Investigación y Desarrollo;
h) Planes Fundamentales de Telecomunicaciones;
i) Ingeniería y Homologación;
j) Planeación y Administración del Espectro;
k) Ejecutiva;
l) Licitaciones del Espectro Radioeléctrico;
m) Inspección, Verificación y Radiomonitoreo;
n) Recaudación y Coordinación Regional;
o) Cooperación Internacional;

p) Organismos de Regulación Internacional;
q) Comunicación Vía Satélite;
r) Televisión y Audio Restringidos;
s) Servicio Local y Radiocomunicación, y
t) Larga Distancia y Valor Agregado.

VII. La Contraloría Interna;

VIII. El Secretario Técnico del Pleno, y

IX. Las demás unidades y personal técnico y administrativo que autorice el Presidente, de acuerdo con el presupuesto autorizado y sujeto a las normas y lineamientos que la Secretaría de Hacienda y Crédito Público establezca para las unidades de gasto autónomo.

Una vez que describimos y analizamos los elementos necesarios para realizar una conexión segura, en el próximo capítulo se definirá y se describirá los requerimientos mínimos necesarios para realizar una conexión de tipo remota.

CAPÍTULO 6

REQUERIMIENTOS MÍNIMOS PARA LA CONEXIÓN REMOTA

6.1 CONECTIVIDAD DE REDES

La empresa TESYS tiene la necesidad de realizar el acceso remoto de sus empleados utilizando los más recientes avances de la tecnología para garantizar la seguridad, integridad y rapidez al realizar dicho enlace.

Como se menciona en capítulos anteriores se implementará una red LAN la cual tendrá acceso a Internet por medio de un switch que a su vez se enlazará a un firewall que será el que dará protección a nuestra información. Este se puede esquematizar de la manera siguiente.

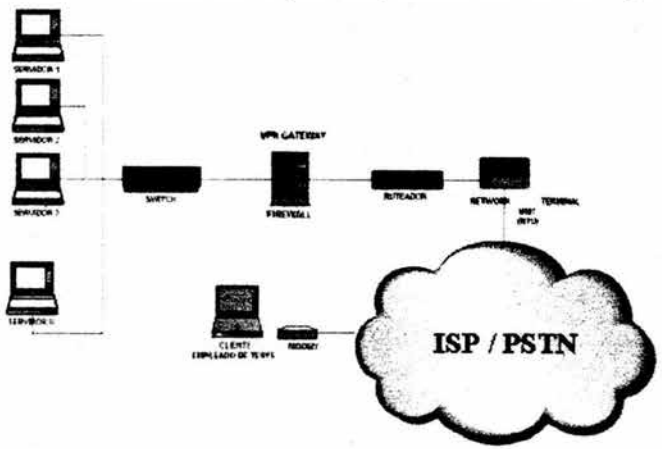


Figura 6.1 Conectividad de la Red

Para describir una de las formas por la cual se estructurará la conexión remota, debemos de mencionar que la conexión remota se realizará cuando el empleado se comunique vía telefónica a la red LAN de TESYS, esta comunicación se llevará a cabo gracias a un equipo denominado MODEM (Modulador/ Demodulador) que realizará la operación de comunicar su computadora con otro dispositivo, que en este caso será un dispositivo dentro de TESYS.

El empleado podrá utilizar un MODEM interno que traerá ya de fábrica los equipos Laptop.

6.1.1 Configuración ideal de la red LAN o Intranet de la compañía

Un aspecto importante de mencionar con relación a la conectividad entre oficinas es el tráfico de banda ancha (broadcast) que existe en todas las redes actuales debido a que no se genera por la tecnología sino por las aplicaciones mismas que utilizan este tipo de tráfico para enviar o recibir información, un ejemplo de esto es en multimedia. El tráfico broadcast se controlará a través de una segmentación en la red LAN, o bien, mediante el análisis del comportamiento de las aplicaciones antes de instalarlas.
En la operación normal de la red, el tráfico broadcast puede llegar a tener un bajo funcionamiento en algunos de los dispositivos, como las tarjetas de red de las estaciones de trabajo, del concentrador/conmutador o del ruteador; o bien, al mal estado de algún dispositivo adicional como el puente, repetidor y/ o pasarela (en caso de utilizar alguno de estos). Si este tipo de tráfico no se maneja bien, puede causar serios problemas a la red e incluso puede darla de baja en su totalidad. Este tipo de falla se debe primordialmente al uso inadecuado de protecciones contra este tipo de tráfico (muro de fuego), a la generación de círculos en la interconectividad, a la falla de los dispositivos y/o a las aplicaciones que hacen un uso intenso de broadcast para operar.

Por lo tanto, los administradores de red de TESYS deberán tomar todas las precauciones necesarias contra este tipo de tráficos. Una forma común y muy utilizada para hacerlo es la segmentación de la red con dispositivos que no permitan la propagación del broadcast, como son los ruteadores en hardware y el muro de fuego. Éstos protegen a los demás segmentos dentro de la red en el caso de que alguno de ellos tengan problemas, debido a que los broadcast no serán propagados hacia los demás segmentos ocasionando fallas en la red.

Un aspecto muy importante a considerar cuando se migra a redes de switch o virtuales es que el tráfico de broadcast funciona en el nivel 2 de la capa del modelo OSI al igual que las redes virtuales.

Si no se considera un esquema de protección contra el tráfico no deseado (broadcast), cuando ocurra un problema en la red éste será propagado hacia todos los puertos del switch y, por consiguiente, hacia toda la red, ocasionando que todas las aplicaciones dejen de funcionar. A este tipo de configuraciones se le conoce como "red plana" debido a que toda la red opera como un solo dominio de broadcast. Las ventajas de las redes planas son la reducción en el tiempo de retraso de los paquetes y el incremento en el rendimiento de la red; la desventaja es el incremento en la susceptibilidad de los problemas de broadcast a través de todos los conmutadores, puertos, backbone y usuarios.

Al igual que los ruteadores actuales, las redes privadas virtuales ofrecen mecanismos eficientes para el manejo de los problemas potenciales de broadcast, sin perder sus ventajas. Para poder manejar de forma controlada estos problemas, cada puerto del switch, al igual que los usuarios, se integrará a grupos de trabajo o de redes privadas virtuales con el fin de aislarlos cuando se genere algún problema en cualquiera de ellos. El tráfico broadcast de un grupo de trabajo o VLAN no se transmite fuera del mismo. Con esta sencilla estrategia, el administrador de red de TESYS podrá controlar fácilmente el tamaño de los grupos de trabajo o VLAN, de tal forma que el tráfico broadcast generado en esa VLAN no sea perjudicial para ella misma. Entre más pequeñas sea la VLAN, menor será el tráfico de broadcast generado.

6.1.2 Conectividad entre redes LAN

Debido a las necesidades de interconexión de TESYS dentro de su LAN y de manera externa se requiere una línea digital de alta velocidad que pueda dividir para voz, datos y, en su momento de así requerirse video, en varios canales, por lo que se escogió un enlace E1 (2,048Kbps) suficiente para los 300 usuarios existentes (100 internos, 200 externos) esto es para el primer escenario:

Pasarela para Red Privada (VPN gateway), y un enlace 1024 Mbps para el segundo escenario: Servidor para Acceso Remoto(RAS).

Sin embargo, no se descarta a mediano plazo el cambio a un enlace de mayor capacidad E2, que ofrece una velocidad de hasta 8.448Mbits por segundo para el VPN y un E1 para el RAS respectivamente.

Esta última consideración será llevada a cabo a partir del crecimiento de TESYS en cuanto a recursos humanos y demanda de información.

6.2 USUARIOS DE ACCESO REMOTO Y AUTENTICIDAD SOBRE INTERNET

La tecnología de VPN proporciona un medio para usar el canal público de Internet como una canal apropiado para comunicar los datos privados de TESYS; sin embargo, para que los usuarios reciban continuamente información dentro de la VPN es necesario seguir los pasos descritos a continuación:

Solicitud de Información

Un usuario solicita información usando una aplicación tal como un browser de Internet, desde su PC. El intercambio de información comenzará cuando el usuario envíe o solicite la información al servidor y /o aplicaciones de la compañía.

Envió y Aseguramiento del Mensaje

La aplicación envía y asegura el mensaje. Cuando un cliente y el VPN Gateway detecten que se necesita seguridad para transmitir la petición y para ver el nuevo documento, ellos se interconectarán en un mutuo protocolo de autentificación. Este paso verificará la identidad de ambas partes, antes de llevar a cabo cualquier acción. Una vez que se produzca la autentificación, pero antes de que la aplicación envíe la petición, asegurará el mensaje encriptándolo.

Transmisión del Mensaje

El mensaje se transmite a través de Internet. Para que la petición alcance el servidor y /o aplicaciones de la compañía, deberá dejar la red LAN del sitio remoto donde se encuentre el usuario y viajará a través de Internet, lo cual le permitirá alcanzar el servidor en algún punto de la misma. Durante este viaje, puede darse el caso de que atraviese 1 o más firewall antes de alcanzar su objetivo. Una vez atravesado el firewall, la petición circulará a lo largo del túnel en Internet hasta alcanzar el destino.

Controles de Seguridad

El mensaje recibido debe pasar controles de seguridad. Cuando el mensaje alcance su destino, tendrá que atravesar el firewall de TESYS. Este firewall protegerá cuidadosamente el tráfico entrante asegurando que se ciñe a la política corporativa, antes de dejarlo atravesar la red interna. El mensaje posteriormente se transferirá al servidor y/o aplicaciones de la compañía como consecuencia de la autentificación mutua que se produjo entre el cliente y el servidor.

Verificación de los Derechos de Acceso

Durante la petición, se verifican los derechos de acceso de los usuarios. Al igual que en todas las redes corporativas, todos los usuarios no pueden acceder a la totalidad de la información corporativa. En la VPN dinámica de TESYS, el sistema podrá restringir que usuarios pueden y no pueden acceder a la misma.

El servidor determinará si el usuario tiene derechos para realizar la petición de información. Esto se hará, usando un mecanismo de control. El servidor de control de acceso de la pasarela (VPN Gateway), restringirá el acceso a la información en niveles de acceso a servidores y /o aplicaciones internas de TESYS. De modo que, si incluso un usuario presenta un certificado válido, puede ser que se le decline el acceso basándose en otros criterios (por ejemplo, políticas de información corporativa).

Devolución de la información

La petición de información es devuelta por Internet, previamente asegurada. Si el usuario tiene derechos de acceso a la petición de información, el servidor de información encriptará la misma y opcionalmente la certificará. Las claves establecidas durante los pasos de autentificación mutua se usarán para encriptar y desencriptar el mensaje.

6.2.1 Características Mínimas de Acceso a la Red LAN

Como vimos anteriormente aún cuando las PC no estén conectadas a la red local de TESYS, siempre será posible conectarlas por medio de la VPN a través de un acceso "dial up" a las aplicaciones internas de la empresa.
Este tipo de conexiones a la red corporativa de TESYS se pueden manejar a través de una conexión de servidor de acceso remoto (RAS) o por medio de una pasarela (VPN Gateway). Con este tipo de conexiones RAS o VPN Gateway las PC se pueden conectar a la red de TESYS con los protocolos de red TCP/IP, IPX, Net BEUI y bajo encripción IP Sec, soportados por el sistema operativo de Windows y bajo el cual opera tanto la red LAN de TESYS como las PC de los usuarios remotos.

La conexión puede establecerse tanto por línea telefónica digital como por MODEM o cualquier otra línea apta para datos (por ejemplo X.25, el cual es un protocolo de transferencia orientado a paquetes mediante el que se pueden conectar PC´s).

6.2.2 El concepto de Acceso Remoto y Red Privada

El servicio de acceso remoto le permitirá al cliente acceder al servidor RAS y /o equipo VPN Gateway y utilizar, a continuación, todos los recursos de la red como en una LAN "normal". El servicio de RAS y de VPN Gateway acepta los siguientes sistemas operativos tanto para la red LAN como para los clientes remotos:

a) Windows 2000
b) Windows NT
c) Windows para trabajo en grupo
d) MS DOS a partir de la versión 3.1

El hecho de basarnos solamente entre las opciones del servicio RAS o VPN Gateway, es que se diferencian de los demás programas remotos (servicios de control remoto) de otros fabricantes porque funcionan como gateway multiprotocolo; a través de una línea cualquiera de datos (analógica, telefónica o digital) y establecer una conexión entre el servidor RAS o el equipo VPN Gateway y el cliente remoto, lo cual a su vez, les permitirá acceder a las aplicaciones y /o equipos de la red LAN de TESYS.
En cambio, los servicios de control remoto están pensados básicamente para la comunicación entre dos PC.

6.3 CARACTERÍSTICAS NECESARIAS DE LA CONEXIÓN REMOTA

Para configurar, administrar y establecer conexiones con un servidor de acceso remoto (RAS) o la pasarela (VPN Gateway), el sistema operativo de Windows utiliza el programa Conexión Telefónica a la red. En este programa se especifican los parámetros de acceso, números de teléfono y protocolos que se vayan a utilizar para la conexión automática con el servidor de acceso remoto o con la pasarela cada vez que se soliciten recursos de esta red remota.

6.3.1 Software de Conexión Remota

Para lograr la conexión remota es necesario que se instale un software especial para lograr esto en todas las computadoras portátiles o no, de los empleados o usuarios que tendrían este tipo de acceso. Algunas de las marcas más reconocidas venden sus equipos con un software de conexión remota propio, pero como esto no es cierto para todas las marcas y con el objetivo de tener un panorama más amplio, a continuación describiremos algunos de las opciones más reconocidas y recomendables de este tipo de software aplicables a la solución que estamos proponiendo en esta trabajo de investigación.

6.3.1.1 AT&T Network Client.

El AT&T Network Client (ANC), satisface todas nuestras necesidades de conexión remota a un bajo costo, una mayor seguridad y una mayor funcionalidad que la mayoría de los software de conexión remota existentes en el mercado actual.

El Software ANC ofrece básicamente dos servicios en un solo paquete:

1. - El Servicio ANC Narrowband (de banda chica). Este servicio trabaja a través del MODEM instalado en las computadora personales de los empleados o usuarios para conectarlos a la red corporativa a través del Software dial-up Network de AT&T.

2. - El ANC Internet Tunneling el cual te permite conectarte a la red corporativa a través de un proveedor de servicios de Internet externa, tales como los servicios de banda ancha que ofrece Telmex (Prodigy Infinitum), o los servicios de CABLE MODEM.
El ANC es un servicio de AT&T que permite la conexión remota a la red corporativa basado en el más nuevo de los estándares de Internet llamado IPSec el cual permite que el servicio sea más seguro y menos costoso, además este permite la conexión remota a través de MODEM y a través de un proveedor de servicios de Internet (ISP).

Situaciones especiales a considerar:

a) IPSec; este software esta basado en los estándares de IPSec, no puede ser utilizado en conexiones de redes o con proveedores de servicios (ISP) que no soporten IPSec. Se sabe que este estándar será cada vez mas utilizado, pero por el momento aun existen redes y proveedores de servicio que no soportan estos estándares.

b) Servicio en Hoteles: Muchos hoteles ofrecen conexiones de Internet tipo Ethernet y si este tipo de servicio usa un ruteador o firewall que no soporte IPSec el servicio ANC Tunneling no funcionaría, en estos casos se puede utilizar el servicio ANC Narrowband.

6.3.1.2 Aventail Connect 4.1.2

Este software sirve para hacer correr aplicaciones de una red corporativa de forma remota, se utiliza principalmente para empresas que tienen la necesidad de que parte de sus empleados corran procesos o soporten aplicaciones de forma remota. Este tipo de conexión se lleva a cabo en tres pasos que procederemos a describir a continuación.

Paso 1:

Se arranca la aplicación en la computadora del empleado, y esta empieza una búsqueda de DNS para convertir el nombre del host en una dirección de IP. Si la aplicación ya conoce la dirección de IP se brinca este paso, de otra manera se manda un requerimiento de resolución de nombre a la pila de WinSock para obtener una dirección de IP temporal para el servidor remoto. Si la dirección del servidor o host coincide con un host o dirección en el archivo de configuración entonces Aventail connect crea una entrada falsa de DNS que pueda reconocer durante el requerimiento de conexión. Esta entrada se almacena en un archivo del directorio del programa connect y será referenciado para todos los requerimientos de nombres posteriores. Entonces Connect regresara este DNS falso como una dirección IP rechazada, esta dirección estará en el rango de 0.1.0.0/24. Aventail mandará este nombre de servidor al servidor de Extranet Aventail y este realizara la resolución de nombre de servidor. Si el requerimiento de nombre no contiene un nombre de servidor que coincida con una dirección definida en el archivo configuración. Aventail connect ignorara este requerimiento y dejara al WinSock terminar este requerimiento con el nombre del servidor local.

Paso 2:

La aplicación solicita una conexión al servidor remoto. Esto provoca que la pila principal empiece el saludo TCP, cuando este reconocimiento o saludo ha terminado la aplicación es notificada de que se ha establecido la conexión y los datos pueden empezar a ser transmitidos y recibidos. Para lograr esto Aventail Connect hace lo siguiente:

a) Revisa el requerimiento de conexión.

-Si el requerimiento contiene una DNS falso (parecido a 0.1.0.1) este será convertido a una IP ruteable.
-Si el requerimiento contiene una IP ruteable y las reglas establecidas dicen que esta deberá pasar por el proxy aventail, realizará una llamada al Winsock para empezar el saludo TCP con el servidor designado en el archivo de configuración.
-Si el requerimiento contiene una IP real, el requerimiento será pasado al Winsock y se pasará al paso 3 como si Aventail connnect no estuviera trabajando.

b) Cuando la conexión ha sido establecida Aventail Connect empezará la negociación de socks.

-Aventail connect envía la lista de métodos de autentificación que están activos en el archivo de configuración.
-Una vez que el servidor de extranet Aventail selecciona un método de autentificación, Aventail connect ejecuta el proceso de autentificación especificado.
-Entonces Aventail connect envía el requerimiento de proxy al servidor, este incluirá también la dirección IP proporcionada por la aplicación o la entrada de DNS proporcionada en el paso 1.

c) Cuando la negociación de SOCK ha terminado Aventail connect notificará a la aplicación acerca de esto.

Paso 3:

Si el módulo de encriptación esta habilitado y seleccionado por el servidor Extranet Aventail, Aventail connect encriptará los datos que vayan a ser enviados al servidor y si este nos manda datos encriptados de regreso, Aventail connect desencriptará estos de tal manera que la aplicación pueda trabajar de forma correcta.

6.3.1.3 Cisco VPN Client.

Fácil de abrir y operar el software CISCO VPN Client permite a los usuarios establecer túneles encriptados seguros a cualquier servidor VPN Cisco. El diseño e implementación de la tecnología IPSec se consigue con el uso de este software que funciona con cualquier producto de sitio remoto VPN y que viene incluido gratuitamente en el concentrador CISCO VPN de la serie 3000.
Este software puede ser pre-configurado para usos masivos y se requiere una intervención mínima la primera vez que los usuarios remotos se signen a la red.
Las políticas y configuraciones de acceso VPN son instalados mediante el gateway central y enviados al usuario cuando se establece la conexión permitiendo un uso sencillo en la parte remota y un manejo fácil en la red corporativa al mismo tiempo que es muy escalable.
El Cisco VPN client soporta los sistemas operativos Windows 95, 98, 2000, ME, NT 4.0, 2000XP, Linux (Intel), Solaris y Mac OSX 10.1 y 10.2.

El Cisco VPN client es compatible con los siguientes productos de CISCO.

-Concentrador CISCO VPN serie 3000
-Software del Concentrador CISCO VPN serie 3000 Versión 3.0 y posteriores.
-Software CISCO IOS versiones 12.2T y posteriores.
-Software del firewall ICSCO PIX versiones 6.0 y posteriores

6.3.1.4 Contivity Multi OS VPN Client (Nortel)

El Contivity Multi-OS VPN Client provee funcionalidad para los accesos remotos sobre IP a redes de servidores VPN y ruteadores de acceso IP. Este software trabaja virtualmente sobre todas las plataformas de trabajo de PC incluyendo los sistemas operativos Windows 95, 98, 2000, ME, NT, XP, IBM-AIX, SUN-Solaris, HP-VX, Linux y Macintosh.

Características principales.

-Provee completa funcionalidad para accesos desde Windows, Unix/ Linux, Solaris y sistemas Macintosh.

-Impone políticas de seguridad centralizadas, incluyendo el alojamiento de banda ancha, controles de acceso, autentificación, encriptación entre otros.

-Dispara negaciones o terminación de la conexión para clientes que no cumplan con los parámetros preestablecidos.
-Permite a los administradores de red configurar y distribuir de manera rápida y transparente, todas las configuraciones deseadas.

-Soporta balances de carga, interrupciones y compresiones LZS para ofrecer a los usuarios los tiempos de respuesta predecibles, operación continua y un desempeño más eficiente y rápido.

-Integración óptima con productos complementarios de autentificación acceso y control tales como los sistemas de autentificación de cualquier marca, los global dialers, los muros de fuego personales y los sistemas de detección de intrusos entre otros.

-Ha demostrado un desempeño de operación probado en el campo con más de 35 millones de usuarios desde 1998.

Beneficios.

-Encaja fácilmente en los accesos a redes de marcas o plataformas múltiples como las actualmente en el mercado, en las cuales al mismo tiempo los usuarios que accesaran remotamente a la red trabajan también con diferentes plataformas, sistemas operativos y velocidades de acceso.

-Elimina los requerimientos para distribuir e instalará software en todos los equipos de acceso, ya que este se instala silenciosa y automáticamente en los equipos del usuario final cuando este activa su sesión de conexión remota.

-Permite a las empresas establecer y aplicar políticas de seguridad centralizadas que permiten el acceso remoto sin exposiciones de la información confidencial cuando no se cuente con la autorización correspondiente.

-Posee una configuración sencilla y una distribución de configuraciones a masas.

-Optimiza el servicio a los usuarios a través del balanceo de cargas para eliminar los cuellos de botella, las condiciones de sobrecarga, interrupciones y la compresión de datos para preservar los tiempos de respuesta y la continuidad de las conexiones.

-Permite a las empresas tomar ventaja de los mejores productos de seguridad existentes en el mercado tales como los sistemas de autentificación, los sistemas de encriptación y los firewall personales.

6.3.1.5 Nokia.

Nokia ofrece tres sofware VPN client que permiten la conexión remota:

a) Check Point VPN-1 SecureRemote.

Este software encripta y autentifica transparentemente los datos críticos de la red para protegerlos contra intromisiones y falsificaciones de datos mal intencionadas.

b) El Check Point VPN-1 SecureClient.

Esta opción, adiciona un muro de fuego personal y manejo de dispositivos a la funcionalidad del VPN-1 SecureRemote. Después de la instalación inicial el VPN SecureClient actualiza el software en la PC del usuario remoto de forma transparente y automática para el mismo. Todos los componentes son regularmente monitoreados para que en el caso de ser necesarios estos sean automáticamente actualizados.

c) Nokia Mobile VPN Client.

Este software extiende el concepto de VPN a trabajadores móviles que poseen dispositivos de bolsillo en lugar de laptop, estos dispositivos pueden ser combinaciones de un teléfono celular y una pequeña computadora con capacidad para trabajar con aplicaciones de oficina de uso común como el correo electrónico por ejemplo. El Nokia Mobile esta diseñado específicamente para pequeños teléfonos que trabajen con el sistema operativo Symbian y una vez instalado funciona de forma casi transparente para el usuario.

6.3.2 Protocolo IP SEC

IPSec utiliza dos mecanismos que garantizan la seguridad, uno es Authentication Header (AH) que autentifica cada paquete y asegura la integridad de los datos ya que detecta cualquier alteración durante la transmisión; el otro es el Encapsulating Security Payload (ESP) que encripta y desencripta los datos utilizando algoritmos estándar como DES 56bit y 3 DES a 168 bits.

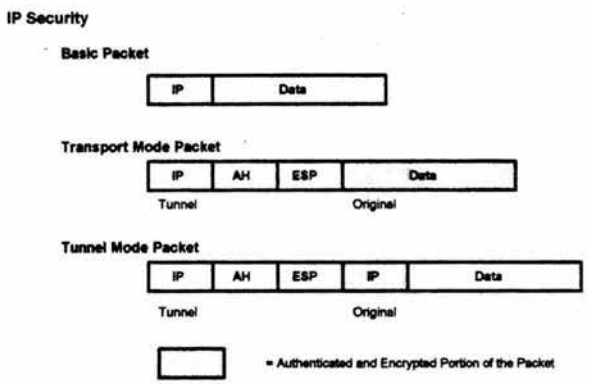


Figura 6.2 IP Sec

Además de estos mecanismos de seguridad contenidos en el túnel IPSec, es necesario establecer ciertas políticas de seguridad por medio de la utilización de un firewall para autentificar a los usuarios remotos de la VPN ya que la estructura de dominios y el sistema de seguridad en general de Windows es deficiente para protegerse del acceso indebido de terceros.

6.4 COMUNICACIÓN A LA RED LAN

En capítulos anteriores ya se definió lo que es un ruteador, switch, servidor, firewall, etc. y los beneficios y limitantes de los mismos, por lo que en este capitulo nos enfocaremos en el estudio de los componentes básicos y describiremos algunos de los principales tipos y marcas de equipos existentes en el mercado nacional.

6.4.1 Ruteador (Router).

De acuerdo a un análisis económico y tecnológico que hemos realizado para TESYS se han comparado diferentes equipos de conectividad de varias marcas. En lo referente a ruteadores dos fueron los más destacados de entre el conjunto seleccionado, debido principalmente a que el soporte técnico ofrecido por los proveedores de Internet (ISP) está enfocado únicamente sobre plataforma Cisco y Lucent.

6.4.1.1 CISCO 2621XM-ADSL

Figure 1
Cisco 2600XM Series Routers

Figura 6.3 Ruteadores Cisco Serie 2600XM

Características generales

a) Permite la comunicación entre la empresa y sus empleados remotos mediante la encriptación estándar 3DES

b) Permite la interacción con VPN's

c) Posee una capacidad de memoria Flash DRAM de 32 MB con posibilidad de incrementarla hasta 96 MB

d) Permite una ideal conectividad con DSL

e) Se venden de manera independiente las tarjetas dependiendo del tipo de conexión y características deseadas (modular)

A continuación se presenta la tabla de comparación de los equipos de esta familia (figura 6.4):

Bundle	Router	IOS Image	WAN Interface Card	Fast Ethernet Ports	Flash (MB)	DRAM (MB)	Router Performance (kpps)
CISCO2611XM-ADSL	2611XM	IP Plus	WIC-1ADSL	2	16	64	20kpps
CISCO2621XM-ADSL	2621XM	IP Plus	WIC-1ADSL	2	32	96	30kpps
CISCO2651XM-ADSL	2651XM	IP Plus	WIC-1ADSL	2	32	96	40kpps
CISCO2611XM-SHDSL	2611XM	IP Plus	WIC-1SHDSL	2	16	64	20kpps
CISCO2621XM-SHDSL	2621XM	IP Plus	WIC-1SHDSL	2	32	96	30kpps
CISCO2651XM-SHDSL	2651XM	IP Plus	WIC-1SHDSL	2	32	96	40kpps

Figura 6.4 Tabla Comparativa

Una característica importante de esta familia de ruteadores es que puede ser optimizada para funcionar mejor sobre VPN's, encriptándo la información dentro de un túnel 3DES mediante IP Sec

a una velocidad de transmisión superior a los 40Mbits. Permitiendo a los consumidores, ya sea por medio de una tecnología ADSL o SHDSL, establecer conexiones remotas de los empleados a sus empresas a un bajo costo.

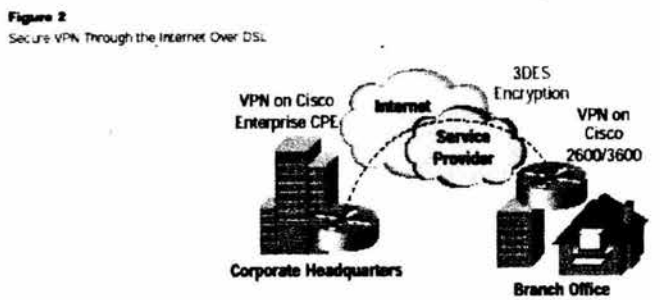


Figura 6.5 Conectividad Punto a Punto con el uso de ruteadores

6.4.1.2 SuperPipe 155 de Lucent Tecnologies

SuperPipe 155, posee un alto desempeño, seguridad, y administración todo en uno. Además, los ruteadores brindan multiservicio para los usuarios concientes de seguridad. SuperPipe es ideal para acceso a Internet, conexiones remotas criticas, redes privadas virtuales (VPN´s) y servicios de voz y datos. SuperPipe 155 integra un rango de interfaces alternativas y provee elecciones de conectividad que los negocios necesitan, incluyendo conexiones duales ISDN BRIs, T1/E1/V.35 para líneas arrendadas dentro de una WAN y jacks duales análogos, así como de avanzadas características de seguridad.

El diseño de todo en uno reduce el costo eliminado la necesidad de software caro para actualizaciones, módulos de memoria, agregar tarjetas, manejar separadamente la VPN y los dispositivos firewall, o externos como son CSUs/DSUs que crean dentro de la red más puntos de posibles fallas.

Figura 6.6 SuperPipe 155

La configuración inicial de un SuperPipe es rápida y fácil de implementar por medio de una interfaz gráfica instalando una aplicación de NavisConnect, y administrando sus opciones incluyendo

SNMP y archivos libremente descargables, permitiendo a los administradores de redes centralizar el control y monitoreo en cualquier parte de la aplicación en donde ellos se encuentren.

Características

a) Alto desempeño con procesadores RISC de alto procesamiento y aplicaciones de misión crítica.

b) Certificado por el estándar ICA como Lucent Secure VPN Solutions Firewall que es un estándar para la protección de las redes de Internet

c) Encripción estándar a 56 bits con IPSec (con posibilidad de incrementarla a 128 bits)

d) Soporte a PAP, CHAP, y Calling Line ID (CLID) como lo es Telnet, SNMP, y perfil de seguridad con password.

e) Transmisión de 10/100 autosensible con Ethernet con fácil migración a redes Fast Ethernet.

f) Soporte a SNMP (MIIB II) – actualizable de manera gratuita.

g) Habilidad a disponer de múltiples perfiles en firewalls lo que significa que todas las interfaces y conexiones a SuperPipe van a filtradas por medio de las políticas de seguridad.

h) Network Addres Translation (NAT) permite a los administradores de redes a no registrar direcciones dentro de su red local y otras redes remotas hasta que acceden a Internet a través de una o más direcciones registradas que son asignadas por medio de un proveedor (ISP, direcciones estáticas o dinámicas)
A continuación se muestra un uso común del ruteador SuperPipe 155 en una empresa con redes remotas y usuarios remotos.

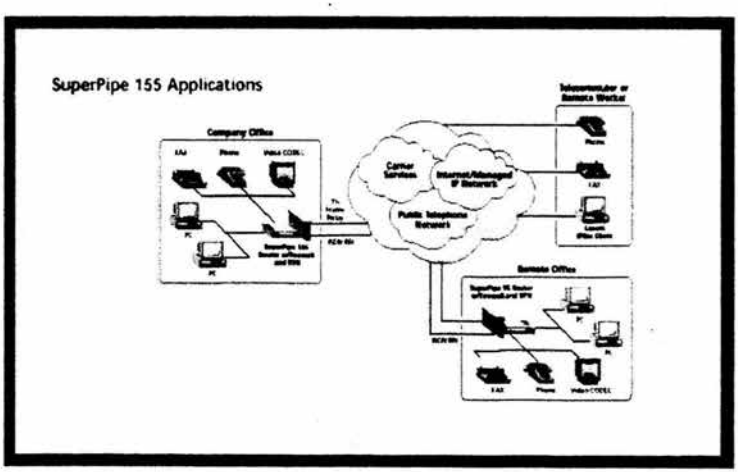


Figura 6.7 Aplicaciones con SuperPipe 155

Adicionalmente el beneficio de estos productos está en la habilitación para proveer conexiones punto a punto, VPN y voz sobre IP para sus suscriptores sin que esto constituya un gran incremento de ancho de banda ni grandes incrementos de seguridad.

Adicional a lo anteriormente descrito, podemos mencionar brevemente la total integración de Superpipe 155 a soluciones de redes remotas. Multiples puertos WAN le dan flexibilidad para conectarse a múltiples rangos de servicios WAN. Oficinas remotas y usuarios de Internet pueden conectarse a servicios Frame Relay no muy caros a una velocidad de transmisión de 64Kbps a 2048Mbps.

a) Circuitos duales BRI disponibles a conexiones de 64Kbps a 256Kbps.

b) Interfaces dedicadas WAN disponibles T1/E1/V.35

c) Asignación de ancho de banda dinámica (Dynamic Bandwidth Allocation - DBA) via MP+, estándar en la industria del protocolo de asignación de ancho de banda dinámica (Bandwidth Allocation Control Protocol -BACP), y Passive DBA para aquellas unidades que no soportan ningún otro protocolo de ancho de banda.

Lucent Secure VPN Solutions ofrece una combinación de firewall dinámicos, que soporta IPSec VPN y autentificación de usuarios en una sólida solución de seguridad. Secure VPN es ideal para empresas que desean seguridad en su información a través de su LAN, oficinas remotas y empleados remotos. También provee de integridad de datos, privacidad y autentificación de datos necesaria cuando se utiliza Internet y se conecta a intranets corporativas.

A continuación se muestra un uso común del ruteador SuperPipe 155 en una empresa con redes remotas, usuarios remotos, dispositivos de seguridad utilizando una conexión E1 o Frame Relay.

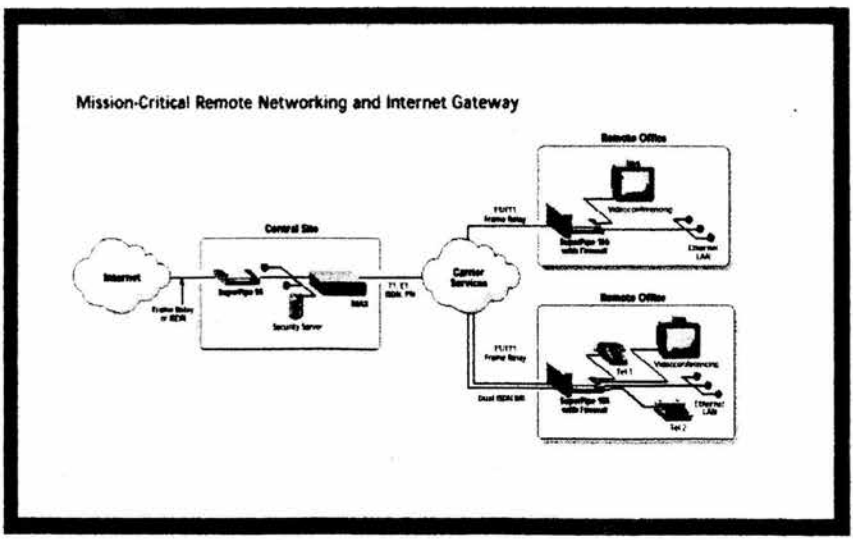


Figura 6.8 Conexiones remotas con SuperPipe 155 y pasarela

A continuación se muestra la distribución de puertos del ruteador SuperPipe 155.

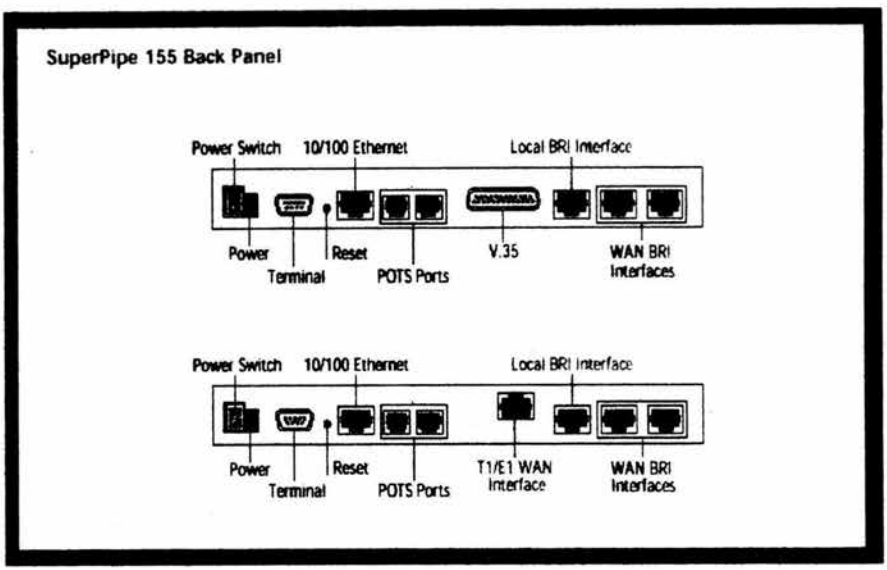


Figura 6.9 Puertos del SuperPipe 155

6.4.2 Muro de Fuego (Firewall).

Para superar los temores y proveer el nivel de protección requerida en la red LAN, TESYS necesita seguir una política de seguridad y la utilización de un muro de fuego que ayude en la prevención del acceso no-autorizado a los recursos propios de la corporación o de la red privada.
A continuación describiremos las principales características de algunos muros de fuego más populares en el mercado nacional con el objeto de tener una idea clara de los aparatos que deberemos tomar en cuenta antes de la decisión final de que muro de fuego utilizaremos en el diseño de solución de conexión remota que le ofreceremos a la compañía TESYS.

6.4.2.1 NOKIA

NOKIA IP380

EL NOKIA IP380 es una plataforma de seguridad diseñada para satisfacer las necesidades de seguridad de las empresas medianas.
Diseñado para trabajar con flexibilidad máxima, el IP380 satisface las necesidades de conectividad de red con 4 puertos de Ethernet integrados completamente ruteables y 2 slots de opción que soportan ya sea tarjetas de WAN o tarjetas duales de puerto Ethernet para hasta 8 puertos 10/100. Dentro de sus nuevas características de serviciabilidad se incluye una bandeja deslizable que permite la instalación fácil y rápida de tarjetas de memoria sin tener que usar los racks de la unidad.

Figura 6.10 NOKIA IP380

Características principales del NOKIA IP380

a) NOKIA IPSO. Sistema Operativo de redes propio de NOKIA integrado con otras aplicaciones diseñadas para soluciones de seguridad.

b) Optimizado para trabajar con Check Point VPN-1 FireWall-1 NG y RealSecure para Nokia.

c) Posee la densidad de puertos más alto en su clase, soportando hasta 8 puertos Ethernet 10/100.

d) Alcanza velocidades de 600 Mbps dentro del alcance de seguridad del Firewall.

NOKIA IP530

Con una plataforma innovadora de seguridad de alto desempeño el NOKIA IP530 es la herramienta óptima para los ambientes de redes más exigentes, tales como los sitios de comercio electrónico con tráfico muy elevado, los almacenes de datos de las grandes corporaciones y los centros de datos de los proveedores de servicios.

El NOKIA IP530 viene equipado con 4 puertos Ethernet 10/100 integrados, 3 slots compactos estándar PCI para soporte de tarjetas de red (incluyendo un puerto individual Ethernet Gigabit de Fibra) y 2 slots PCMCIA para el manejo de MODEM.

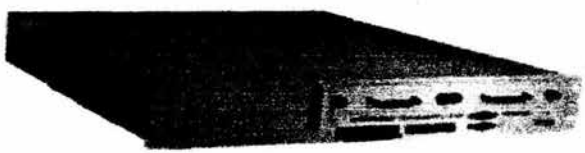


Figura 6.11 Firewall NOKIA IP530

Características principales NOKIA IP530

a) NOKIA IPSO. Sistema Operativo de redes propio de NOKIA integrado con otras aplicaciones diseñadas para soluciones de seguridad.

b) Dispositivo de Firewall/VPN fuertemente integrado con el software de seguridad Checkpoint VPN-1/Firewall-1

c) Detección de intrusos completamente integrado con la aplicación RealSecure para Nokia. (No se requieren instalaciones futuras).

d) Fuerte sistema de densidad de puertos (2 unidades de rack conservan espacio de rack importante).

e) Los slots internos PCM permiten el soporte a hardware robusto de aceleración al mismo tiempo que conserva sus interfaces internas.

NOKIA IP650

El NOKIA IP650 se caracteriza por sus innovadores componentes de "cambio en caliente" tales como las tarjetas de interfase y las bandejas del ventilador que pueden ser removidas y reemplazadas sin que se tenga que tirar la red.
Para medianas y hasta grandes aplicaciones el IP650 provee el tiempo máximo de conexión para las implementaciones de misión crítica. También es posible agregar una fuente de poder opcional "en caliente" para convertir al NOKIA IP650 en un instrumento de seguridad que tolera las fallas eléctricas

Figura 6.12 NOKIA IP650

Características principales NOKIA IP650

a) NOKIA IPSO. Sistema Operativo de redes propio de NOKIA integrado con otras aplicaciones diseñadas para soluciones de seguridad.

b) Dispositivo Firewall/VPN fuertemente integrado con el software de seguridad Checkpoint VPN-1/Firewall-1

c) Detección de intrusos completamente integrado con la aplicación RealSecure para Nokia. (No se requieren instalaciones futuras).

d) La gran cantidad de tarjetas de interfase de red proveen flexibilidad al hacer las conexiones de red.

e) Incrementa grandemente la disponibilidad de la red debido al uso del Protocolo de Redundancia de Ruteador Virtual (Virtual Router Redundancy Protocol; VRRP) y la sincronización de Firewall-1

6.4.2.2 Nortel

El sistema de muro de fuego conmutado Alteon ASF (Alteon Switched Firewall; ASF) es una solución multi-componente que se maneja como un sistema único, este refleja la integración muy estrecha de 2 componentes básicos, un acelerador de firewall conmutado Alteon y hasta 6 directores del muro de fuego conmutado.

El muro de fuego Alteon ASF implementa un plano de control completo del firewall basado en el software líder en la industria, llamado CheckPoint Firewall-1 Next Generation. Con el uso de un conmutador como un acelerador de hardware la sobrecarga de tráfico en la máquina de inspección de firewall puede ser manejada a velocidades de Gigabit mientras se mantiene la completa seguridad del sistema. Con el uso de la tecnología de Check Points Secure XL y la arquitectura de seguridad abierta en redes de Nortel, el director y el acelerador del muro de fuego se entrelazan para realizar la comunicación y descargar las sesiones del muro de fuego en tiempo real.
El director del muro de fuego conmutado Alteon usa el software Firewall-1 y para ejecutar una política de chequeo para cada nuevo requerimiento de conexión maneja las tablas de conexiones y especifica las reglas para el manejo de paquetes en cada sesión.

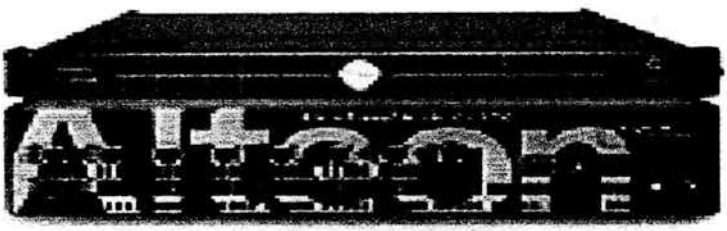


Figura 6.13 Sistema de muro de fuego conmutado Alteon.

Los sistemas de muro de fuego conmutado Alteon ASF se clasifican según el tamaño o la capacidad de la red a proteger en los siguientes tipos:

Sistema de muro de fuego conmutado ASF5710.

Este sistema es el número 1 de las soluciones del muro de fuego de Nortel con un desempeño total que excede los 4Gbps y maneja hasta 32,000 requerimientos de conexión por segundo y hasta un millón de sesiones al mismo tiempo.

Sistema de muro de fuego conmutado ASF5610

Este es un muro de fuego acelerado de alto desempeño que soporta aplicaciones de banda ancha, tráfico irregular sensitivo, y gran número de usuarios simultáneos. Este muro de fuego puede ser utilizado en Intranets y en centros de almacenamiento de datos corporativos. Este muro de fuego es capaz de correr hasta 100 dominios virtuales con el software de check Point FW-1 VSX y cada uno con diferentes políticas de acceso, y por lo mismo puede ser usadas para clientes o para diferentes grupos y departamentos dentro de una red corporativa.

Sistemas de muro de fuego conmutado ASF5408 y ASF5308

Ideales para soluciones en perímetros de seguridad en empresas medianas o partes medianas de la red de una corporación grande. Estos sistemas también cuentan con un nivelador de carga del firewall incluido, chequeo de sanidad de la red y escalabilidad.

Características principales del sistema de muro de fuego conmutado Alteon.

a) Desempeño Multi-Gigabit

b) Disponibilidad alta de la red.

c) Uso del Software FW-1 NG que pertenece a la tecnología de Check Point.

d) Funcionamiento Plug and Play

e) Escalable y muy manejable (tamaño pequeño).

6.4.2.3 CISCO PIX

La serie de muro de fuego CISCO PIX provee una gran seguridad en un dispositivo firewall de hardware/software integrado muy fácil de instalar que ofrece un desempeño sobresaliente. La familia líder a nivel mundial en firewall PIX de CISCO extiende el espectro de seguridad completa del dispositivo desde un muro de fuego plug and play de desktops para oficinas móviles hasta muro de fuego de Gigabits de clase transportadora para los ambientes empresariales más demandantes y los ambientes de proveedores de servicios. Los CISCO PIX proveen un rendimiento sobresaliente para hasta 500,000 conexiones simultáneas y un ancho de banda cercano a los 1.7 Gbps, ancho de banda en el cual provee una seguridad e clase mundial, confiabilidad y servicio a clientes

CISCO PIX501

El CISCO PIX501 provee seguridad de tipo innovador para oficinas pequeñas y teletrabajadores con un dispositivo plug and play de seguridad confiable ideal para asegurar ambientes de banda ancha y altas velocidades que necesitan estar siempre activos. El CISCO PIX501 es parte de la serie de muro de fuego líder del mercado CISCO PIX y provee capacidades robustas de seguridad, tamaño pequeño, y poderosas capacidades de manejo remoto por medio de un equipo compacto de soluciones all-in-one.
Ofreciendo seguridad de tipo innovador para ambientes de oficinas pequeñas, el CISCO PIX501 es un dispositivo de seguridad de propósito predefinido que provee un gran numero de servicios de seguridad incluyendo la inspección completa del estado de la red, trabajo en redes virtuales (VPN) y protección contra intrusos en un sólo dispositivo. Con el uso del algoritmo de seguridad adaptable de CISCO y el sistema operativo PIX, el PIX501 asegura que todos los usuarios dentro del alcance del firewall estén sanos y seguros contra ataques provenientes del Internet. Su poderosa tecnología de firewall de inspección del estado de la red mantiene records del estado de todos los usuarios autorizados, requerimientos de la red y previene los accesos no autorizados a la misma.
El CISCO PIX501 puede también asegurar todas las comunicaciones de red entre las oficinas remotas y las redes corporativas a través de Internet con el uso de su llave de Intercambio de Internet de bases estándar (IKEI), el IP Security (IPsec) y sus capacidades e VPN.

Figura 6.14 CISCO PIX501

Con la encriptación de datos realizada con el estándar de encriptación de datos de 56 bits (DES) o con el DES avanzado de 156 bits llamado de triple encriptación (3DES) los datos corporativos viajan de forma segura a través de Internet.

CISCO PIX506E

El CISCO PIX506E, el cual es una versión aumentada del muy popular CISCO PIX506, provee una seguridad de clase innovadora para ambientes de oficinas remotas en un instrumento robusto y confiable.
Ideal para asegurar las conexiones de Internet de una oficina o sección remota el CISCO PIX506E parte de la serie líder en el mercado de CISCO PIX, el cual provee un rango de capacidades de seguridad y capacidades poderosas de manejo remoto en una solución de costo razonable y alto rendimiento. El PIX506E también provee un rendimiento de 3DES VPN mejorado con hasta 70% más rendimiento que el PIX506 cuando esta usando ciertas aplicaciones.

El CISCO PIX506E es un dispositivo de propósito predefinido que provee grandes servicios de seguridad incluyendo la inspección muro de fuego de estado de la red, Red Privada Virtual (VPN) y protección de intrusos en un sólo dispositivo.

Figura 6.15 CISCO PIX506E

6.4.3 Conmutador (Switch)

En cuanto al conmutador, se realizó un análisis comparativo entre los proveedores de conmutadores más reconocidos en el mercado. Por lo cual se consideran marcos como son: 3Com, Cabletron y Enterasys a continuación se resumen sus principales características.

Empezando con los productos de Cabletron que cumplen con nuestras necesidades podemos mencionar a los siguientes:

6.4.3.1 Cabletron

SmartSwitch 6000

a) Conmutador de 5 slots que soporta hasta 120 puertos Ethernet o 40 puertos FastEthernet, así como enlaces de alta velocidad FastEthernet conmutados, FDDI, ATM o WAN.

- ancho de banda de hasta 3,2 Gbps
- potencia de conmutación de 2.000.000 pps

b) Tolerancia a fallos:

-administración distribuida sobre cada módulo
- motor de conmutación incluido en cada módulo
- redundancia de tomas

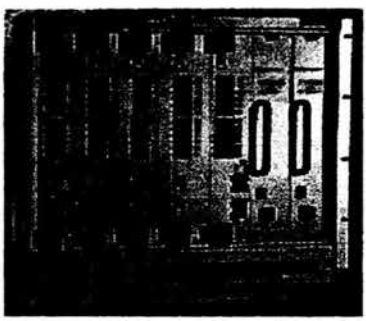


Figura 6.16 SmartSwitch 6000

SmartSwitch 2200

a) Conmutador autónomo de gran rendimiento dotado de 24 puertos Ethernet y 2 puertos FastEthernet modulares y conmutados, así como un enlace de gran flujo FDDI, ATM o WAN.

b) Este elevado rendimiento le permite ser utilizado como conmutador de estaciones de trabajo o como conmutador de grupo de trabajo alimentando el backbone de edificios y campus.

c) Potencia de conmutación de 400.000 pps

Figura 6.17 SmartSwitch 2200

6.4.3.2 Enterasys

Ahora analizando algunos de los productos de Enterasys, mencionaremos los siguientes: VH-2402S2, y Matrix E1.

A continuación se ilustra la familia de conmutadores dentro de Enterasys:

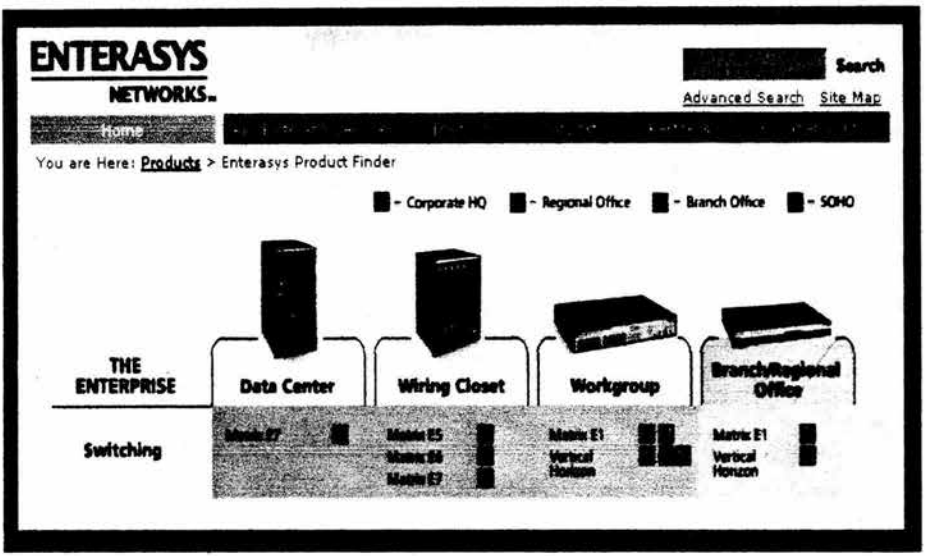


Figura 6.18 Productos de Enterasys

Enterasys Vertical Horizon VH-2402S2

El Vertical Horizon Fast Ethernet Stackable Switch (VH-2402S2) provee de 24 puertos RJ45 a 10/100 Mbps y dos slots para expansión, como también de un slot dedicado. Gran desempeño en velocidad y en la industria permite que VH-2402S2 integre a pequeñas y medianas redes.

El VH-2402S2 provee de conexiones a 10/100Base-TXpara conexiones de alto desempeño de workstations, archivos de servidor, switch de escritorio y accesos compartidos de hubs. Dos slots modulares opcionales 100Base-FX y 1000Base-X escalables que le permiten a los clientes flexibilidad en su infraestructura de conexión y capacidad de conectar múltiples switch.

Especificaciones técnicas:

Especificaciones Físicas	
Dimensiones	6.4 cm (2.53") H x 44 cm (17.37") W x 28.5 cm (11.22") D
Peso	4.82 kg (10.63 lbs)
Opción de interfaces	24 ports of 10Base-T/100Base-TX RJ45 and 2 option slots for uplinks and/or expansion modules
Memoria principal	8 MB
Buffer de Memoria	128k for 10/100 port; 2 MB for 1000 Mbps port
Memoria Flash	2 MB
Tamaño de tabla de direcciones	8k entries
Técnicas	
Performance Throughput Capacity	6.55 Mpps (single unit)/45.85 Mpps (7 high stack); all calculations based on 64 bytes per packet
Capacidad de ancho de banda	16 Gbps
MTBF (predicted)	6 years
Especificaciones Ambientales	
Temp. de Operación	32° to 122° F (+0° to +50° C)

Humedad de operación	5 to 95% (non-condensing)
Operación de voltaje	100 to 240 VAC
Agencias y Especificación de Estándares	
Seguridad	UL1950, CSA C22.2 No. 950, EN60950, IEC950, 72/73/EEC
Compatibilidad Electromagnética	FCC Part 15, CSA C108.8, 89/336/EEC, EN 55022, EN 61000-3-2,EN 61000-3-3, EN 50082-1, AS/NZS 3548, VCCI V-3

Enterasys Matrix E1

Ideal para desempeño en trabajo en grupo, el Matrix E1 1H582-51 Workgroup Switch (WS) y el 1G582-09 Gigabit Workgroup Switch (GWS) son conmutadores de nivel 3 con funcionalidad completa de ruteo. El 1H582-51 provee de 48 puertos Ethernet y 3 slots expandibles, mientras que el Matrix 1G582-09 provee de 5 puertos RJ45 10/100/1000Base-TX mejorados como también de 3 slots expandibles. En los conmutadores Matrix WS y GWS la expansión de slots soportan conectividad 10/100 y Gigabit Ethernet

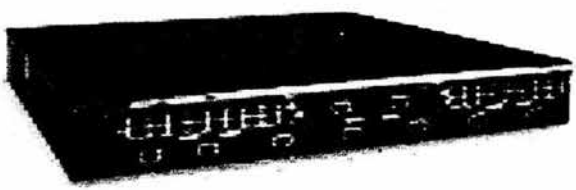


Figura 6.19 Matrix E1

Especificaciones técnicas:

Technical Specifications	
Switching Bandwidth	24 Gbps
MAC Address Capacity	64,000
VLAN Capacity	3,000
Flash Memory	8 MB
DRAM	64 MB expandable to 256 MB
Power System	AC Input Power (auto-sensing) 85 VAC - 264 VAC
Heat Dissipation	173 BTU/hr maximum
ACVA Rating	54 ACVA maximum
System LED Indicators	Power Supply Status CPU Status Port Status (link and activity)
System MTBF	>91,000 hours predicted
Media Type Supported	1H582-51 48 10/100 RJ45 ports, 3 expansion slots 1G582-09 6 fixed 10/100/1000Base-TX ports, 3 expansion slots 1H-16TX 16 10/100 RJ45 ports 1G-2GBIC 2 GBIC ports 1G-2TX 2 1000Base-T RJ45 ports
Management Access	
In band	SNMP, HTTP, Telnet
Out of band	Serial RS-232 COM port
Physical	
Dimensions	8.9 cm (3.5") H x 44.45 cm (17.5") W x 43.9 cm (17.3") D
Rack Unit Height	2
Weight	8.75 kg (19.23 lb)

Environmental	
Operating Temperature	5° C to +40° C (41° F to 104° F)
Non-Operating Temperature	-30° C to 73° C (-22° F to 164° F)
Operating Humidity	5%-90% RH, non-condensing
Agency and Standards Specifications	
IEEE Standards	IEEE Standards Support IEEE 802.3 IEEE 802.3ad IEEE 802.1D 1998 IEEE 802.1Q IEEE 802.1w IEEE 802.1X

6.4.3.3 3COM

Finalmente analizaremos las características que tienen en especial la familia de 3COM Switch 4000

3Com® 4000

a) La familia 3Com® 4000 proporciona switching Gigabit y Fast Ethernet versátil y resistente ante fallas con capacidades multilayer avanzadas para configuraciones del core de la red y agregación de switch de borde particularmente exigentes. Esta familia se compone de dos categorías: modulares de alto rendimiento 3Com 4005 y 4007/4007R, y core conmutador únicamente Gigabit de configuración fija 3Com 4050 y 4060.

b) El 3Com 4005 es una solución de switching de Layer 3 rica en características y económicamente asequible para empresas que no necesitan un ruteador caro. Este conmutador de chasis es escalable de 8 a 96 puertos Fast Ethernet y de 1 a 24 puertos Gigabit Ethernet.

c) El 3Com 4007 y el 4007R ofrecen switching de alta densidad altamente customizable con hasta 216 puertos Ethernet/Fast Ethernet o 54 puertos Gigabit Ethernet, y proporcionan enrutamiento IP, IPX, y AppleTalk. El conmutador 4007R se entrega con un slot de chasis adicional para que un conmutador Fabric redundante proporcione el mayor nivel de disponibilidad de la red.

d) Los 3Com 4050 y 3Com 4060 ofrecen una combinación única de rendimiento, disponibilidad y flexibilidad en configuraciones compactas y duraderas. Un slot de expansión en cada conmutador soporta un módulo Gigabit adicional de 4 puertos. Ambos soportan la tecnología XRN™ de alto rendimiento y tolerante a fallas que utiliza múltiples conmutadores distribuidos configurados como un Fabric Distribuido XRN.

3Com® 4005

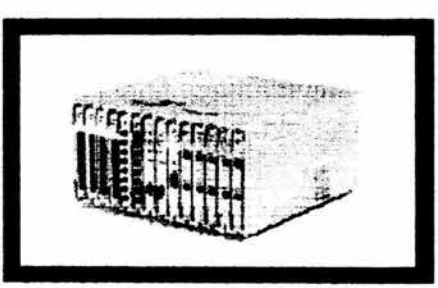


Figura 6.20 Conmutador 4005

Características y ventajas:

a) Switching Modular para Grupos de Trabajo

b) La modularidad del Switch 4005 de 3Com hace que sea ideal para la agregación Fast Ethernet de PCs, o en el núcleo de una pequeña red.

c) La posibilidad de añadir al chasis o a los Starter Kits módulos adicionales Fast Ethernet ó Gigabit, para fibra óptica o cable de cobre, permite adaptar el conmutador 4005 a los cambios necesarios a medida que crezca la red.

d) El soporte para 100Base-FX hace que el conmutador 4005 de 3Com sea un agregador ideal para Fast Ethernet de fibra óptica en el PC, o para la conectividad de larga distancia con una buena relación precio-rendimiento.

e) El 4005 de 3Com ofrece la redundancia hardware necesaria, con capacidad para soportar conmutador fabrics y fuentes de alimentación redundantes. Las características de resistencia ante fallos del software tales como OSPF y Agregación de Enlaces ayudan a garantizar la disponibilidad del 4005.

f) El soporte para switching de Layer 3 permite la futura protección y seguridad mediante el uso de Listas de Control de Acceso.

g) 3Com 4005 Version 2.0 Advanced Software ahora incluido como standard en todas las nuevas adquisiciones del producto (se requiere registrar el producto).

h) El chasis de 14 ranuras puede escalarse hasta 96 puertos Fast Ethernet ó 24 puertos Gigabit Ethernet, con 2 ranuras para las configuraciones de doble conmutador fabric resistente a fallos

i) Módulos Fast Ethernet de 8 puertos para cable de cobre y para fibra óptica, con switching local para óptimo rendimiento

j) Módulos Gigabit Ethernet de puerto simple y doble para cable de cobre, fibra óptica y GBIC, con switching local para óptimo rendimiento

k) Rápida instalación plug-and-play y fácil operación, con módulos intercambiables en caliente (hot-swappable) para ampliar los Starter Kits del conmutador 4005

l) Switching Layer 3 wire-speed, para las tareas de networking más exigentes

m) Soporta RIP v1, RIP v2, OSPF, y DVMRP

n) Soporta LANs virtuales y 802.1Q VLAN tagging, filtrado multicast, y RMON

o) Soporte multimedia para switching desde Layer 2 hasta Layer 4

p) Diseño redundante que proporciona un 100% de disponibilidad

q) Puede administrarse vía Telnet, interfaz integrada de administración web o mediante el 3Com Network Supervisor

3Com® 4060

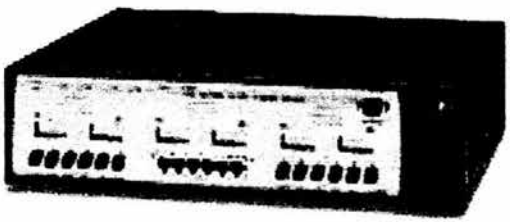


Figura 6.21 Conmutador 4060

Características y ventajas:

Switching Gigabit de alta disponibilidad para el LAN Core.

a) Diseñado para los requerimientos más exigentes de la red troncal de las redes empresariales, el 3Com® 4060 ofrece una combinación exclusiva de rendimiento, disponibilidad y flexibilidad.

b) El chasis de metal duradero es una unidad compacta de 2RU de alto, instalable en un armazón que está equipada con seis puertos 1000BASE-SX y seis puertos GBIC para conectividad con la red troncal, así como 12 puertos integrados 10/100/1000 para conexiones con los servidores.

c) Las funciones de tolerancia a fallas incluyen fuentes de poder modulares, con cargas compartidas con tecnología hot-swap; bandejas de poder modulares con tecnología hot-swap; y transceptores GBIC con tecnología hot-swap. Además se le puede instalar una fuente de poder adicional para gozar de mayor redundancia de potencia.

d) El 3Com 4050 soporta el software 3Com Gigabit Multilayer Switching, que ofrece funcionalidades de Layer 2 con extensas características, switching de Layer 3 para redes IP, y avanzadas capacidades de priorización de tráfico y seguridad para ajustarse a los requerimientos siempre crecientes de core backbones Gigabit.

e) La tecnología 3Com XRN™ (eXpandable Resilient Networking) permite la implementación de configuraciones de alta disponibilidad usando dos 4050s o 4060s interconectados, escalando el backbone a 48 puertos de switching Gigabit de Layer 3 con capacidad wire-speed (con la compra opcional del 3Com XRN Interconnect Kit).

f) Las funcionalidades avanzadas Layer 2 y Layer 3 tales como filtración multicast, servicios mejorados de calidad de servicio y clase de servicio (QoS / CoS, por sus siglas en inglés), LANs virtuales, y la clasificación y establecimiento de prioridades de tráfico en múltiples niveles, proveen control de tráfico en toda la red

g) La arquitectura ASIC desarrollada por 3Com ofrece capacidad de switching de 56 Gbps en múltiples niveles por unidad, rendimiento wirespeed en todos los puertos, y una velocidad de envíos de más de 41 millones pps

h) Las capacidades de switching Layer 3 tales como IP unicast utilizando rutas estáticas, RIP/RIPv2 y CIDR ayudan a mejorar el rendimiento, proveen control y seguridad de la red, y capacitan el enrutamiento entre VLANs

i) Soporte para características software de alta disponibilidad tales como Agregación de Enlaces usando 802.3.ad, Enlaces Redundantes, Spanning Tree y Rapid Spanning Tree (802.1w), siete grupos de RMON, y alertas por e-mail

j) Características de seguridad como soporte de cliente RADIUS y listas de control de acceso enrutado protegen la información sensible de la red y garantizan que los usuarios tienen acceso a recursos autorizados

k) Una redirección transparente del webcache permite que el tráfico Web sea redirigido automáticamente a un 3Com SuperStack® 3 Webcache, facilitando así la administración

l) Los módulos de expansión adicionales 1000BASE-SX, 1000BASE-T, 1000BASE-LX y basados en GBIC ofrecen cuatro puertos de switching rico en funcionalidades de alto rendimiento, sobre cobre o fibra multi-modalidades

3Com® 4005 Copper Fast Ethernet Starter Kit de 40 puertos

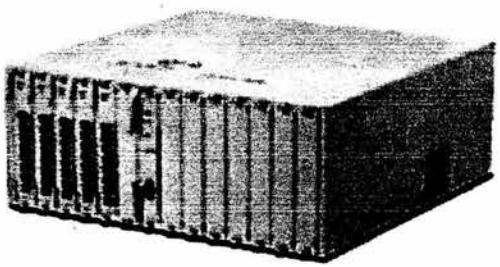


Figura 6.22 Conmutador 4005

Características y ventajas

a) Switching Modular para Grupos de Trabajo

b) La modularidad del 4005 de 3Com hace que sea ideal para la agregación Fast Ethernet de PCs, o en el núcleo de una pequeña red.

c) Este Starter Kit proporciona 40 puertos de conectividad Fast Ethernet a cable de cobre, con capacidad para soportar otros siete módulos I/O.

d) 3Com 4005 Version 2.0 Advanced Software ahora incluido como standard en todas las nuevas adquisiciones del producto (requiere registrar el producto).

e) El chasis de 14 ranuras puede escalarse hasta 96 puertos Fast Ethernet ó 24 puertos Gigabit Ethernet, con 2 ranuras para las configuraciones de doble conmutador fabric resistente a fallos

f) Rápida instalación plug-and-play y fácil operación, con módulos sustituibles en caliente para ampliar los Starter Kits del Switch 4005.

g) Swtching Layer 3 wire-speed, para las tareas de networking más exigentes.

h) Soporta RIP v1, RIP v2, OSPF, y DVMRP

i) Soporta LANs virtuales y 802.1Q VLAN tagging, filtrado multicast, y RMON

j) Soporte multimedia para switching desde Layer 2 hasta Layer 4

k) Diseño redundante que proporciona un 100% de disponibilidad

l) Puede administrarse vía Telnet, interfaz integrado de administración web o mediante el 3Com Network Supervisor.

6.4.4 Servidores

Las siguientes tablas muestran diferentes modelos de servidores con sus respectivas especificaciones técnicas:

6.4.4.1 ProLiant DL320

Figura 6.23 Servidor ProLiant DL 320

Ambiente ideal:

a) Proveedores de servicio local y emergente.

Uso típico:

a) Servidor de Web, Vídeo, Aplicaciones Media, Pasarelas, DNS, Muro de Fuego y Aplicaciones Web.

Problemas y Requerimientos:

a) Requiere de bajo costo y es un rack ultra denso

b) Necesita flexibilidad para desplegar una variedad de racks

c) Como todos los Proliant, el DL320 tiene soporte en las industrias, permitiendo verdadera seguridad en un sistema remoto desde cualquier sitio web en el mundo

Resolviendo problemas a usuarios:

a) El Proliant DL320 proporciona al cliente un sistema diseñado para sus requerimientos, sin tener que pagar un alto costo innecesariamente por ciertas características
Servicios

El Proliant DL320 nos permite encontrar servicios a bajo costo

a) 1U/1P Tecnología que permite el uso óptimo del espacio en la base de datos sin exorbitantes costos

b) Opción a múltiples racks

c) El servicio y el soporte de Proliant garantizan la seguridad de la completa solución

MODELOS EN COMPARACIÓN

	DL320	DL360	DL380G2
Processor	Pentium III 1.0GHz or 800MHz FC-PGA	Pentium III 1.26GHz or 1.13GHz with 512k cache FC-PGA or Pentium III 1.0GHz, 933MHz or 866MHz FC-PGA	Pentium III 1.26GHz or 1.13GHz with 512k cache FC-PGA 1
MP	1P	1-2P	1-2P
RAM Slot/Max	128MB / 2GB	128MB / 4GB	256MB / 6GB
Drive controller	Ultra ATA/100 (ATA models); Wide Ultra2 SCSI (SCSI models)	Integrated Smart Array Controller	Integrated Smart Array 5i Controller, with 32MB memory
NIC	Two Compaq NC3163 Fast Ethernet NIC Embedded 10/100 WOL (Wake On LAN)	Two Compaq NC3163 Fast Ethernet NIC Embedded 10/100 WOL (Wake On LAN)	Two Compaq NC3163 Fast Ethernet NIC Embedded 10/100 WOL (Wake On LAN)
Hard Drive Bays	2 x 1" ATA or Ultra2/3 SCSI non Hot-Plug	2 x 1" Ultra2/3 Hot-Plug	5 x 1" Ultra3 hot plug drive bays 1x1.6" Ultra3 HP drive or tape drive bay
Slots	1 Total =1-64bit PCI	2 Total =1-64bit PCI , 1-32bit PCI	3 PCI expansion slots (2 x hot plug 64-bit/66MHz and 1 x 64-bit/33MHz)
Chassis	1U Rack	1U Rack	2U Rack
Software and Server Management	SmartStart, Compaq Insight Manager XE, ActiveUpdate, Compaq Availability Agents	SmartStart, Compaq Insight Manager XE, ActiveUpdate, Compaq Availability Agents	SmartStart, Compaq Insight Manager XE, ActiveUpdate, Compaq Availability Agents

6.4.4.2 ProLiant DL 320 G2

Figura 6.24 Servidor ProLiant DL 320 G2

Ambiente ideal:

a) Proveedores de servicio y centro de datos

Uso típico:

a) Servidor para varias funciones sencillas: Web, Vídeo y Aplicaciones Media

b) Servidor usado como controlador de dominio, Pasarelas, DNS, Aplicaciones Web, Muro de Fuego

Resolviendo problemas a usuarios:

a) 1U/1P Tecnología que permite el uso óptimo del espacio en la base de datos sin exorbitantes costos

b) Pentium 4 a 2.26GHz/512K cache, PC2100 ECC DDR SDRAM, 2 gigabit NICs

c) Opción de múltiples racks, para incrementar el desarrollo

d) Como todos los Proliant, el DL320 tiene soporte en las industrias, permitiendo verdadera seguridad en un sistema remoto desde cualquier sitio web en el mundo

e) El servicio y el soporte de Proliant garantizan la seguridad de la completa solución

MODELOS EN COMPARACIÓN

	DL320G2	DL360G3	DL380G3
Processor	2.26GHz P4 (1P)	2.4 and 2.8GHz Xeon (2P)	2.4 and 2.8GHz Xeon (2P)
Processor Cache	512k L2	512k L2	512k L2
FSB	533MHz	533MHz	400MHz
Drive Controller	ATA/100 standard (supports RAID 1 or 0), optional Slot-less SCSI U3	Embedded Smart Array 5i	Embedded Smart Array 5i+
NICs	Dual 10/100/1000	Dual 10/100/1000	Dual 10/100/1000
Memory	PC2100, 266MHz, 1 DIMM at a time	PC2100, 266MHz, 2:1 interleaved	PC2100, 200MHz, 2:1 interleaved
Drive bays	2 non-hot plug	2 - 1.0" (U320 drives only)	5x1.0" and 1x1.6"
Management	Optional RILOE II in a slot	Embedded iLO	Embedded iLO
I/O slots	1 PCI	1 or 2 PCI-X (1 with redundant power installed, 2 without)	3 PCI-X slots, 2 hot plug
Max Memory	4GB ECC DDR SDRAM	8GB ECC DDR SDRAM	6GB ECC DDR SDRAM
Power supply	Non-HP, non-redundant	HP, redundant	HP, redundant
Fans	Non-HP, non-redundant	HP, redundant	HP, redundant

6.4.4.3 ProLiant ML310

Proliant digno de confianza y fácil de usar para sofisticadas empresas y soluciones de oficina.

Figura 6.25 Servidor ProLiant ML 310

Ambiente Ideal

a) Empresas en desarrollo y aplicaciones en pequeños negocios

Problemas y Requerimientos

a) Depende de las aplicaciones de la empresa, necesita de un servidor seguro para estas aplicaciones

b) Las empresas no pueden tener los medios para perder clientes o contabilizar datos, necesitan calidad emprendedora de protección de datos a un costo razonable

c) Necesitan un servidor que sea fácil de organizar y mantener

Uso Típico

a) Archivos/Impresoras/Fax, Web, correo electrónico

b) Aplicaciones como CMR, ERP, SCM

c) Base de datos pequeñas o de grupo

d) Muro de Fuego, DNS

MODELOS EN COMPARACIÓN

	ML330	ML330e	ML330G2
# of Users	<100	<100	<100
processor	667MHz - 1.0GHz PIII, 256K iL2 cache, 1 standard	800MHz, 933MHz, or 1.0GHz PIII, 256K iL2 cache standard	1.26GHz 512K iL2 cache or 1.4GHz 512K iL2 cache, 1 standard
MP	1P	1P	1-2P
Chipset	ServerWorks 3.0 LC	ServerWorks 3.0 LC	ServerWorks 3.0 LE
RAM std/max	64MB/2GB	64MB/2GB	128MB/4GB
drive controller	Integrated, single-channel Ultra2 SCSI	Integrated, dual-channel Ultra ATA-100	Integrated, dual-channel Ultra3 SCSI (SCSI models) or Integraed, dual-channel Ultra ATA-100 w/ Integrated ATA RAID 0, 1, & 1+0 support (ATA models)
NIC	Integrated NC3163 Fast Ethernet 10/100 Wake on LAN)	Integrated NC3163 Fast Ethernet 10/100 Wake on LAN)	Integrated NC3163 Fast Ethernet 10/100 Wake on LAN)
hard drive bays	2 non-hot-plug	2 non-hot-pluge	2 non-hot-plug
Removable Media Bays	4x1.5" (3 available) Support NHP Drives, AIT, DAT	4x1.5" (3 available) Support NHP Drives, AIT, DAT	4x1.5" (3 available) Support NHP Drives, 2-bay HP SCSI cage, AIT, DAT
slots	2 X 64bit; 3 X 32bit (33MHz)	2 X 64bit; 3 X 32bit (33MHz)	4 X 64bit; 1 X 32bit (33MHz)

6.4.4.4 ProLiant ML330 G2

Figura 6.26 Servidor ProLiant ML 330

Ambiente ideal

a) Oficinas pequeñas de menos de 100 clientes

Problemas de Usuario:

a) Necesita un servidor confiable y precio justo

b) Requiere de un servidor que sea fácil de organizar al igual que el mantenimiento y el servicio

c) Requiere de un completo soporte, flexibilidad y opciones de financiamiento

Uso Típico:

a) Archivos/Impresoras

b) Bases de Datos pequeñas

c) Correo Electrónico/ Acceso a Internet

d) Pasarelas, DNS, Muro de Fuego

e) Funciones de Red

MODELOS EN COMPARACIÓN

	ML350G2	ML310	tc2110
Processor support	2P Intel Xeon, 400MHz FSB	1P Intel Pentium 4 533MHz FSB	1P Intel Pentium 4 or Celeron, 400MHz FSB
Chipset	ServerWorks GC LE	ServerWorks GC SL	Intel 845
RAM Slots/Max	256MB / 8GB DDR SDRAM, (4) sockets, interleaving capable	256MB / 4GB DDR SDRAM, (4) sockets, no interleaving	128MB / 1.5GB SDRAM, (3) sockets, no interleaving
Int. HDD Controller	dual channel U3	single channel U3 or dual channel ATA-100 w/integrated ATA RAID	single channel U3 (PCI card) or dual channel ATA-100
Hard Drive only bays	(6) 1" HP HDDs	(2) 1" NHP HDDs	(2) 1" NHP HDDs
Ram media bays	(4) 1.6" (2 avail), DAT/AIT/2-Bay HP drive cage/NHP HDD	(4) 1.6" (3 avail), DLT/DAT/AIT/2-Bay HP drive cage/NHP HDD	(3) 1.6" (2 avail), DAT/NHP HDD
I/O slots	(5) avail: (4) 64-bit 100MHz PCI-X; 1 32-bit 33MHz PCI	(4) 64-bit 33MHz PCI	(3) 32-bit 33MHz PCI
Integrated NIC	Broadcom 10/100/1000 (NC7760)	Broadcom 10/100/1000 (NC7760)	Intel 10/100
Chassis	(5U) T & R models; R conv. Kit, Quick Deploy Rails	(5U) T; R enabling kit, Quick Deploy Rails	T only
RILOE support	Yes	Yes	No
Smart Array Support	Yes	Yes	No
ProLiant Essentials support	Yes	Yes	No

Una vez que ya definimos los requerimientos mínimos necesarios para realizar la conexión remota en esta propuesta de solución para TESYS, en el siguiente capítulo diseñaremos y desarrollaremos la red VPN que proponemos como solución a las necesidades de acceso remoto que tiene esta compañía actualmente.

CAPÍTULO 7

DISEÑO DE LA RED PRIVADA

7.1 JUSTIFICACIÓN DE LA SOLUCIÓN

En el capítulo 1 se mencionó la problemática de TESYS, para lo cual se propuso un sistema de conexión remota que abarcara alguno de los dos siguientes escenarios de conexión:

7.1.1 Primer Escenario. Pasarela para Red Privada (VPN Gateway)

En este primer escenario mencionamos que a manera de reducir el movimiento de los empleados desde las instalaciones del cliente a las oficinas de TESYS, la necesidad de lugares de trabajo en las instalaciones de la compañía, los viajes al interior de la República y la lentitud en los tiempos de respuesta de procesos administrativos, se proponía la creación de una Red Privada Virtual (VPN) por medio de la cual se logrará la conexión remota entre la PC portátil y la red de la compañía. De esta manera los empleados tendrían la capacidad de accesar y actualizar las bases de datos de TESYS, con solo tener un acceso a Internet, ya sea en la Ciudad de México o en el interior de la República.
El propósito principal de este escenario es que los empleados se pudieran conectar desde las oficinas de los clientes o desde sus casas por medio de una conexión telefónica. Para lograr esta conexión es necesario la construcción de un túnel entre la red telefónica pública y la red LAN de TESYS (mediante un acceso dedicado), el cual funcionará mediante la instalación de un software en cada PC portátil. Las comunicaciones en una VPN estarán protegidas ya que en este tipo de redes solo se permite la comunicación entre direcciones pertenecientes a la misma, aun así, con el objeto de robustecer la seguridad, se propone que la información que se transmite esté siempre encriptada al momento de realizar cualquier intercambio de información.

7.1.2 Segundo Escenario. Servidor para Acceso Remoto (RAS)

Para este tipo de conexión se mencionó que era necesario que TESYS cuente con un servidor de acceso remoto RAS (Remote Server Access), un banco de 30 modems y dos enlaces E1 de 30 troncales digitales cada uno para la conectividad de los usuarios de acceso remoto. Además, como en el primer escenario, la compañía deberá proveer a los empleados una PC portátil con el software necesario para hacer este tipo de conexión. Para lograr este tipo de comunicación los empleados deberán comunicarse al número 01-800 asignado a los enlaces E1, los cuales recibirán la llamada y la asignarán a una línea desocupada en ese momento, ya posteriormente, y por medio del RAS, obtendrán el acceso a la red LAN.

Para llevar a cabo cualquiera de las dos soluciones anteriores, también se mencionó que serán candidatos los empleados que trabajen en el desarrollo y diseño de aplicaciones o soluciones completas, en equipos de soporte y mantenimiento o help desk y algunos de los empleados de las áreas de recursos humanos, calidad y gerencia, Pero en el caso de que el crecimiento no sea el esperado con esta solución, se podría pensar en reducir los costos de operación que se tienen actualmente en las instalaciones de TESYS.

7.2 ESTUDIO ECONÓMICO

A continuación un cuadro en el que se muestra el estudio económico del primer escenario de conexión remota propuesto para solucionar las necesidades de TESYS.

1er ESCENARIO		INSTALACION	RENTA		
Rubro	**Descripción**	**Cargo Único**	**12 Meses**	**24 Meses**	**36 Meses**
VPN GATEWAY	Contivity 1600, 200 tuneless, Doble puertos 10/100 Ethernet LAN, 1 Slot PCI Exp, Server S/W con (128- Bit). Licencias ilimitadas de encripción Ipsec con software de cliente	$8,620	$9,024	$6,317	$5,234
Telefonía Local	1 Enlace E1 (2048Kbps) con 30 troncales	$135,900	$13,500	$13,500	$13,500
Acceso a Internet en TESYS	Enlace dedicado E1 (2048Kbps) a Internet en las oficinas de TESYS para 300 usuarios	$90,971	$54,416	$51,688	$43,506
(100) Cuentas Dial Up	Cuentas de acceso remoto a Internet con roaming nacional y sin límite de tiempo de conexión	-	$8,367	$7,446	$7,446
Ruteador	Cisco 2621 XM Interfaces LAN: 2, 10/100 Mbps. Interfaces de voz: 12, digitales G.703 (Conexión a PBX en E1 solo 12 canales) Interfaces WAN: 2, G.703	$13,100	$10,610	$5,510	$4,250
Firewall	PIX 515E, 6 puertos ethernet, peocesador 433Mhz, 64MB RAM, 16 MB Flash	$3,710	$3,000	$1,560	$1,210
(3)Switch	Smart Switch 6000, 5 slots que soporta hasta 120 puertos Ethernet o 40 puertos FastEthernet	$57,584	-	-	-
(3) Servidores	ProLiant DL360 G2 Intel® Pentium® III Processor 1.40GHz/133 Rack Model (256MB) - Power Pick	$62,940	-	-	-

Ahora un cuadro en el que se muestra el estudio económico para el segundo escenario de la propuesta de solución para las necesidades de conexión remota de TESYS.

2o. ESCENARIO		INSTALACION	RENTA		
Rubro	Descripción	Cargo Único	12 Meses	24 Meses	36 Meses
RAS	Cisco AS 5300, 240 conexiones asíncronas, 120 sesiones de voz, 8MB Flash, 16MB Ram, 2 puertos 10BaseT, 4 puertos síncronos serial E1	$21,590	$17,470	$9,070	$6,990
Telefonía Local	2 Enlaces E1 (2048Kbps) con 30 troncales cada uno	$271,800	$27,000	$27,000	$27,000
Larga Distancia	Número 01 800 de Larga Distancia para los usuarios remotos (tomando en consideración una conexión promedio de 4 horas diarias)	-	$648,000	$648,000	$648,000
Acceso a Internet en TESYS	Enlace dedicado a Internet a DS0 a 1024Kbps en las oficinas de TESYS para 200 usuarios	$58,086	$34,196	$32,541	$27,576
Ruteador	Cisco 2621 XM Interfaces LAN: 2, 10/100 Mbps. Interfaces de voz: 12, digitales G.703 (Conexion a PBX en E1 solo 12 canales) Interfaces WAN: 2, G.703	$13,100	$10,610	$5,510	$4,250
Firewall	PIX 515E, 6 puertos ethernet, peocesador 433Mhz, 64MB RAM, 16 MB Flash	$3,710	$3,000	$1,560	$1,210
(3) Switch	Smart Switch 6000, 5 slots que soporta hasta 120 puertos Ethernet o 40 puertos FastEthernet	$57,584	-	-	-
(3) Servidores	ProLiant DL360 G2 Intel® Pentium® III Processor 1.40GHz/133 Rack Model (256MB) - Power Pick	$62,940	-	-	-

Como resultado de este análisis económico podemos asegurar que el primer escenario es de mayor factibilidad para TESYS, ya que aunque técnicamente los dos escenarios ofrecen la conectividad de manera similar, a diferencia de la solución con la pasarela para red privada que sólo involucra un gasto fijo mensual, en el segundo escenario los gastos por concepto de telefonía local y de larga distancia tienen un impacto económico importante y de manera variable.

7.3 JUSTIFICACIÓN DEL RUTEADOR A UTILIZAR

El ruteador es una parte esencial al momento de implementar la solución tecnológica de TESYS, ya que este determinará en gran medida la velocidad de transferencia de información a través de la red y las conexiones remotas de sus empleados. Por lo que, tomando el análisis del capítulo anterior se desprende la siguiente tabla que resume las características técnicas más importantes de los dos ruteadores que más se adaptan a los requerimientos técnicos de la red propuesta a TESYS.

Nombre del Ruteador	Características				
2621XM- AD6	encriptación estándar 3DES mediante IPSec	Interacción con VPN's	Memoria Flash DRAM de 32 MB con posibilidad de incrementarla hasta 96 MB	conectividad con ADSL o SHDSL	
SuperPipe 155	Alto desempeño con procesadores RISC de alto procesamiento y aplicaciones de misión crítica	Certificado por el estándar ICA como Lucent Secure VPN Solutions Firewall que es un estándar – protegiendo a las redes de Internet	Encripcion estándar a 56 bits con IPSec (con posibilidad de incrementarla a 128 bits)	Transmisión de 10/100 autosensible con Ethernet con fácil migración a redes Fast Ethernet	Asignación de ancho de banda dinámica (Dynamic Bandwidth Allocation - DBA) via MP+

Como se mencionó anteriormente aunque es de suma importancia tomar en cuenta los rubros de configuración, mantenimiento, disponibilidad en el país, soporte técnico y opciones de escalabilidad del producto; de los cuales tuvimos una respuesta favorable por parte de los fabricantes (Cisco, Nortel, Lucent, etc.) e ISP´s (Avantel, Telmex y AT&T), el precio en este caso fue un elemento decisivo para la selección del ruteador a utilizar, y por lo mismo el ruteador más conveniente fue el 2621XM de Cisco, y el cual además de poseer todas las características técnicas y de soporte necesarias para nuestra propuesta de solución, es más económico que las demás opciones consideradas.

7.4 JUSTIFICACIÓN DEL MURO DE FUEGO A UTILIZAR

El Muro de Fuego es la parte medular de la seguridad en el diseño de redes de cómputo para lo cual se deben tomar en cuenta los siguientes puntos:

1.- Que Muro de Fuego están usando actualmente otras empresas con necesidades similares a la nuestra.

2.- Que tan manejable es el producto. (Que tan fácil o difícil es administrarlo).

3.- Que tan sólida y creíble es la empresa que vende este producto. (Que tan fácil es conseguir soporte por parte de esta compañía).

4.- El precio.

A continuación un análisis competitivo de los puntos anteriores para las principales marcas de firewall en el mercado mexicano.

Series de Cisco PIX.

1.- El mejor desempeño de la industria si se utiliza solo como firewall.

2.- Configuración simple lo cual da como resultado el gasto de administración más bajo del mercado.

3.- Alto rango de soporte multimedia.

4.- Actualmente posee el 40% de la división del mercado local.

5.- Líder en grandes redes corporativas y actualmente el más estable en el mercado mexicano.

6.- Ofrece el mejor servicio de soporte de México. (Soporte 7X24 los 365 días del año).

7.- Muy buena relación costo-beneficio.

Sistema de Muro de Fuego conmutado Alteon ASF. (Nortel)

1.- Él más veloz al ser una solución multicomponente. (Desempeño Multi Gigabit)

2.- Configuración de firewall multicomponente que basa su funcionamiento en el software líder en la industria, llamado CheckPoint Firewall-1 Next Generation.

3.- División del mercado local actualmente de aproximadamente el 30%.

4.- La más alta disponibilidad de la red del mercado.

5.- Funcionamiento Plug and Play.

6.- Mejor escalabilidad del mercado.

7.- No es el más económico del mercado.

Sistema de Muro de Fuego Nokia IP

1. - Provee el manejo de paquetes pequeños más veloz del mercado. (Excede los 180Mbps).

2.- Posibilidad de manejo remoto por medio del "viajero" para redes de NOKIA.

3.- División del mercado de aproximadamente el 15%.

4.- Incrementa grandemente la disponibilidad de la red debido al uso del protocolo de redundancia de ruteador virtual (Virtual Router Redundancy Protocol; VRRP) y la sincronización de Firewall-1

5.- Dispositivo Firewall/ VPN fuertemente integrado con el software de seguridad Checkpoint VPN-1/Firewall-1 y con su sistema operativo de redes propio de Nokia (Nokia IPSO).

6.- La mejor detección de intrusos del mercado debido al uso de la aplicación RealSecure para Nokia. (No se requieren instalaciones futuras).
7.- Es el más caro del mercado.

Tomando en cuenta el análisis anterior se llegó a la conclusión de que la serie de Muro de Fuego PIX de CISCO es la mejor opción para la protección de la red VPN que propondremos a TESYS. A continuación una tabla en la que se muestran las características de funcionamiento de cada una de las versiones de los muros de fuego de Cisco PIX.

PIX Muro de Fuego	501	501-50	506	515E	525	535
Software	v 5.1(1)	v 5.1(1)	v 5.1(1)	v 5.3(1)	v 5.3(1)	v 5.3(1)
Mercado	Oficina-casa/ ofic pequeña	Oficina-casa/ Oficina pequeña	Oficina-casa/ oficina pequeña	Negocios medianos	Empresas	Empresas grandes / ISP
Licencias	10	50	N/A	N/A	N/A	N/A
Conexiones VPN	5	5	25	N/A	N/A	N/A
Procesador	133 MHz	133 MHz	200 MHz	433 MHz	600 MHz	1000 MHz
RAM	16	16	32	64	256	1000
Flash (MB)	8	8	5	16	16	16
Integración de puertos 10/100	1-4 (Interruptor de puertos)	1-4 (Interruptor de puertos)	2	2	2	0
Slots PCI	0	0	0	2	3	9
Ethernets Máximo	1-4 (Interruptor de puertos)	1-4 (Interruptor de puertos)	2	6	8	8
Anti-Interrupciones	No	No	No	Si	Si	Si
Throughput bi-directional	10	10	20	188	320	1700
Paquetes por segundo	10000	10000	20000	26000	130000	210000
Throughput de 3DES	3	3	10	10	70	95
Paquetes por segundo de 3DES	1000	1000	9000	7000	41000	43000

De acuerdo con las necesidades de conexiones remotas de TESYS se decidió que el Muro de Fuego Cisco PIX 515E es el modelo que utilizaremos en el diseño de esta red, ya que el mismo cubre las necesidades de seguridad que necesitaremos en la red propuesta a TESYS.

Faltan páginas

N° 197-198

7.6 JUSTIFICACIÓN DEL CONMUTADOR A UTILIZAR

Por otra parte los conmutadores van a ser una parte importante al momento de conectar tanto la red interna hacia Internet como para la formación de la VPN de TESYS y que deberán cumplir con funciones de transferencia de archivos y seguridad de la información. Por consiguiente se contemplo un rango mayor de equipos mismos que se resumen en la siguiente tabla.

Nombre del Switch	Características			
SmartSwitch 9000	Conmutador de 5 slots que soporta hasta 120 puertos Ethernet o 40 puertos FastEthernet	Ancho de banda de hasta 3,2 Gbps	Potencia de conmutación de 2.000.000 pps	Redundancia de tomas
SmartSwitch 2200	Conmutador autónomo de gran rendimiento dotado de 24 puertos Ethernet	Un enlace de gran flujo FDDI, ATM o WAN	Le permite ser utilizado como conmutador de estaciones de trabajo	
Enterasys Vertical Horizon VH-2402S2	24 puertos RJ45 a 10/100 Mbps y dos slots para expansiones	En la industria permiten que VH-2402S2 integre a en pequeñas y medianas redes	El VH-2402S2 provee de conexiones a 10/100Base-TX	Dos slots modulares opcionales 100Base-FX y 1000Base-X escalables
Enterasys *Matrix E1*	Switch de nivel 3 con funcionalidad completa de ruteo	Soportan conectividad 10/100 y Gigabit Ethernet		
3Com® Switch 4005	Ideal para la agregación Fast Ethernet de PCs, o en el núcleo de una pequeña red	Posibilidad de añadir al chasis o a los Starter Kits módulos adicionales Fast Ethernet ó Gigabit	Ofrece la redundancia hardware necesaria, con capacidad para soportar switch fabrics y fuentes de alimentación redundantes	
3Com® Switch 4060	Equipada con seis puertos 1000BASE-SX y seis puertos GBIC para conectividad con la red troncal	12 puertos integrados 10/100/1000 para conexiones con los servidores	Fuentes de poder modulares, con cargas compartidas con tecnología hot-swap	
3Com® Switch 4006 Copper Fast Ethernet	Kit proporciona 40 puertos de conectividad Fast Ethernet a cable de cobre, con capacidad para soportar otros siete módulos I/O	El chasis de 14 ranuras puede escalarse hasta 96 puertos Fast Ethernet ó 24 puertos Gigabit Ethernet	Soporta RIP v1, RIP v2, OSPF, y DVMRP	Diseño redundante que proporciona un 100% de disponibilidad

Al igual que en el caso de los demás equipos se debe de tomar en consideración los siguientes puntos: la facilidad de configuración, mantenimiento, disponibilidad en el país, soporte técnico de la empresa que lo vende o distribuye, precio y opciones de actualización o escalabilidad del producto.

Analizando a fondo las características técnicas, el precio y los puntos mencionados anteriormente llegamos a seleccionar el producto SmartSwitch 6000 que cumple con nuestras necesidades de número de puertos (120 como máximo), velocidad de transmisión y lo más importante tiene un precio muy accesible de acuerdo a sus características.

7.7 SERVIDORES A UTILIZAR

Cada computadora dentro de TESYS conectada a Internet por medio de TCP/IP debe conocer la siguiente información:

a) Su dirección IP
b) Su máscara de red
c) La dirección IP del ruteador
d) La dirección IP de un servidor de nombres o DNS

Por lo tanto TESYS manejará tres tipos de servidores en red para sus diferentes aplicaciones y debido a sus características técnicas y compatibilidad con otros equipos de la red se ha considerado utilizar el Proliant DL 320 de Hewlett Packard. A continuación se mencionan algunas aplicaciones que realizarán estos servidores dentro de la empresa.

7.7.1 Servidor Dinámico de Protocolo de Configuración (DHCP)

El protocolo utilizado en un servidor DHCP, es el protocolo de configuración dinámica de estación (DHCP;Dynamic Host Configuration Protocol) que proporciona una configuración dinámica, en la cual el administrador no necesita especificar una dirección IP en particular.

Algunas características del servidor DHCP son:

a) El servidor DHCP es una extensión de BOOTP

b) El servidor DHCP mejora al servidor BOOTP y es compatible hacia atrás con BOOTP

c) El servidor DHCP es necesario cuando una estación se mueve de una red a otra se conecta o desconecta desde una red (como un abonado a un proveedor de servicios)

d) El servidor DHCP proporciona direcciones IP temporales durante un periodo de tiempo limitado.

Esto significa que si una estación que ejecuta el usuario de un servidor BOOTP puede solicitar una configuración estática de un servidor DHCP. El servidor DHCP cuida la asignación de la dirección IP hacia la estación.

7.7.2 Servidor de Nombres (DNS)

Para identificar una entidad, los protocolos TCP/IP utilizan direcciones IP, que identifican de forma única la conexión de una PC a Internet. Sin embargo, la gente prefiere utilizar nombres en lugar de direcciones.
Por lo tanto, es necesario un sistema con un servidor que puede proyectar un nombre en una dirección y de forma inversa una dirección en un nombre.

El protocolo que utiliza un servidor DNS es el sistema de nombres de dominio (DNS; Domain Name System) es un protocolo que se puede utilizar en plataformas diferentes. En internet, el espacio de nombres de dominio (árbol) se divide en tres secciones diferentes:

a) Dominios genéricos (com., edu., gov., int., mil., etc.)
b) Dominios de país (us.,fr.,ae.,ca.,mx., etc.)
c) Dominios inversos

En una mediana o extensa red un número de servidores DNS son instalados: un servidor primario y algunos secundarios. Los nombres y direcciones son almacenados en el servidor primario y los servidores secundarios obtienen la información del servidor primario. Los servidores secundarios preguntan al servidor primario periódicamente para determinar sí ha ocurrido algún cambio en la base de datos. Sí algún cambio se ha efectuado, el servidor secundario solicita una zona de transferencia (AXFR) que copia completamente la base de datos desde el servidor primario al servidor secundario. Una estación puede necesitar información del servidor primario o de algún secundario y recibir exactamente la misma información.

7.7.3 Servidor de Correo Electrónico (SMTP)

El servidor de red más popular es el de correo electrónico (e-mail). El protocolo que soporta el correo electrónico en Internet es el protocolo sencillo de transferencia de correo electrónico (SMTP; Simple Mail Transfer Protocol). Por medio de este servidor se envían mensajes a otros usuarios de computadoras basadas en direcciones de correo electrónico. El servidor SMTP ofrece el intercambio de correo electrónico entre usuarios de la misma empresa o de diferentes computadoras.

El servidor SMTP permite:

a) El envío de un único mensaje a uno o más receptores
b) El envío de mensajes que incluyen texto, voz, vídeo, o gráficos
c) El envío de mensajes a usuarios de redes situadas fuera de Internet

7.7.4 Servidor de Aplicaciones

El servidor de aplicaciones permitirá tanto a los usuarios internos como los remotos consultar las aplicaciones desarrolladas por TESYS y que le permitirán operar día a día.

Como se mencionó anteriormente, las funciones que realizarán estos servidores dentro de la empresa TESYS serán ejecutadas por los equipos Proliant DL320 de HP.

7.8 DISEÑO E IMPLEMENTACIÓN DE LA RED

Una vez que ya se realizó la selección de los equipos a utilizar en el diseño de la VPN propuesta a TESYS para la solución de sus necesidades de conexión remota, estamos listos para el diseño e implementación de la misma, lo cual se muestra en la fig. 7.1 y 7.2.

La red de área local (LAN) de la compañía fig. 7.1, es la red de comunicaciones que servirá a los usuarios de computadoras personales dentro y fuera de TESYS, que en un área geográficamente confinada se compone de servidores, estaciones de trabajo, sistemas operativos de redes y enlaces de comunicaciones etc.

Las **Terminales de Voz y Datos**, son máquinas de usuario que funcionan como computadoras personales autónomas. Las Terminales de voz y datos sin disquete o las terminales de voz y datos con sólo disco flexible recuperan todo el software y todos los datos del servidor, como con cualquier computadora personal, una impresora se puede unir a cualquiera de las terminales de voz y datos o a algún servidor y esta pueda ser compartida por todos los usuarios de la red.

La red LAN, también permitirá que cada terminal de voz y datos funcione como un servidor dentro de la red y que todos los usuarios internos y remotos accedan a los datos en todas las terminales dentro de TESYS.

Los 3 **Servidores** (ProLiant DL360, HP), son máquinas de alta velocidad que contendrán programas y datos que todos los usuarios internos y remotos de la red, que se puedan compartir. Cada servidor dedicado siempre podrá manejar varias transacciones por segundo. Debido a esto en nuestra red se utilizan varios servidores por manejar un alto volumen de información. El primer servidor contendrá la base de datos de TESYS y a su vez trabajará como servidor de nombres (DNS) que se encargará de la conversión de los nombres en direcciones y viceversa esto con el objeto de convertir los nombres en direcciones IP y que sean compatibles con el protocolo de comunicaciones TCP/IP. Nuestro siguiente servidor es el de Aplicaciones, que permitirá a los usuarios internos y remotos consultar las aplicaciones de TESYS diseñadas para las operaciones diarias. Por último el servidor de correo electrónico y de web, el cual contendrá la base de datos de correo y de almacenaje de la página web de la compañía.

Para la conexión entre redes iguales se utilizaron 3 **Conmutadores** (Smartswitch 6000, Enterasys) que conectan de un piso a otro, un conmutador por cada piso dentro de TESYS, el cual manejará de 65 a 70 estaciones de trabajo, estos a su vez están interconectados realizando la función de respaldo entre ellos, en caso de que alguno llegase a fallar, por lo cual TESYS no correrá el riesgo de que la red falle. Estos conmutadores permiten la interconexión de la red de computadoras personales por ejemplo; se interconectan con una red de minicomputadoras o con una red de computadoras de gran tamaño. Estos conmutadores soportan hasta 120 puertos ethernet con un ancho de banda de 3.2 Gbps. y una potencia de conmutación de 2,000,000 de paquetes por segundo. Además nuestros 3 conmutadores, tendrán la funcionalidad de concentradores en nuestro diseño de la red, debido a que dedicarán todo el ancho de banda de forma exclusiva a cualquier comunicación entre sus puertos, dado que únicamente envía paquetes de datos hacia donde irán dirigidos. A su vez darán servicio a nuestras terminales de voz y datos personales como a nuestros otros segmentos de la red. De manera que de esta forma conseguiremos que el tráfico interno en los distintos segmentos de la red local conectados a cualquiera de nuestros conmutadores no afecten al resto de la red local de TESYS. Todo esto dará como resultado la eficiencia del uso del ancho de banda y del diseño de nuestra red LAN.

El software de control en la red LAN, es el sistema operativo de la red, como Netware, Lantastic y Appletalk, que reside en los servidores. En cada terminal de voz y datos reside un componente del software y permite que una aplicación lea y escriba datos de un servidor como si estuviera en una máquina local.

La transferencia física de los datos se lleva acabo por el método de acceso Ethernet, que aparece en forma de adaptadores de red y se conectan a cada computadora. El enlace real o la vía de acceso de las comunicaciones es por medio del cable (par trenzado, coaxial, fibra óptica), que se conecta a cada adaptador de red que a su vez conecta todas las terminales de voz y datos y servidores juntos.

El **Ruteador** (Router 2621XM-ADS, Cisco) es la parte esencial en nuestro diseño de la red dentro de TESYS, ya que este determina en gran medida la velocidad de transferencia de datos y las conexiones remotas de los empleados. Nuestro ruteador de 32Mb de memoria RAM con soporte de encriptación estándar 3 DES mediante el protocolo IPSec, es un dispositivo inteligente el cual se encargará de enviar paquetes de datos de un protocolo común, desde nuestra red LAN a otra o desde nuestra red de TESYS a algún usuario remoto, a la vez convertirá paquetes de información de la red LAN de TESYS en paquetes capaces de ser enviados mediante redes de área extensa (WAN).

Durante la transferencia de datos el ruteador examina el paquete buscando la dirección de destino, consultando en su propia lista de direcciones, la cual se mantiene actualizada debido al intercambio de direcciones con los demás ruteadores que establecen rutas de enlace a través de las redes que los interconectan.

El **Muro de fuego** (Firewall PIX515E, Cisco) acepta un número ilimitado de conexiones remotas, posee anti-interrupciones y maneja hasta 7000 paquetes por segundo encriptados en 3 DES. En nuestro diseño de la red es de suma importancia, porque es la parte medular de la seguridad que se encargará de suministrar el nivel de protección necesario dentro de la red LAN de TESYS. Este a su vez ayudará en la prevención del acceso no-autorizado a los recursos propios de la compañía y por supuesto a nuestra red privada virtual. Por lo cual nuestro muro de fuego impondrá una política de seguridad entre la red privada de TESYS y el Internet. Este muro de fuego determinará quien podrá accesar para utilizar los recursos de la compañía. Debido a esto el muro de fuego tendrá mayor efectividad porque todo el tráfico de información a través del Internet deberá pasar a través del mismo donde podrá inspeccionar toda la información y hacerla llegar de forma segura a sus respectivos servidores o terminales de voz y datos.

La **Pasarela** (VPN Gateway Contivity 1600, Nortel) dentro de nuestra red privada soporta hasta 200 túneles simultáneos con 128Mb en RAM, facilitará el acceso entre sistemas o entornos el cual soporta diferentes protocolos de comunicación (multiprotocolo). También llevará acabo la conversión de protocolos para que se pueda dar la interconexión de redes con protocolos diferentes de alto nivel. A su vez es considerado un dispositivo universal, independientemente del número de redes y de los diferentes tipos, por cumplir con las especificaciones de la nueva tecnología y estándar en la creación de redes virtuales llamada IPSec. También se encarga de la autentificación y autorización de los usuarios y al mismo tiempo será el punto de terminación de los túneles que permitirán el intercambio de información entre los usuarios remotos e internos de la red local de TESYS y deberá asegurarse que los datos de la red local al transportarse sean compatibles con los de otra red.

Al conjunto de estos dispositivos, se consideran herramientas de una red privada (VPN), además de ser una "área segura" dentro de la red LAN de TESYS.

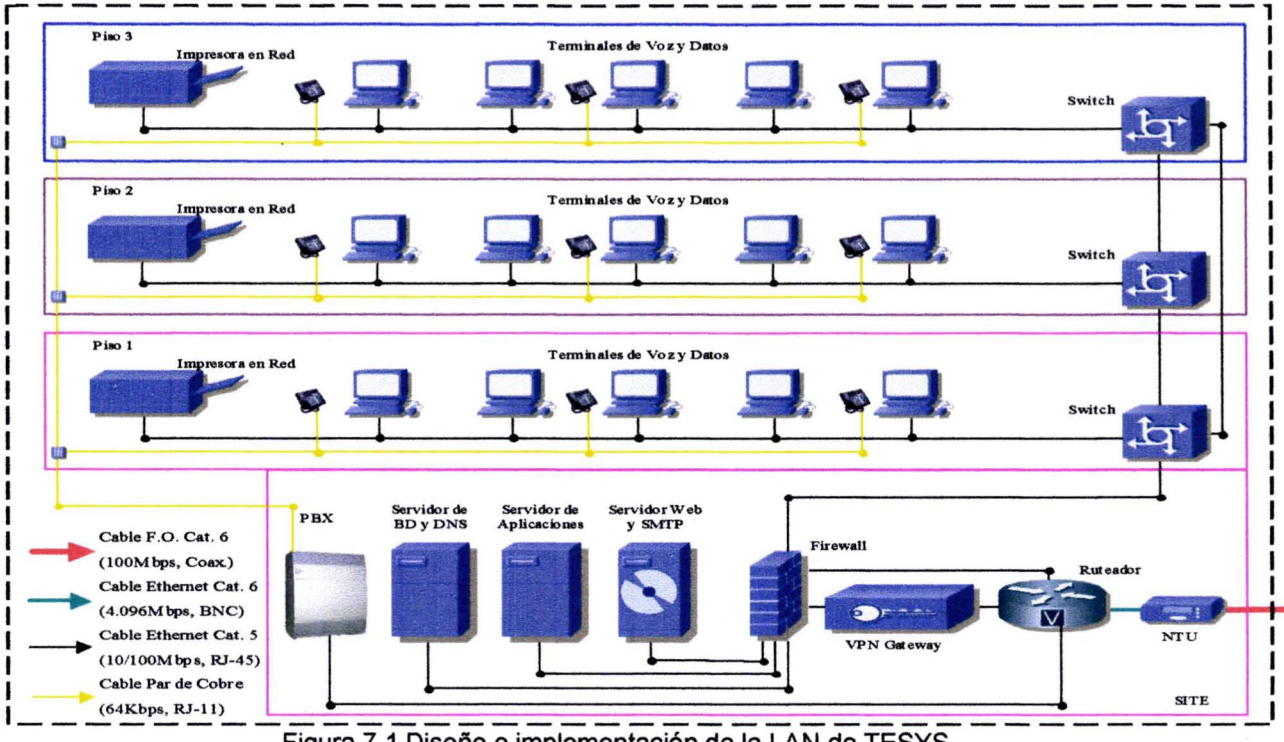


Figura 7.1 Diseño e implementación de la LAN de TESYS.

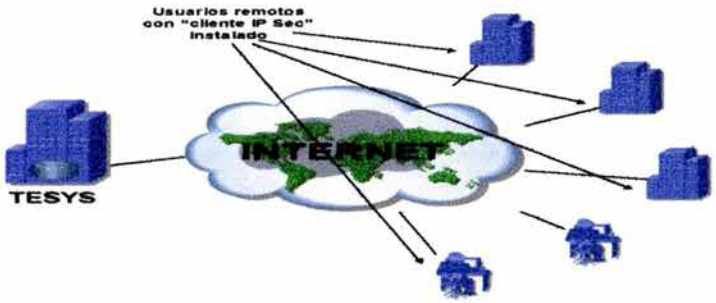


Figura 7.2 Diseño de la VPN de TESYS.

7.9 CONFIGURACIÓN DE LA PASARELA PARA LA RED PRIVADA (VPN GATEWAY)

Como se muestra en la figura 7.2, la VPN esta formada por usuarios remotos que se conectarán desde sus casas o desde las oficinas de los clientes, es decir el objetivo es que se puedan conectar desde cualquier lugar en donde exista una línea telefónica para poder tener acceso a Internet.

La conexión remota se realizará cuando el empleado se comunique vía telefónica a la red LAN de TESYS, esta comunicación se llevará acabo gracias a un equipo denominado MODEM que realizará la operación de comunicarlo al servidor del proveedor de Internet (AVANTEL), el empleado remoto podrá utilizar un módem interno que traerá ya de fábrica los equipos Laptop. Una vez dada la conexión, el empleado correrá el software de conexión remota (Contivity Multy OS Client, Nortel), este software realizará otra llamada hacia una dirección IP la cual por cierto será la dirección IP de la pasarela de la red de TESYS, una vez que la pasarela conteste la llamada, quedará establecido el túnel que permitirá la comunicación entre el usuario remoto y la red local de TESYS.

De manera externa se requerirá una línea digital de alta velocidad, que divida voz, datos y en su momento de así requerirlo vídeo, un enlace E1 (2048 Kbps). La tecnología de la Red Privada Virtual suministra un medio para usar el canal público de Internet como un canal apropiado para la comunicación de los datos privados de TESYS.

En concreto, los empleados remotos llegaran a Internet a través del enlace dedicado E1,el ruteador reconocerá la dirección a la que se dirigen y los guiará hacia la Pasarela, la Pasarela buscará a estos usuarios dentro de sus listas y passwords válidos y en el caso de que así lo aplique lo autentificará, terminará entonces la creación de los túneles y los conectará directamente hacia el Muro de Fuego, una vez en el Muro de Fuego serán parte de la Red Virtual de TESYS y de los

accesos definidos a cada uno de ellos. Tendrán acceso a los recursos de la red local de TESYS, permitiendo la creación de la VPN.
La red privada ofrece mecanismos eficientes para el manejo de los problemas potenciales de banda ancha, para poder manejar de forma controlada estos problemas, cada puerto de los conmutadores al igual que los usuarios se integrarán en grupos de trabajo o redes privadas virtuales esto con el fin de aislarlos cuando se genere algún problema en cualquiera de ellos.

Para poder soportar las funcionalidades mostradas con anterioridad, la plataforma básicamente deberá ser una integración entre la plataforma de Dial Up de cualquier ISP (Telmex, Avantel o AT&T) y el equipo que terminará los túneles remotos en TESYS. El esquema general de la manera en que esta información viajará será usando MPLS desde el cliente emisor hasta el equipo terminador de túneles en TESYS.
El escenario bajo el cual está colocado la pasarela y el muro de fuego permitirá terminar los túneles en la red DMZ y protegida de TESYS, de tal forma que, se mantiene la información en clear text en un área segura y además se permite anexarle reglas de acceso del muro de fuego para permitir tráfico hacia la red interna, por ello se instala la pasarela en una red anexa del muro de fuego, independiente de la red interna.

La solución de la pasarela incluye los protocolos de tunelaje más populares, IP Security (IPSec), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Fowarding Tunneling Protocol (L2TP) y Layer 2 Fowarding (L2F).

IPSec a su vez utiliza certificados digitales, llaves basadas en passwords, y tokens para autenticación.

PPTP, L2TP, y L2F usan Challenge Handshake Authentication Protocol (CHAP) o Password Authentication Protocol (PAP) en sus autenticaciones. El módulo para la implementación de PPTP soporta autenticación MS-CHAP con encriptación de llaves de 56 a 128 bits. Para el control de accesos y autenticación , el switch soporta un servidor interno o externo de Lightweight Directory Access Protocol (LDAP) y servidores externos de Remote Authentication Dial-In User Service (RADIUS). Para restringir el acceso la pasarela usa un filtrado de paquetes basado en el protocolo ID, dirección IP fuente y destino, puertos fuente y destino, establecimiento de conexión TCP y dirección. Adicionalmente pasarela provee un conjunto de filtros predeterminados. La admisión de llamadas y las prioridades de reenvío de paquetes, así como el soporte del protocolo Resource ReSerVation Protocol (RSVP) proveen calidad en los métodos de servicio.
La interfase de administración vía HTML y Java Web permite que múltiples administradores tengan privilegios diferentes, incluyendo configuración, status y monitoreo.

Para lograr la formación de un túnel, el usuario remoto deberá:

a) Establecer una conexión con el punto de presencia (POP) de la red de datos pública, típicamente a través de un proveedor de servicios de Internet (ISP).

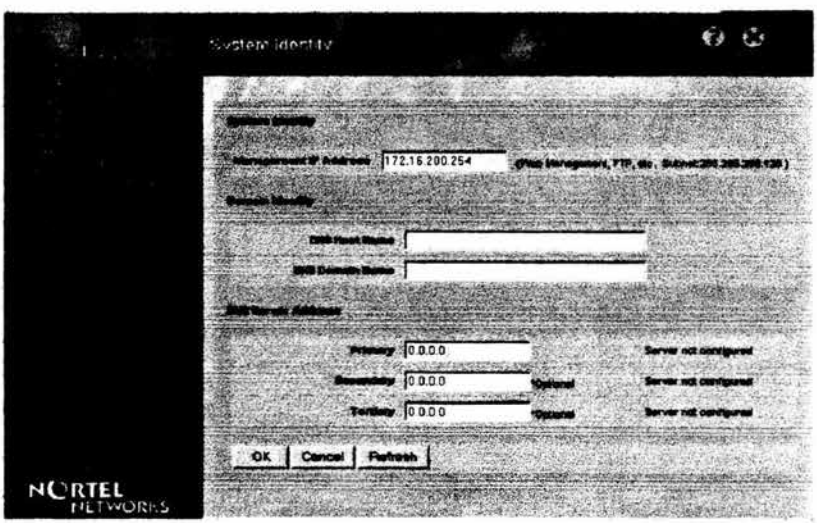
b) Después de que la conexión se ha establecido, el usuario remoto envía una segunda conexión dial-up y especifica una conexión al switch. En lugar de usar un teléfono para establecer la sesión, la segunda conexión usa una dirección de IP (o un nombre si la dirección IP esta dentro de un servidor de servicios de nombres de dominio, DNS.).
c) Esta segunda conexión podrá usar el protocolo de tunelaje punto a punto (PPTP) o el de IP seguro (IPSec). Los túneles establecidos por L2TP o L2F son ligeramente diferentes.

d) El túnel comienza en algún equipo de red (servidor de acceso de red) localizado en el ISP en lugar de la PC del usuario. El usuario simplemente marca al ISP con un número telefónico que provoca un túnel L2TP o L2F para conectarse directamente a TESYS.

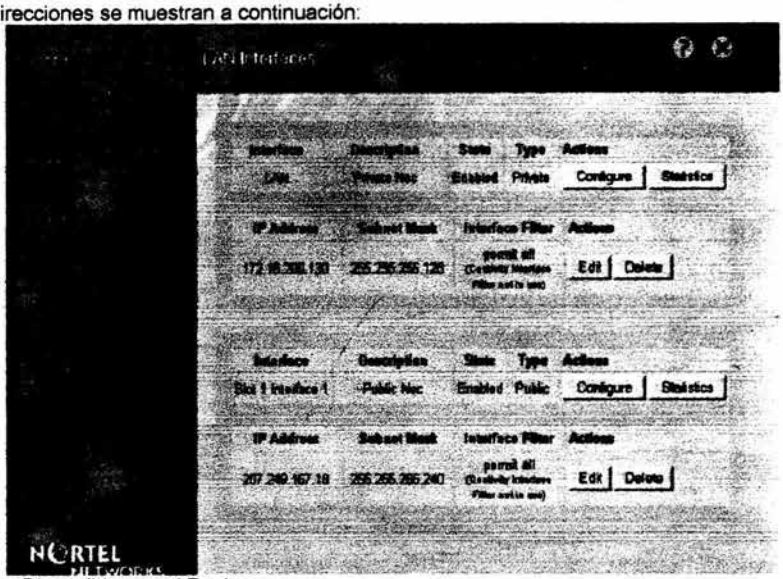
Una vez establecido un túnel y se han autenticado y autorizado los usuarios, se deberá encriptar la información para que viaje de un medio seguro por una red pública.
En la mayoría de los casos, los métodos de encriptación y las tecnologías de tunelaje están ligados. Por ejemplo PPP con PPTP incluye encriptación RC4 (de 56 o 128 bits). IPSec puede soportar múltiples tipos de encriptación con longitudes de llaves variantes, tales como DES y Triple DES, y códigos de token desde Securid y AXENT.

7.9.1 Configuración del Sistema de la Pasarela (VPN Gateway)

La dirección IP de Administración es la siguiente: IP:172.16.200.254 Máscara: 255.255.255.128
Como lo muestra la siguiente pantalla:

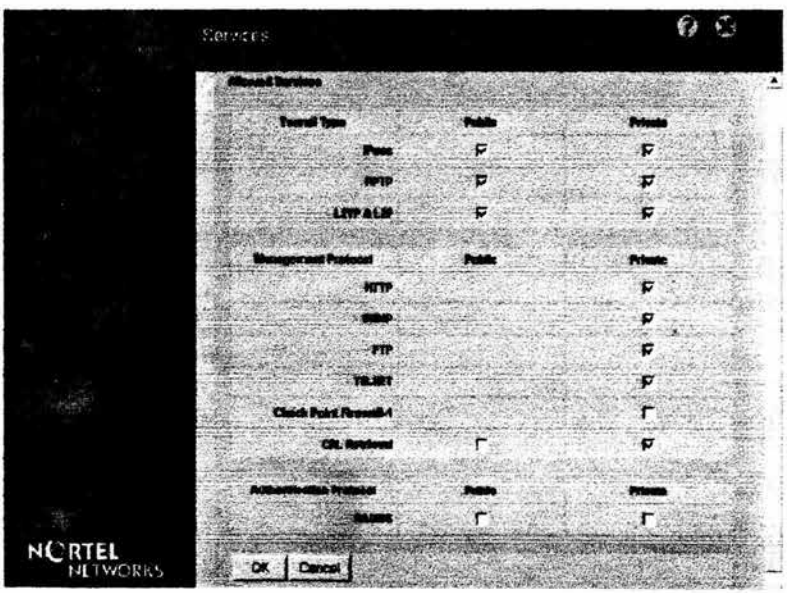


Las direcciones IP públicas y privadas quedaran de la siguiente manera: IP Privada: 172.16.200.130 IP Pública: 207.249.167.18 Mascara: 255.255.255.128 Mascara: 255.255.255.240 Estas direcciones se muestran a continuación:



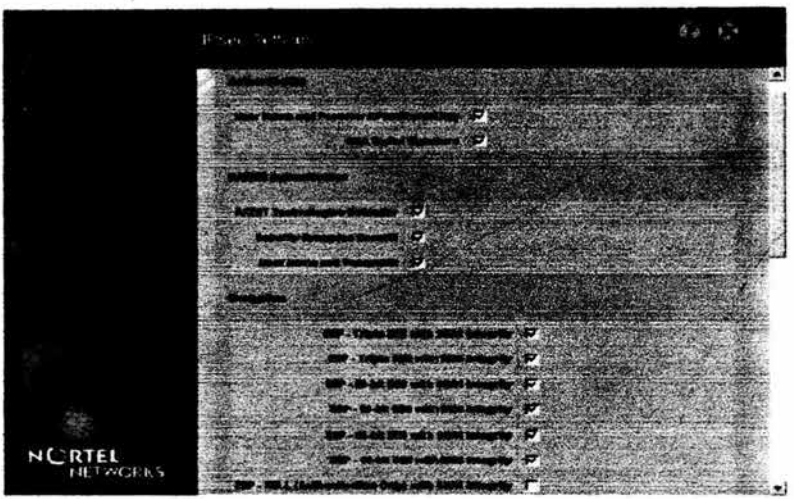
Servicios Disponibles en el Equipo

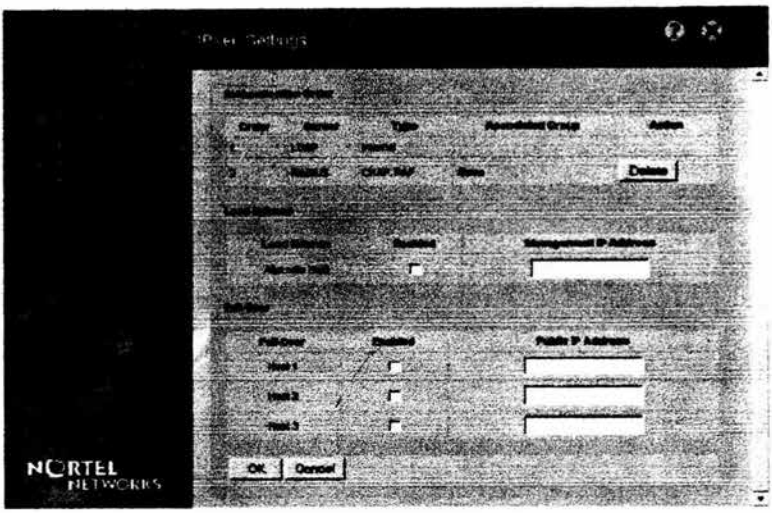
Los servicios disponibles y permitidos por el equipo son tipo de tuneling, Protocolo de manejo, y protocolo de autentificación como se muestra en las siguientes pantallas:



Servicios del Protocolo IPSEC

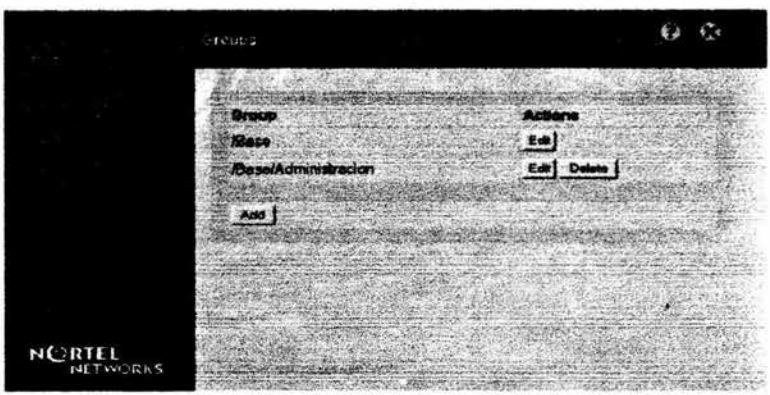
Los parámetros configurados para el protocolo de IPSEC se muestran a continuación:



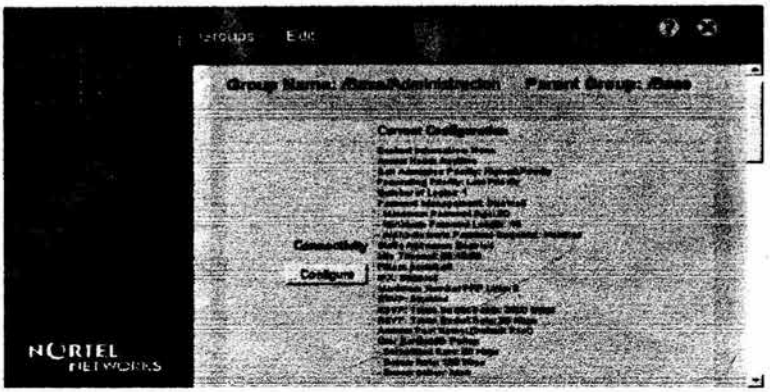


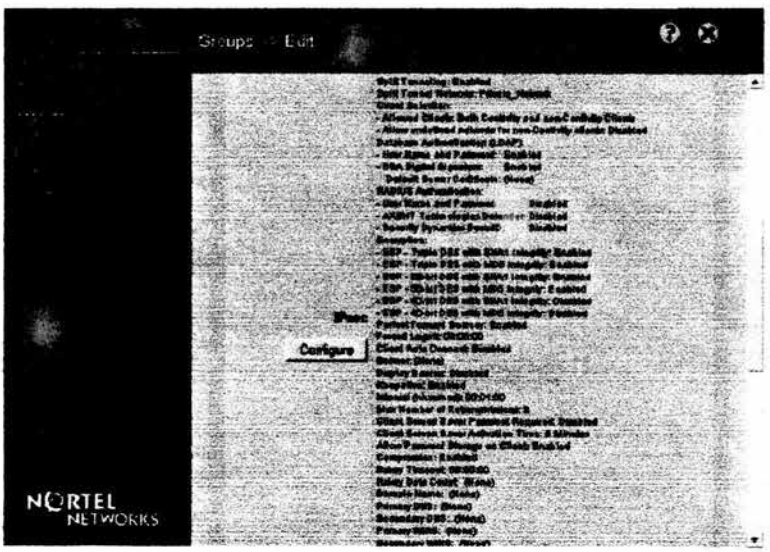
PERFILES

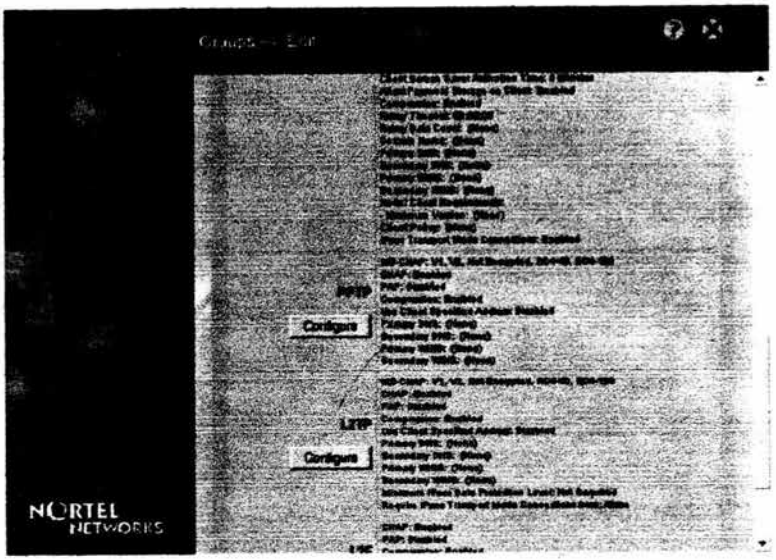
El grupo configurado en el equipo, de nombre / Base/ Administrador, es solo para fines de administración y se muestran a continuación:

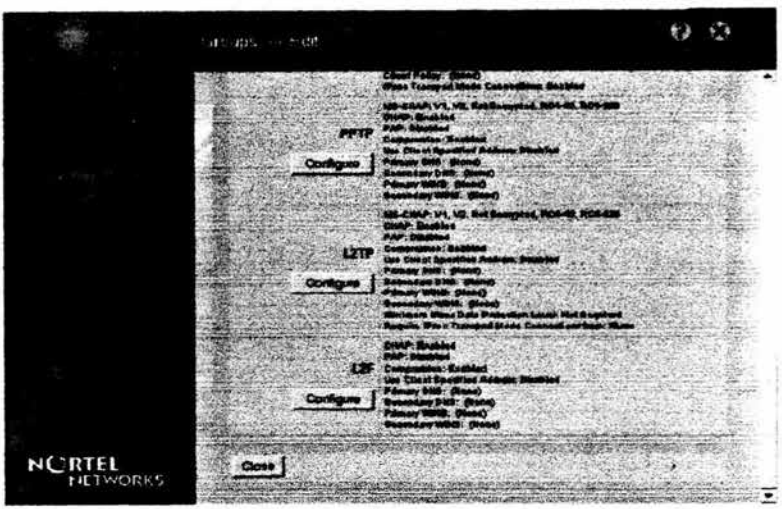


El Grupo Administración tiene los siguientes parámetros configurados:





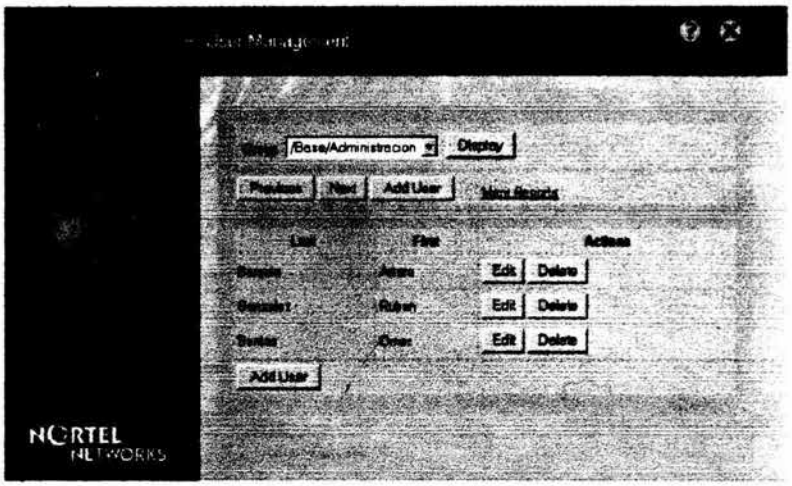




Usuarios

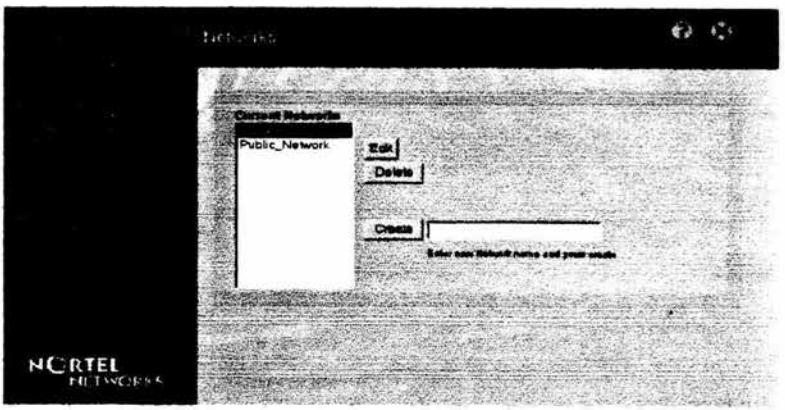
Los Usuarios configurados dentro del grupo /Base /Administración son 3 como se muestra en el siguiente ejemplo:

Nombre de usuario	ID	Password	Derechos
Arturo Barquin	abarquin	abarquin	Administrador
Ruben Gonzalez	rgonzalez	rgonzalez	Administrador
Omar Santos	osantos	osantos	Administrador

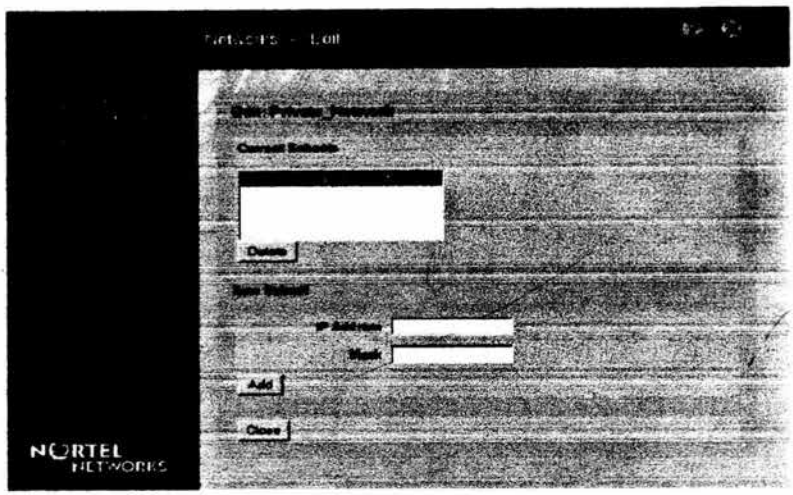


Redes definidas en el equipo

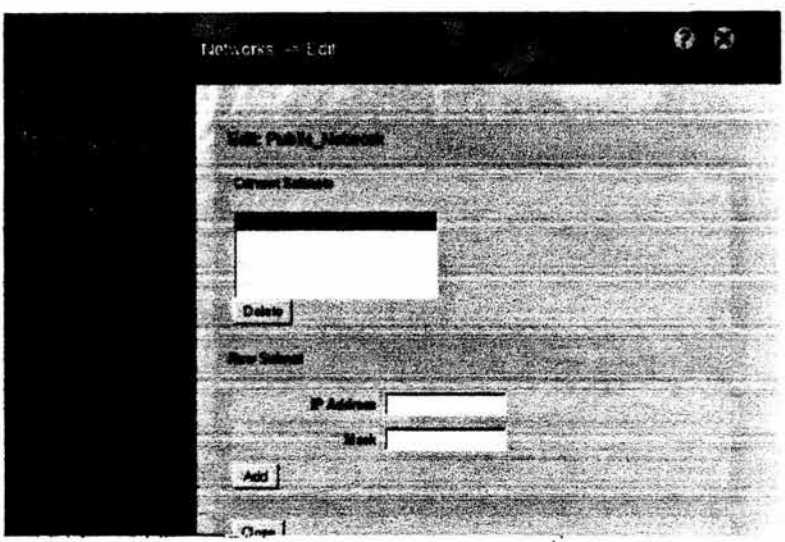
En el sistema se encuentran definidas dos redes; la red privada y la red pública como se muestran en la siguiente pantalla:



La red privada contiene los siguientes datos:



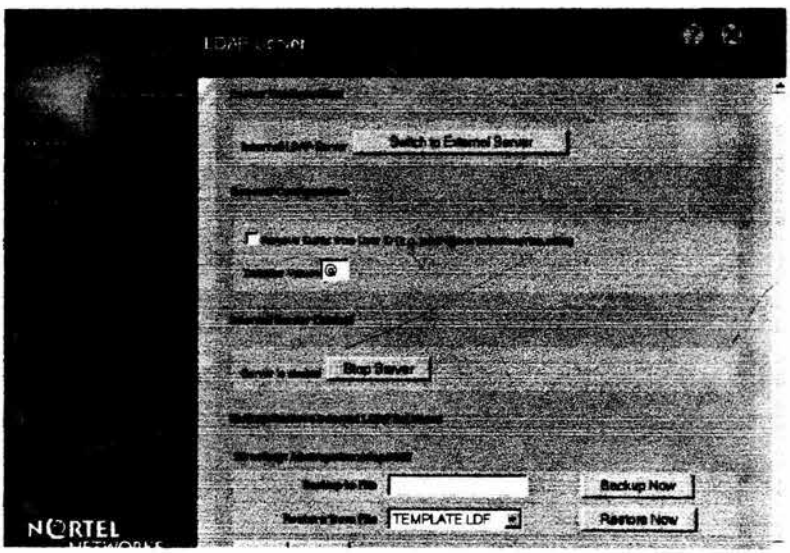
La red pública cuenta con los siguientes datos:



SERVIDORES

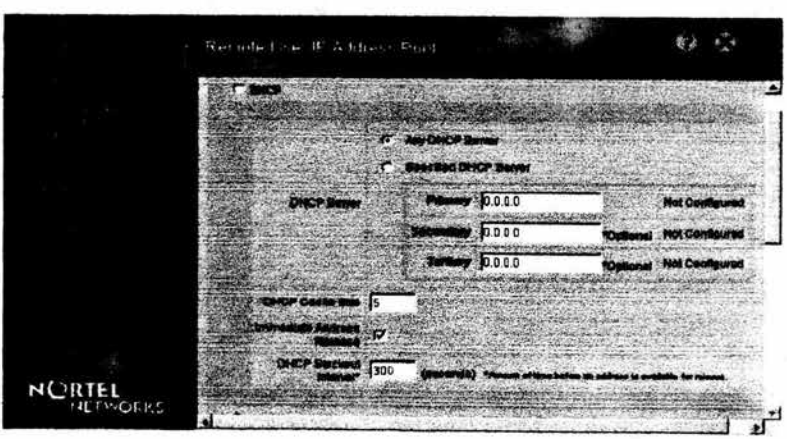
El equipo cuenta con dos tipos de servidores de autenticación internos los cuales son LDAP y RADIUS, para este caso se encuentra configurado el servidor LDAP y se utiliza para validar a los usuarios antes mencionados.

Servidor LDAP
La configuración del servidor LDAP es como se muestra en la siguiente pantalla:

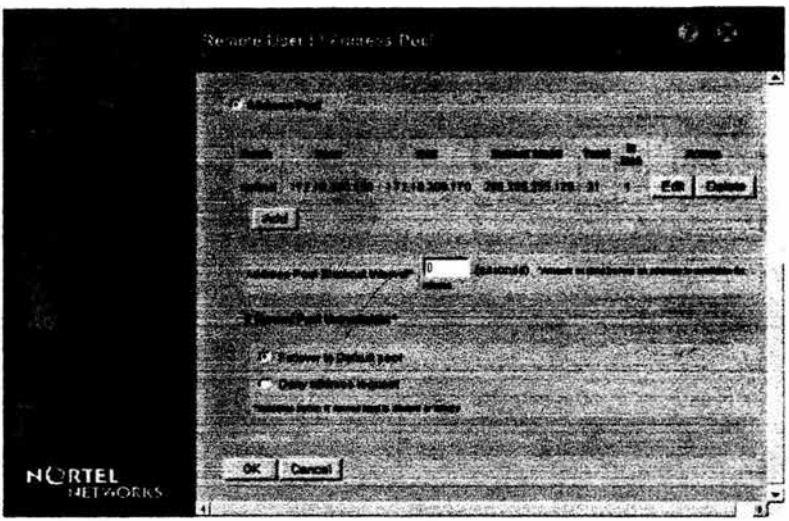


Distribución de Direcciones IP de Usuario
Las Distribución de Direcciones IP de Usuario, sirve para asignar las direcciones IP del segmento privado, a los clientes que se conecten vía cliente IPSEC.

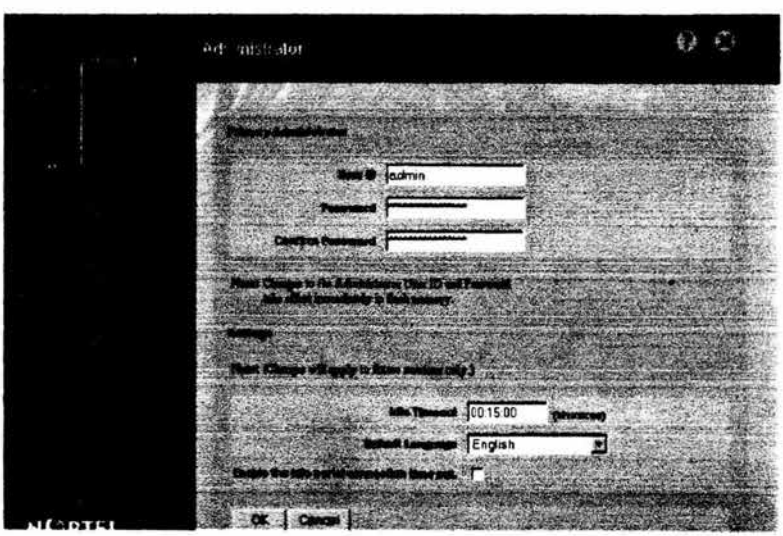
Y se encuentra configurado como se muestra en las siguientes pantallas:



El Rango de direcciones que asigna a los clientes es el siguiente:
172.16.200.150 a 172.16.200.170 con mascara 255.255.255.128



Administrador
Para accesar al equipo se requiere contar con un usuario y password.
El usuario por default es: admin.
El password: setup
Donde se puede modificar el usuario y password es en el siguiente menú y se muestra a continuación:



7.10 POSIBILIDADES DE CRECIMIENTO DE LA RED

A partir de nuestra propuesta y pensando en el crecimiento moderado de empleados en TESYS, los cuales requerirán en mayor capacidad la comunicación remota a las bases de datos de la red local de TESYS es necesario indicar las capacidades actuales de crecimiento a fin de no hacer una nueva inversión en un corto plazo.

Lo anterior será posible mediante la consideración inicial de que se pueda atender 200 usuarios internos y hasta 100 usuarios remotos con un crecimiento anual en aproximadamente un 10% del total de empleados.

7.10.1 Crecimiento del ruteador y enlace dedicado

Aunque la capacidad de crecimiento del ruteador esta en el límite en cuanto a slots y memoria disponibles (ya que por el mismo estará pasando tanto el tráfico de Internet como el de la telefonía local), es importante hacer la anotación que el ancho de banda contratado hacia el ISP nos permitirá dar cabida a los actuales 200 usuarios internos y hasta 100 usuarios remotos, ya que según los análisis proporcionados por Avantel, Telmex, y AT&T (principales proveedores de Internet y Telefonía en México) los dos enlaces E1 de Internet y Telefonía Local (2048Kbps c/u) contratados nos permitirán un crecimiento en número de usuarios de hasta 640 para el de Internet y de hasta 600 para el de Telefonía Local; con lo cual tomando en consideración el crecimiento en un 10% anual de TESYS el tiempo de vida útil estaría dado hasta por 7 años:

Número de Usuarios	Año
300	0
330	1
363	2
400	3
440	4
484	5
533	6
587	7

7.10.2 Crecimiento de la Pasarela (VPN Gateway)

En el caso del equipo Contivity de la serie 1600 de Nortel podemos observar que la capacidad de túneles simultáneos es de hasta 200, por lo que tomando en consideración el plan de crecimiento de TESYS, la vida útil de este equipo vendría dado por la siguiente relación:

Número de Usuarios	Año
100	0
110	1
121	2
134	3
148	4
163	5
180	6
198	7

Aunado a lo anterior y como lo podemos observar en el estudio económico, tanto el VPN Gateway como el ruteador serán adquiridos en esquema de renta con el ISP (Avantel), lo cual permitirá a TESYS que en un supuesto caso de crecimiento fuera de lo proyectado, estos sean cambiados por unos de mayor capacidad, de lo cual sólo tendrá que realizarse una modificación a la alza en la renta mensual.

7.10.3 Crecimiento del Muro de Fuego (Firewall)

De acuerdo con las necesidades de conexiones remotas de TESYS el Firewall Cisco PIX 515E propuesto nos permitirá hasta 500,000 conexiones simultaneas y hasta 6 puertos ethernet necesarios en el caso de TESYS). De esto último es importante hacer la anotación que aunque existirá la demanda por mayor capacidad hacia las aplicaciones, éstas no se incrementarán, con lo cual no habría necesidad de considerar el firewall Cisco PIX 525 de hasta 8 puertos.

7.10.4 Crecimiento de los Conmutadores (Switchs)

El producto SmartSwitch 6000 que cumple con nuestras necesidades actuales de número de puertos (120 como máximo c/u), velocidad de transmisión y lo más importante que tiene un precio muy accesible de acuerdo a sus características, podemos obtener la vida útil de los 3 equipos que se encontrarán instalados en TESYS, dado por la siguiente relación:

Número de Usuarios	Año
200	0
220	1
242	2
267	3
294	4
324	5
357	6

7.10.5 Crecimiento de los Servidores

Con respecto al crecimiento de los servidores este fue tomado bajo las mismas circunstancias de crecimiento que como fue para los demás equipos (10% anual). De inicio los servidores de la serie ML fueron descartados ya que el proveedor no nos recomendó utilizarlos para más de 100 usuarios simultáneos, como consecuencia se definió que dentro de la serie DL se pudiera contar con un alto nivel de procesamiento y desempeño, esto debido básicamente al tipo de aplicaciones que serán montadas y capacidad de accesos que se requerirán a cada uno de estos servidores tomando en consideración que un gran porcentaje de usuarios lo hará de manera remota.

A partir de la anterior información se obtuvo que los servidores DL 360G3 nos permitirán un excelente procesamiento (Pentium 1.4 GHz) a un aceptable desempeño (256MB SDRam).

Aunado a lo anterior la capacidad de sus discos duros (36.4GB) cumplen con los requerimientos actuales y futuros de TESYS (actualmente entre sus aplicaciones y correo requieren 80GB).

Con el diseño de esta red privada descrita anteriormente, se satisfacen todas las necesidades de comunicación remota de la compañía TESYS, a continuación procederemos a la concluir este trabajo de investigación con las conclusiones que obtuvimos durante el desarrollo del mismo.

CONCLUSIONES

Como es bien sabido, las compañías de servicios del mundo actual deben ser cada vez más competitivas al mismo tiempo reducir sus gastos de operación y la conexión remota representa hoy en día una de las opciones mas viables para lograr esta meta tan ambiciosa y agresiva a la vez. La conexión remota disminuye los gastos por renta de espacios y servicios de los mismos, con la promoción del "trabajo desde casa" o teletrabajo, reduce también los constantes traslados de los empleados que trabajan con cliente a las oficinas de TESYS, y reduce también de manera muy significativa las necesidades de viajes al interior de la república o al extranjero.

Ahora bien, según lo planteado en el capítulo 1, se propusieron dos escenarios de solución para satisfacer las necesidades de conexión remota que tiene TESYS. Para hacer la selección correcta de el escenario de solución mas conveniente para TESYS se tomaron en cuenta varios puntos de competencia entre los cuales sobresalen la funcionalidad técnica, la compatibilidad con terceros y el Soporte disponible como se describe a continuación:

a) **Funcionalidad técnica de la plataforma**, es la consideración del cumplimiento de las necesidades técnicas que TESYS requiere para el servicio de Redes Virtuales Privadas (VPN), para ello se consideran aspectos de acceso remoto dial-up, autenticación, tunneling, encripción, filtrado de IP, ruteo, interfaces soportadas, administración de VPN´s, compatibilidad, escalabilidad, disponibilidad. Sobre la base de la tabla de resultados se puede concluir que, en este aspecto ambas plataformas satisfacen las necesidades tecnológicas de TESYS, mostrándose una ligera ventaja en la solución de Servido para acceso remoto (RAS) en cuanto a seguridad ya que en ningún momento cruza por una red pública como lo es Internet; sin embargo, de acuerdo a las necesidades del mercado mexicano, este no es un punto tan relevante para una decisión como si lo es el aspecto económico, lo cual decide a favor de la solución con la Pasarela para red privada (VPN Gateway) por el concepto de telefonía de larga distancia.

b) **Compatibilidad con plataformas de terceros**, cuando se menciona la compatibilidad para terceros en el servicio de VPN se tiene que hablar forzosamente de IPSec como medio de interacción entre elementos, en este punto se puede encontrar que ambas plataformas probadas soportan las plataformas más comunes en el mercado mundial de tecnologías, un ejemplo de lo anterior es que la Pasarela para red privada de Nortel cuenta con la certificación de ICSA, (International Computer Security Association), autoridad central de la industria de seguridad para la investigación, inteligencia y certificación del 95 % de la base instalada de productos de seguridad y IPSec en el mundo. Es conveniente mencionar, que en aspectos de compatibilidad hacia el proveedor del servicio (Avantel) la plataforma de Contivity es completamente trasparente.

c) **Soporte Técnico en México**, de acuerdo a las características intrínsecas de los esquemas de la Pasarela y el Servidor de acceso remoto, se requiere el uso de CPE (Customer Premises Equiment) asociado al servicio, lo cuál es en gran medida responsabilidad de TESYS y dado que no se puede tener total dependencia del proveedor del servicio (esto en el sentido de que existe una alta probabilidad de requerimientos específicos en las instalaciones y activaciones en la red de TESYS y de su equipo terminador de túneles), es muy conveniente verificar que el proveedor de tecnología cuente con el expertise técnico (cuyos profesionales deben de estar ubicados dentro de México) y la cobertura necesaria (al menos en las tres ciudades mas importantes de México) para brindar dicho soporte técnico.

En este aspecto, existe una diferencia fuertemente marcada entre ambas tecnologías, la Pasarela para red privada cuenta con el soporte por parte de los proveedores de tecnología Intersys, Qualita y Datacraft; los cuales cuentan con el expertise técnico necesario para apoyar en estas tareas, sin embargo, la plataforma del RAS, a pesar de que el servidor Cisco también cuenta con el soporte técnico de los 3 anteriores proveedores de tecnología, los principales ISP´s (Telmex, Avantel y AT&T), que también juegan un rol importante en el esquema global de la solución, no soportan a través de su personal técnico este tipo de solución, por lo que se manifiesta una probabilidad de incumplimiento en el servicio de TESYS hacia sus usuarios finales al momento de requerir apoyo de su ISP (Avantel) debido al escaso soporte técnico que podrá brindar.

Ahora bien, la creación de redes virtuales a través de Internet es hoy en día una de las opciones mas viables para lograr la conexión remota y esto se demuestra ampliamente en la siguiente gráfica en la cual se muestra como ha aumentado últimamente el uso del Internet para comunicarse en las pequeñas, mediana y grandes compañías de servicios.

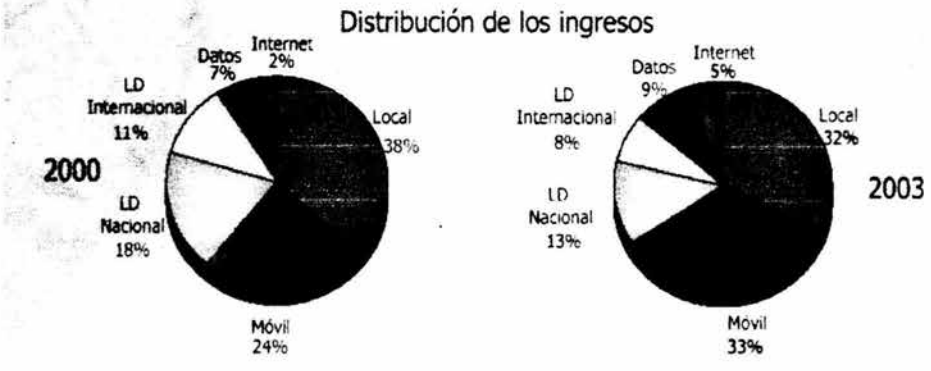


Figura C.1 Aumento del uso del Internet en las comunicaciones.

Como se definió a lo largo de este trabajo de investigación y se resumió en el capítulo 7 la creación de una Red Virtual (VPN), puede solucionar los problemas de conexión remota de compañías pequeñas, medianas y grandes y al mismo tiempo apoyar fuertemente a la reducción de costos de operación de las mismas. Con la solución propuesta en esta trabajo de investigación Pasarela para red privada (VPN Gateway) TESYS podrá seguir creciendo su número de clientes y empleados sin aumentar drásticamente sus costos de operación, lo cual la convertirá en una de las compañías más competitivas del mercado mexicano.

El diseño y puesta en operación de la VPN propuesta para TESYS cumple con los diferentes puntos del objetivo propuesto al inicio de este trabajo de investigación como se resume a continuación:

a) TESYS podrá reducir los gastos de locación por medio de la facilidad de acceso remoto para los empleados desde su casa promoviendo el teletrabajo o trabajo desde casa.

b) TESYS reducirá el número de viajes y por consiguiente los gastos que estos representan por medio del uso de la VPN, la cual permitirá la conexión remota por medio de internet desde cualquier parte de la república o del mundo en donde se posea con un acceso a internet o una línea telefónica.

c) Se agilizaran los trámites administrativos y se reducirán los tiempos de respuesta por medio del acceso remoto que tendrán los empleados para hacer consultas y actualizaciones en las bases de datos de TESYS. A su vez los empleados no tendrán que esperar prolongados lapsos de tiempo para la entrega de su documentación (como lo es actualmente en el caso de los viajes).

APÉNDICE A
GLOSARIO DE TERMINOS

Adaptador: Dispositivo que conecta un equipo (por ejemplo un PC) a la red y controla el protocolo eléctrico para la comunicación con esa red; también se denomina tarjeta adaptadora de red, o NIC.

Alta frecuencia (HF): Ondas de radio en el rango de los 3 Mhz a los 30 Mhz que utiliza propagación por visión directa.

Amplitud: Valor de una señal, normalmente se mide en Voltios (tensión), amperios (corriente), o vatios (potencia).

Análisis de Fourier: Técnica matemática utilizada para obtener el espectro de frecuencias de una señal periódica a partir de su representación en el dominio del tiempo.

Ancho de Banda: Diferencia entre las frecuencias más alta y más baja de una señal compuesta. También mide la capacidad de transmisión de información de una línea o de una red.

Angulo de Reflexión: En óptica, el ángulo formado por un rayo de luz que cruza dos medios y la línea perpendicular a la superficie de contacto entre ellos.

Angulo de Refracción: En óptica, el ángulo formado por un rayo de luz refractado cuando cruza dos medios y la línea perpendicular a la superficie a la superficie de contacto entre ellos.

Anillo en estrella: Esta topología se utiliza con el fin de facilitar la administración de la red. Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo.

Antenas de Cornete: **Antena con forma de embudo gigante utilizada en la comunicación de microondas terrestres.**

Antenas Parabólicas: Una antena parabólica se basa en la geometría de una parábola: cada línea paralela a la línea de simetría (línea de vista) refleja la curva en ángulos tales que inciden en un punto común denominado foco. El plato parabólico funciona como un embudo, capturando un amplio rango de ondas y dirigiéndose a un punto común.

APIs (Application Programming Interface): Las interfases de programación de aplicaciones aplicaciones son conjuntos de funciones y comandos que son llamados programáticamente por el código de la aplicación para ejecutar funciones de red

ARP: Protocolo que utiliza las transmisiones a nivel de MAC (Media Access Control, MAC) para convertir una dirección IP de redireccionamiento conocida a su dirección MAC

ASK (Amplitud Shift Keying) : Método de modulación en el que la amplitud de la señal portadora se varia para representar el 0 o el 1 binario.

ATM (Asynchronous Transfer Mode): Una tecnología de redes de alta velocidad que transmite múltiples tipos de información (voz, vídeo, datos) mediante la creación de "paquetes de datos".

AT&T Network Client: software especial para conectar una VPN Gateway y un usuario remoto. Este software es como su nombre lo indica de la compañía AT&T y tiene entre muchas otras ventajas que trabaja con módems a través de un dial-up y un ISP, además de contar con IPSec que aumenta la confidencialidad de la información.

Autenticidad: Característica indispensable en la comunicación a través del Internet y cualquier otro medio de comunicación para garantizar que la persona con la que nos comunicamos es realmente quién dice ser, ya que si no podemos estar facilitando datos íntimos y/o sensibles a una persona o entidad no deseada, que puede hacer con ellos luego lo que le venga en gana.

Autentificación:
El proceso para determinar la identidad de un usuario que está intentando acceder a un sistema.

Autorización:
Proceso destinado a determinar que tipos de actividades se permiten. Normalmente, la autorización, está en el contexto de la autentificación: una vez autentificado el usuario en cuestión, se les puede autorizar realizar diferentes tipos de acceso o actividades.

Aventail Connect: software que sirve para hacer correr aplicaciones de una red corporativa de forma remota, se utiliza principalmente para empresas que tienen la necesidad de que parte de sus empleados corran procesos o soporten aplicaciones de forma remota.

Baja frecuencia (LF): Ondas de radio situadas en el rango de los 30 Khz a los 300 KHz.

Banda ancha: Se refiere a una tecnología en la que la señal comparte el ancho de banda de un medio.

Backbone: La parte de la red que transporta el tráfico más denso: conecta LANs, ya sea dentro de un edificio o a través de una ciudad o región.

Bastion Host:
Un sistema que ha sido configurado para resistir los ataques y que se encuentra instalado en una red en la que se prevé que habrá ataques. Frecuentemente, los Bastión hosts son componentes de las firewalls, o pueden ser servidores Web "exteriores" o sistemas de acceso público. Normalmente, un bastión hosts está ejecutando alguna aplicación o sistema operativo de propósito general (por ejemplo: UNIX, VMS, WNT, etc...) más que un sistema operativo de firewall.

Bridges : Son elementos inteligentes, constituidos como nodos de la red, que conectan entre sí dos subredes, transmitiendo de una a otra el tráfico generado no local. Al distinguir los tráficos locales y no locales, estos elementos disminuyen el mínimo total de paquetes circulando por la red por lo que, en general, habrá menos colisiones y resultará más difícil llegar a la congestión de la red.

Bps: Unidad de medida generalizada para el intercambio de información en Internet y equivale a bits por segundo, siendo un bit la unidad mas pequeña de la representación de información que puede ser un 1 o un 0.

Bus en estrella: Topología híbrida en la cual un "bus" que se cablea físicamente como una estrella por medio de concentradores.

Bus pasivo corto: Topología en la cual se dispone de un cable de hasta 200m, sobre el que se pueden instalar, distribuidas y aleatoriamente, un máximo de 10 rosetas en las que se permite tener conectados simultáneamente hasta 8 terminales.

Bus pasivo extendido: Topología en la cual en el caso de que 200m no sean suficientes para llegar desde la TR1 hasta el emplazamiento donde se encuentran los terminales, se puede instalar este tipo de bus caracterizado por que con él se alcanzan hasta 500m.

Bus largo: Denominado así porque alcanza los 1000m. Presenta una sola rama con resistencia de terminación en su extremo. En este caso, solo se puede conectar una única terminal.

Cable de par trenzado sin blindaje (UTP): Un par trenzado está formado por dos conductores (habitualmente de cobre), cada uno con su aislamiento de plástico de color. El aislamiento de plástico tiene un color asignado a cada banda para su identificación.

Cable de par trenzado blindado (STP): Tiene una funda de metal o un recubrimiento de malla entrelazada que rodea cada par de conductores aislados. La carcasa de metal evita que penetre ruido electromagnético.

Cable coaxial: Transporta señales con rangos de frecuencias más altos que los cables de pares trenzados, en parte debido a que ambos medios de están construidos de forma bastante distinta. En lugar de tener dos hilos, el cable coaxial tiene un núcleo conductor central formado por un hilo sólido o enfilado (habitualmente cobre) recubierto por un aislante de material dieléctrico

Capa de Aplicación ("Application layer"); Esta capa describe como hacen su trabajo los programas de aplicación (navegadores, clientes de correo, terminales remotos, transferencia, etc).

Capa de enlace ("Data Link layer"): Esta capa especifica como se organizan los datos cuando se transmiten en un medio particular. Por ejemplo esta capa define como son los cuadros ("Frames"), las direcciones y las sumas de control ("Checksum") de los paquetes Ethernet.

Capa Física o de Acceso de Red ("Network Access Layer"), responsable del envío de la información sobre el sistema hardware utilizado en cada caso; utiliza un protocolo distinto según el tipo de red física.

Capa de Presentación ("Presentation layer"); Esta capa se ocupa de los aspectos semánticos de la comunicación (describe la sintaxis de los datos a transmitir), estableciendo los arreglos necesarios para que puedan comunicar máquinas que utilicen diversa representación interna para los datos.

Capa de Red: También llamada capa Internet ("Internet Layer"), es la responsable de enviar los datos a través de las distintas redes físicas que pueden conectar una máquina origen con la de destino de la información. Los protocolos de transmisión como el IP están íntimamente asociados a esta capa.

Capa de Sesión ("Session Layer"); es una extensión de la capa de transporte que ofrece control de diálogo y sincronización, aunque en realidad son pocas las aplicaciones que hacen uso de ella. Por ejemplo, las comunicaciones de Internet no la utilizan.

Capa de Transporte ("Transport layer"); esta capa se ocupa de garantizar la fiabilidad del servicio, describe la calidad y naturaleza del envío de datos. Por ejemplo esta capa define cuando y como debe utilizarse la retransmisión para asegurar su llegada.

Capa de aplicación ("Application layer"): Conformada por los protocolos que sirven directamente a los programas de usuario, navegador, e-mail, FTP, TELNET, etc.

CAPI: Para manejar dispositivos RDSI desde los programas de aplicaciones se ha creado el CAPI, que es el acrónimo de "Common ISDN API", y define un protocolo que comunica el programa con el driver a través de dos colas de mensajes, una de envío, para los mensajes enviados por la aplicación al driver, y otra de recepción, para los mensajes enviados desde el driver a la aplicación. Si el sistema es multitarea, cada programa que esté en marcha dispondrá de una cola de recepción de mensajes propia, en cambio, la cola de envío es común a todas las aplicaciones. Cuando un programa envía un mensaje, la respuesta a ese mensaje se envía también como un mensaje.

CCITT: El CCITT tiene como propósito mantener y extender la cooperación internacional para el mejoramiento y el uso racional de las telecomunicaciones de todos los tiempos; promover el desarrollo de facilidades técnicas y sus operaciones más eficientes con una visión para mejorar la eficiencia de los servicios de telecomunicaciones, mejorar su completa utilización y hacer de ellos, en lo posible disponible para todo público; armonizar las acciones de las naciones en el logro de estos fines comunes.

CD Carrier Detect (Detección de Portadora) Indica que existe una portadora en la línea telefónica. Esto es que existe una señal eléctrica valida para envío o recepción de datos.
Certificados digitales: documentos electrónicos basados en la criptografía de clave pública y en el sistema de firmas digitales. La misión principal de un certificado Digital es garantizar con toda confianza el vínculo existente entre una persona, entidad o servidor web con una pareja de claves correspondientes a un sistema criptográfico de clave pública. Un certificado digital es un documento electrónico que contiene datos identificativos de una persona o entidad (empresa, servidor web, etc.) y la llave pública de la misma, haciéndose responsable de la autenticidad de los datos que figuran en el certificado otra persona o entidad de confianza, denominada autoridad certificadora. Las principales Autoridades certificadoras actuales son Verisign (filial de RSA Data Security Inc.) y Thawte.

Certificados digitales: Un certificado digital es un documento electrónico que contiene datos identificativos de una persona o entidad (empresa, servidor web, etc.) y la llave pública de la misma, haciéndose responsable de la autenticidad de los datos que figuran en el certificado otra persona o entidad de confianza, denominada autoridad certificadora. Las principales Autoridades certificadoras actuales son Verisign (filial de RSA Data Security Inc.) y Thawte

Chat de Internet: Medio de comunicación por medio de internet en el cual dos o mas personas pueden estar conversando entre ellos.

Cifrado de clave publica: Un método de cifrado basado en un algoritmo no reversible. El método utiliza dos tipos de claves: la clave publica, que es conocida de forma publica; la clave privada (clave secreta), que es conocida solo por el receptor.

Circuitos Virtuales: Un circuito virtual es una técnica que se utiliza en protocolos de comunicaciones basados en paquetes (la unidad mínima de información es un paquete de bits o bytes). Cada paquete lleva una etiqueta que identifica un camino dentro de la red, camino que indica la ruta que deben seguir estos paquetes para ir desde la computadora origen hasta el destino. Los protocolos de circuitos virtuales disponen de un subprotocolo para abrir y cerrar dichas rutas, es decir, para "llamar" (crear una ruta que conecte nuestra máquina con otra máquina de red) y "colgar" (eliminar esa ruta).

Circuito Virtual Conmutado (SVC): Método de transmisión basado en circuitos virtuales en la que el circuito virtual se crea y solo existe durante el intercambio de información.

Circuito Virtual Permanente (PVC): Un método de transmisión basado en circuitos virtuales en el que el mismo circuito virtual se utiliza en el origen y el destino de forma continua.

Cisco VPN Client: software que permite a los usuarios establecer túneles encriptados seguros a cualquier servidor VPN Cisco, además de soportar los sistemas operativos Windows 95, 98, 2000, ME, NT 4.0, 2000XP, Linux (Intel), Solaris y Mac OSX 10.1 y 10.2.

Clave privada: En cifrado convencional, una clave compartida solo por un par de dispositivos, un emisor y un receptor.

Clave pública: en el cifrado de clave publica, la clave conocida por todos.

Cliente: Un "nodo de la red, como la estación de trabajo de un usuario, que utiliza recursos proporcionados por un servidor; o bien un programa que inicia la comunicación con otro programa denominado servidor.

Codificación: Transformación de la información en señales.

Codificación Bipolar: Un método de codificación bipolar en el que una amplitud 0 representa un 0 binario y amplitudes positivas y negativas representan 1 alternativos.

Codificación polar: Un método de codificación digital a analógico que utiliza dos niveles (positivo y negativo) de amplitud.

Código RUZ (Return to Zero – Código de Retorno a Cero). También se le conoce como código Neutral debido a que solo posee un valor único positivo en volts para representar un 1 binario y cero volts para representar un 0 binario.

Código NRZ (NonReturn to Zero – Código sin Retorno a Cero). En este tipo de código se usa un voltaje positivo para referenciar un 1 binario y un voltaje negativo para representar un 0 binario sin que la señal regrese a un valor de 0 volts en ausencia de señal

COFETEL
La Comisión Federal de Telecomunicaciones, es un órgano administrativo desconcentrado de la Secretaría de Comunicaciones y Transportes, con autonomía técnica y operativa, el cual tendrá las atribuciones que le confiere el Decreto de Creación y el Reglamento Interior de la Secretaría de Comunicaciones y Transportes, con el objeto de regular y promover el desarrollo eficiente de las telecomunicaciones.

Compresión de datos: Describe el proceso de tomar un bloque de datos y reducir su tamaño. Se emplea para eliminar información redundante y para empaquetar caracteres empleados frecuentemente y representarlos con sólo uno o dos bits.

Compresión lógica
Se debe procurar reducir al máximo un volumen de datos almacenados. Esta reducción, en verdad resulta de la eliminación de los campos redundantes y de un uso de la menor cantidad de indicadores lógicos posibles para los campos restantes. Un dato puede ser comprimido usando representación numérica y representación binaria (esta es la más recomendada).

Compresión física
Son varias las técnicas utilizadas, como la sustitución de caracteres repetidos por un comando capaz de expandirlos en la otra extremidad, o hasta la aplicación de un algoritmo que resulte menos los datos a transmitir.

Concentradores (Hubs): Son equipos que permiten estructurar el cableado de las redes. La variedad de tipos y características de estos equipos es muy grande. En un principio eran solo concentradores de cableado, pero cada vez disponen de mayor número de capacidades, como aislamiento de tramos de red, capacidad de conmutación de las salidas para aumentar la capacidad de la red, gestión remota, etc. La tendencia es seguir incorporando más funciones en el concentrador.

Confidencialidad: Debemos estar seguros de que los datos que enviamos no pueden ser leídos por otra persona distinta del destinatario final deseado, o que si ocurre esto, el espía no pueda conocer el mensaje enviado. O en su defecto, que cuando consiga obtener los datos éstos ya no le sirvan para nada. Es decir, debemos estar seguros de que ninguna persona ajena a la transacción puede tener acceso a los datos de la misma. Imaginemos ahora que trabajamos en una empresa y deseamos enviar un correo al director general explicándole el fabuloso contrato que estamos a punto de firmar con un cliente.

Conmutación: Proceso por el que los paquetes son recibidos, almacenados y transmitidos al puerto de destino apropiado.

Conmutadores (Switchs): Los conmutadores tienen la funcionalidad de los concentradores a los que añaden la capacidad principal de dedicar todo el ancho de banda de forma exclusiva a cualquier comunicación entre sus puertos. Esto se consigue debido a que el conmutador no actúa como repetidor multipuerto, sino que únicamente envía paquetes de datos hacia aquella puerta a la que van dirigidos. Esto es posible debido a que los equipos configuran unas tablas de ruteamiento con las direcciones MAC (nivel 2 de OSI) asociadas a cada una de sus puertas.

Conmutación de paquetes: Proceso por el que los paquetes son recibidos, almacenados y transmitidos al puerto de destino apropiado.

Contivity Multi OS VPN Client: software que provee de funcionalidad para los accesos remotos sobre IP a redes de servidores VPN y ruteadores de acceso IP. Este software trabaja virtualmente sobre todas las plataformas de trabajo de PC incluyendo los sistemas operativos Windows 95, 98, 2000, ME, NT, XP, IBM-AIX, SUN-Solaris, HP-VX, Linux y Macintosh.

Control de errores: La ineludible presencia de ruido en las líneas de transmisión provoca errores en el intercambio de información que se debe detectar introduciendo información de control. Así mismo puede incluirse información redundante que permita además corregir los errores cuando se presenten. El problema de ruido puede causar perdidas importantes de información en módem a velocidades altas, existen para ello diversas técnicas para el control de errores.

Concesionamiento: Medio por el cual una empresa o un gobierno otorga el permiso para poder explotar o comercializar con algo (que pueden ser servicios).

Control lógico de enlace LLC ("Logical Link Control"): Define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.
Control de acceso al medio MAC ("Medium Access Control"). Se encarga de administrar la utilización del medio físico cuando varios equipos compiten por su utilización simultanea. El

mecanismo CSMA/ CD ("Carrier Sense Multiple Access with Collision Detection") utilizado en Ethernet es un típico ejemplo de esta subcapa.

CRL: Listas de Certificados Revocados: Para llevar un control de los certificados revocados (no válidos) las autoridades de certificación han implementado unos servidores especiales que contienen bases de datos en las que figuran los certificados anulados, que se conocen con el nombre de lista de certificados revocados, (CRL; Certificate Revoked List). Un CRL es pues un archivo, firmado por la autoridad certificadora, que contiene la fecha de emisión del mismo y una lista de certificados revocados, figurando para cada uno de ellos su número de identificación y la fecha en que ha sido revocado. Cuando nuestro software de seguridad recibe un certificado digital de otra persona o entidad comprueba antes de darlo por bueno si dicho certificado se encuentra en la lista más actualizada de certificados revocados. Si está en la lista, el certificado será rechazado.

Datagrama: En conmutación de paquetes, una unidad de datos independiente.

Datagrama IP: La unidad de datos del protocolo entre redes.

Decibelio (dB): Medida de la energía relativa entre dos puntos de una señal.

Decodificación: Proceso de recuperación de un mensaje codificado a su forma precodificada.

Demodulación: Proceso de separación de una señal portadora de la señal de información.

Desencriptar: Método que se utiliza para descodificar un mensaje o una señal que llega a un determinado destinatario de forma que solo este pueda entenderlo.

Detección de errores: Proceso que determina si algunos bits se han cambiado durante la transmisión.

Detección de intrusión: Detección de rupturas o intentos de rupturas bien sea manual o vía sistemas expertos de software que atentan contra las actividades que se producen en la red o contra la Información disponible en la misma.

Diafonía: Ruido de una línea provocado por las señales que transitan por otras lineas.

Direccionamiento IP: Cada servidor TCP/IP está identificado por una dirección IP lógica. La dirección IP es una dirección de la capa de red y no tiene dependencia sobre la dirección de la capa de enlace de datos (tal como una dirección MAC de una tarjeta de interfase de red). Una dirección IP única es necesaria para cada servidor y componente de red que se comunique usando TCP/IP.
La dirección IP identifica una localización del sistema en la red de la misma manera en que una dirección de postal identifica una casa en la cuadra de una ciudad. Tal como una dirección postal identifica una residencia única, una dirección IP globalmente única y debe tener un formato uniforme.

Dominio del tiempo: Representación matemática que se utiliza para mostrar al tiempo en función de otras variables.

Dominio de la frecuencia: Representación matemática que se utiliza para mostrar a la frecuencia en función de otras variables.

DPSK (Differential Phase Shift – Keying): Método de codificación digital a digital en el que el patrón de bits define el cambio de fase en lugar de la fase actual.

Dual Homed Gateway: Un "Dual Homed Gateway" es un sistema que tiene 2 o más interfaces de red, cada uno de los cuales está conectado a una red diferente. En las configuraciones firewall, un "dual homed gateway" actua generalmente, como bloqueo o filtrador de parte o del total del tráfico que intenta pasar entre las redes.

EHF: Las ondas de frecuencia extremadamente alta (EHF, Extremely High Frecuency) usan la propagación espacial. Los usos para el EHF son predominantemente científicos e incluyen radar, satélite y comunicaciones experimentales.

Encriptar: Método que se utiliza para codificar un mensaje o una señal agregando seguridad a este, de manera que solo el destinatario pueda entenderlo con el respectivo método o algoritmo para desencriptar.

Enlaces E1 : Los Accesos E1 permiten interconectar Redes de Arrea Local (LAN), interconexión de centrales telefónicas de clientes y otras arquitecturas de comunicaciones predominantes en el mercado (SNA, TCP/IP; IPX; DEC Net, entre otros) de forma sencilla y eficiente con insuperable calidad. El servicio de Accesos E1es un sistema que posee un ancho de banda de 2 Mbps compuesto por 32 canales de 64 Kbps en un solo medio de transporte.

Equipos de conectividad: Los equipos de conectividad son todos aquellos dispositivos que ayudaran a que se realice la comunicación remota entre las bases de datos corporativas y los empleados que por alguna u otra razón se encuentren trabajando remotamente, a continuación realizaremos un estudio detallado de equipos de conectividad necesarios el objetivo de TESYS, como son: ruteadores, switch y hubs, modems, gateways, y bridges

Error de bit : El termino error de bit significa que únicamente un bit de una unidad de datos determinada (tal como un byte, unidad de datos o paquete) cambia de 1 a 0 o de 0 a 1

Error de ráfaga: El termino error de ráfaga significa que dos o mas bits de la unidad de datos han cambiado de 1 a 0 o de 0 a 1.

Escritorio: Un PC en red; también denominado cliente.

Explorador: Un paquete de software utilizado para buscar información publicada en el Web; Microsoft Internet Explorer es el navegador más popular.

Espectro de frecuencia.: es la colección de todas las frecuencias componentes que contiene y se muestra representado en un grafico en el dominio de la frecuencia

Estrella jerárquica: Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada par formar una red jerárquica.

Fibra óptica: La fibra óptica, por otro lado, está hecha de plástico o de cristal y transmite las señales en forma de luz. Para comprender cómo funciona la fibra óptica es necesario explorar primero varios aspectos de la naturaleza de la luz.

Firewall(s): Un Firewall 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 red puede ser accesados dentro de esta 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

trafico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. Este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

Firewall a nivel de aplicación: Un sistema firewall en el que el servicio se proporciona por procesos que mantienen estados de conexión completos con TCP y secuenciamiento. Las firewalls a nivel de aplicación, a menudo redirigen el tráfico, de modo que el tráfico saliente, es como si se hubiera originado desde la firewall y no desde el host interno.

Firewall a nivel de red: Una firewall en la que el tráfico es examinado a nivel de paquete, en el protocolo de red.

Firmas digitales: El procedimiento de firma digital lo que hace es obtener un resumen de un documento o de un texto aleatorio y cifrarlo con llave privada del propietario del certificado. Cuando nos llega un certificado, y su firma digital asociada, tan sólo debemos obtener nosotros el resumen el mismo, descifrar la firma con la llave pública del remitente y comprobar que ambos resúmenes coinciden, lo que nos hace estar totalmente seguros de la autenticidad del certificado. Se firma un resumen del documento y no el documento mismo para evitar ataques contra el sistema de cifrado RSA (por ejemplo, encriptar un documento especialmente concebido por un pirata, con lo que éste podría llegar a obtener la llave privada) y para no hacer el proceso demasiado lento.

Frame Relay: Especificación de conmutación de paquetes definida por los dos primeros niveles del modelo OSI. No hay nivel de red. La corrección de errores se realiza extremo a extremo en lugar de realizarla en cada enlace.

Frecuencia: Numero de ciclos por segundo de una señal periódica.

FSK (Frecuency Shift Keying): - Codificación por cambio de frecuencia.

FTP (Protocolo de transferencia de archivos): El objetivo principal de este protocolo son varios puntos, promover el compartir archivos entre computadoras (programas y/ o datos), alentar al uso remoto de las computadoras, y transferir datos de una forma segura y optima por computadora. FTP (File Transfer Protocol; FTP) más que para ser usado por un usuario directamente es para que los programas lo usen entre ellos para comunicarse.

Gateway: Estos dispositivos están pensados para facilitar el acceso entre sistemas o entornos soportando diferentes protocolos. Operan en los niveles más altos del modelo de referencia OSI (nivel de transporte, sesión, presentación y aplicación) y realizan conversión de protocolos para la interconexión de redes con protocolos de alto nivel diferentes. Los gateways incluyen los 7 niveles del modelo de referencia OSI, y aunque son más caros que un bridge o un ruteador, se pueden utilizar como dispositivos universales en una red corporativa compuesta por un gran número de redes de diferentes tipos. Los gateways tienen mayores capacidades que los ruteadores y los bridges porque no sólo conectan redes de diferentes tipos, sino que también aseguran que los datos de una red que transportan son compatibles con los de la otra red. Conectan redes de diferentes arquitecturas procesando sus protocolos y permitiendo que los dispositivos de un tipo de red puedan comunicarse con otros dispositivos de otro tipo de red.

Grupo de trabajo: Un grupo de estaciones de trabajo, servidor(es) y cualquier dispositivo de red dedicado a funciones similares, utilizando aplicaciones similares y/o compartiendo recursos comunes, y actuando como entidad de subred; los miembros pueden tener una zona geográfica o función común; por ejemplo, ingeniería, mercadeo, fabricación y administración.

HF: Las señales de frecuencia alta (HF, High Frecuency) usan propagación ionosférica. Estas señales se desplazan dentro de la ionosfera, donde la diferencia de densidad las refleja de nuevo hacia la tierra. Los usos de señales HF incluyen los radioaficionados (ham radio), la radio de bandas de ciudadanos (CB), las emisiones internacionales, comunicaciones militares, comunicación de larga distancia para aviones y barcos, teléfonos, telégrafos y faxes.

Hiperenlaces: "Puntos vivos" incrustados en páginas Web que permiten a los usuarios desplazarse de un documento a otro, independientemente de su ubicación en la Internet.

HS (High Speed) : Alta velocidad

HTML (HyperText Markup Language): El lenguaje de autoría de Internet; se utiliza para crear páginas Web.

HTTP (Protocolo para la transferencia de hipertextos): El protocolo para la transferencia de hipertextos HTTP (Hyper Text Transfer Protocol;HTTP) es para todos los sistemas de información distribuidos que tengan la necesidad de mostrar la información y pasarla por una comunicación normal haciendo uso de las ligas de este lenguaje. La primera versión de este lenguaje (HTTP 0.9) se uso desde 1990. El Protocolo fue implementado inicialmente para WWW en 1991 como una iniciativa de software y se denominó HTTP 0.9. El protocolo completo fue definido en 1992 e implementado en marzo de 1993.

Hub: El punto central de conexión para un grupo de nodos; útil para la administración centralizada, la capacidad de aislar nodos de problemas y ampliar la cobertura de una LAN.

ICMP: El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol, ICMP) proporciona servicios de resolución de problemas y de reporte de errores para los paquetes que no son entregables. Por ejemplo, si el IP es incapaz de entregar un paquete al servidor destino, el ICMP enviará un mensaje de Destino Inalcanzable (Destination Unreachable) al servidor origen

Identificador de red: El identificador de red (también conocido como dirección de red) identifica los sistemas que están localizados en la misma red física rodeados por ruteadores IP. Todos los sistemas en la misma red física deben tener el mismo identificador de red. El identificador de red debe ser único en la red global.

Identificador de Servidor : El identificador de servidor (también conocido como dirección de servidor) identifica una estación de trabajo, servidor, ruteador u otro dispositivo TCP/IP dentro de una red. La dirección de cada servidor debe ser única al identificador de red.
Una dirección IP tiene 32 bits de longitud. En lugar de trabajar con 32 bits a la vez, es una práctica común segmentar los 32 bits de la dirección IP en cuatro campos de 8 bits llamados octetos. Cada octeto es convertido a un numero decimal (al sistema de numeración de base 10) en el rango de 0 a 255 y separados por un punto. Este formato es llamado notación decimal punteada.

IGMP: El Protocolo de Administración de Grupos de Internet (Internet Group Management Protocol, IGMP) es un protocolo que administra la membresía de los servidores en los grupos IP multicast. Un grupo IP multicast, también conocido como un grupo de servidores (host group), es un conjunto de servidores que escuchan el tráfico IP destinado a una dirección IP multicast específica. El tráfico IP multicast es enviado a una sola dirección MAC pero es procesado por múltiples servidores IP. Un servidor dado escucha en una dirección IP multicast específica y recibe todos los paquetes de esa dirección IP. Algunos aspectos adicionales de la transmisión IP multicast (IP multicasting):

Integridad : Es necesario estar seguro de que los datos que enviamos llegan íntegros, sin modificaciones, a su destino final. En este caso estamos realizando el pedido de una computadora a una tienda virtual, introducimos nuestro número de tarjeta de crédito y nuestra dirección de entrega del equipo. Pero nuestro simpático pirata está a la escucha, intercepta el envío, cambia los datos de la dirección por otros a su gusto y deja que continúe el envío. El resultado será que nuestro amigo disfrutará de una computadora que hemos pagado nosotros. La integridad se consigue combinando Criptografía, funciones hash y firmas digitales.

IP: El IP es un protocolo de datagramas no confiable, sin conexión y principalmente responsable del direccionamiento y enrutamiento de los paquetes entre servidores. Sin conexión significa que una sesión no se establece antes de intercambiar los datos. No confiable significa que la entrega no está garantizada. Un paquete IP podría perderse, entregarse fuera de secuencia, duplicado o retrasado. El IP no intenta recuperarse de este tipo de errores. La confirmación de la entrega de los paquetes y la recuperación de paquetes perdidos es responsabilidad de un protocolo de alguna capa superior, tal como el TCP.

IPSec: Protocolo especialmente creado para aumentar la seguridad de la información cuando esta para a traves de una red publica, como lo es internet. IPSec utiliza dos mecanismos que garantizan la seguridad, uno es Authentication Header (AH) que autentifica cada paquete y asegura la integridad de los datos ya que detecta cualquier alteración durante la transmisión; el otro es el Encapsulating Segurity Payload (ESP) que encripta y desencripta los datos utilizando algoritmos estándar como DES 56bit y 3 DES a 168 bits.

ISO (International Standards Organization): Organismo internacional dedicado a establecer acuerdos mundiales sobre estándares internacionales.

Líneas dedicadas: Son líneas en las cuales el acceso al Web y el acceso a su propio sitio Web no se verán afectados por ninguna otra actividad de los enlaces de su ISP. También puede alquilar líneas telefónicas a operadores de redes telefónicas para constituir el backbone de una WAN. El principal beneficio de las líneas dedicadas es la facilidad de acceso y la gran cantidad de ancho de banda.

Listas de Certificados Revocados. (CRL): listas generadas por las autoridades de certificación. Un CRL es pues un archivo, firmado por la autoridad certificadora, que contiene la fecha de emisión del mismo y una lista de certificados revocados, figurando para cada uno de ellos su número de identificación y la fecha en que ha sido revocado.

Local: Normalmente hace referencia a dispositivos adjuntos a la estación de trabajo del usuario, en contraposición a dispositivos remotos a los que se tiene acceso a través de un servidor.

LF: De forma similar al VLF, las ondas de baja frecuencia (LF, Low Frecuency) se propagan también como ondas de superficie. Las ondas LF se usan para radio-navegación de largo alcance y para las radio balizas o localizadores de navegación. La atenuación es mayor durante el día, cuando se incrementa la absorción de las ondas por los obstáculos naturales
Máscaras de subred: Con el advenimiento de las subredes, ya no se puede apoyar en la definición de las clases de direcciones IP para determinar el identificador de red en la dirección IP. Se necesita un nuevo valor para definir que parte de la dirección IP es el identificador de red y que parte es el identificador de servido, sin importar si se utilicen identificadores de red basados en clase o en subredes.

Medios Guiados: Los medios guiados son aquellos que proporcionan un conductor de un dispositivo al otro e incluyen cables de pares trenzados, cables coaxiales y cables de fibra óptica. Una señal viajando por cualquiera de estos medios es dirigida y contenida por los límites físicos del medio.

Medios no guiados: Los medios no guiados, o comunicaciones sin cable, transportan ondas electromagnéticas sin usar un conductor físico. En su lugar, las señales se radian a través del aire(o el agua, en algunos pocos casos, el agua) y, por tanto, están disponibles para cualquiera que tenga un dispositivo capaz de aceptarlas.

MF: Las señales de frecuencia alta (MF, Middle Frecuency) se propagan en la troposfera. Estas frecuencias son absorbidas por la ionosfera. La absorción se incrementa durante el día, pero la mayoría de las transmisiones MF se efectúan con antenas de visión directa para incrementar el control y evitar también los problemas de absorción. Los usos de las transmisiones MF incluyen radio AM , radio marítima, buscadores audiodireccionales (RDF) y frecuencias de emergencia.

Módems. Un módem es un dispositivo que traduce datos a ondas eléctricas que pueden ser transportadas a través de líneas telefónicas. Esta tecnología es muy económica y puede ser suficiente para la transmisión diaria de pequeños archivos y de correo electrónico. La velocidad de transmisión más habitual ha pasado de 28.800 bits por segundo (28,8 Kbps) a 57.600 bits por segundo (57,6 Kbps).

Módem: El módem es un dispositivo que permite conectar dos computadoras utilizando la línea telefónica de forma que puedan intercambiar información entre sí. El módem es uno de los métodos mas extendidos para este tipo de interconexión de computadoras por su sencillez y bajo costo. La gran cobertura de la red telefónica convencional posibilita la casi inmediata conexión de dos computadoras si se utiliza módem. Por todas estas razones el modem es considerado el método más popular de acceso a la Internet por parte de los usuarios privados y muchas de las empresas.

Modelo OSI: Es una arquitectura por niveles para el diseño de sistemas de red que permite la comunicación entre todos los tipos de computadoras. Esta compuesto por siete niveles separados, pero relacionados, cada uno de los cuales define un segmento del proceso necesario para mover la información a través de una red.

Modos de propagación: La tecnología actual proporciona dos modos de propagación de la luz a lo largo de canales ópticos, cada uno del os cuales necesita fibras con características distintas: multimodo y monomodo. A su vez, el multimodo se puede implementar de dos maneras: índice escalonado o de índice de gradiente gradual.

Modulación Digital: Los Módem digitales no ejecutan exactamente una modulación, sino una especie de codificación de una señal que difiere mucho con relación a una señal analógica generada por los Módem analógicos.

Modulación Analógica: Una señal digital generada por el equipo de procesamiento de datos es generada en la onda portadora generada por el módem, siendo que las características originales de la onda padrón son modificadas de acuerdo a la técnica de modulación utilizada por el módem y esta transporta los datos hasta la otra extremidad del enlace donde otro módem demudará la señal y la entregará a un equipo de procesamiento de datos en su forma original.

Modulación ASK: La amplitud de la onda es alterada de acuerdo con la variación de la señal de información. Exige un medio en que la respuesta de amplitud sea estable, ya que este tipo de modulación es bastante sensible a ruidos y distorsiones.

Modulación FSK: Consiste en un procedimiento de 2 osciladores con Frecuencias Diferentes para dígitos 0 y 1. Normalmente es usada para transmisión de datos en bajas velocidades y puede ser: Coherente: Donde no ocurre variación de fase de la portadora para dígitos del mismo valor. No Coherente: Donde puede ocurrir variación de fase de la portadora para dígitos del mismo valor.

Modulación PSK: Consiste en un procedimiento de la onda portadora en función de un bit de dato (0, 1). Un bit 0 corresponde a la fase 0; en cuanto al bit 1, corresponde a la fase g . Por tanto, este ángulo está asociado con un dato al ser transmitido y con una técnica de codificación usada para representar un bit. Es decir, cada cambio de fase es como si la porción de onda que sigue a dicho cambio, se adelantara (o atrasara) con relación a lo que debiera ser una forma senoidal continua, pura.

Modulación DPSK: Variación de la modulación PSK, que tiene como característica un procedimiento de la fase de acuerdo con un dígito a ser transmitido.

Modulación QAM: Es caracterizada por la superposición de 2 portadoras en cuadratura moduladas en amplitud. Con eso al colocar 4 bits dentro de un tronco de señal y operar con tasas de 2400 bauds, se alcanza tasas de 9600 bps.

Modulación: La Modulación es la Técnica empleada para modificar una señal con la finalidad de posibilitar el transporte de informaciones a través de un canal de comunicación y recuperar la señal en su forma original en la otra extremidad.

Monomodo: Usa fibra de índice escalonado y una fuente de luz muy enfocada que limita los rayos a un rango muy pequeño de ángulos, todos cerca de la horizontal. La fibra monomodo se fabrica con un diámetro mucho más pequeño que las fibras multimodo y con una densidad (índice de refracción) sustancialmente menor. El decrecimiento de densidad da como resultado un ángulo critico que está muy cerca de los 90 grados para hacer que la propagación de los rayos sea casi horizontal. En este caso, la propagación de los distintos rayos es casi idéntica y los retrasos son despreciables. Todos los rayos llegan al destino –juntos- y se pueden recombinar sin distorsionar la señal.

MR Significa Modem Ready (Módem Listo): Indica que el módem se encuentra conectado a la corriente eléctrica.

Multimodo: Se denomina así porque hay múltiples rayos de luz de una fuente luminosa que se mueven a través de del núcleo por caminos distintos. Cómo se mueven estos rayos dentro del cable depende de la estructura del núcleo. En la fibra multimodo de índice escalonado, la densidad del núcleo permanece constante desde el centro hasta los bordes. Un rayo de luz se mueve a través de esta densidad constante en línea recta hasta que alcanza la interfaz del núcleo y la cubierta. En la interfaz, hay un cambio abrupto a una densidad más baja que altera el ángulo de movimiento del rayo. El término de índice escalonado se refiere a la rapidez de este cambio

Niveles de señalización (STS) : Como lo mas importante es la flexibilidad, SONET define una jerarquía de niveles de señalización denominados señales de transporte síncronas (STS) . Cada nivel STS (STS-1 a STS-192) soporta una cierta tasa de datos, especificada en megabits por segundo. Los enlaces físicos definidos para transportar cada nivel de STS se denominan portadoras ópticas (OC) . Los niveles OC describen las especificaciones físicas y conceptuales de los enlaces requeridos para admitir cada nivel de señalización.

Nodo: Cada una de las computadoras individuales u otros dispositivos de la red.

No repudio: Debemos estar seguros de que una vez enviado un mensaje con datos importantes o sensibles el destinatario de los mismos no pueda negar el haberlos recibido. Y en una compra on-line debe garantizarse que una vez finalizada la misma ninguna de las partes que intervienen pueda negar haber participado en ella. Vamos entonces a imaginar que nuestra empresa tiene que enviar un presupuesto antes de una fecha determinada, presupuesto que debe ser recogido por un empleado de otra empresa, y que éste olvida comunicar a sus superiores la recepción del presupuesto.

NFS (Sistema de Archivos de Red): NFS (Network File System; NFS) es un sistema distribuido para archivos, este es para las redes heterogéneas, con este protocolo, el usuario solo ve un directorio cuando esta dentro de la red, claro que tiene ramas dentro pero no puede ver mas arriba de el nivel en el que se entra, tal ves los archivos dentro de esta estructura del directorio ni siquiera están en la misma computadora.

OH Off Hook (Descolgado) Indica que la línea telefónica esta descolgada.

QAM (Quadrature Amplitude Modulation – Modulación por Amplitud en Cuadratura).

Pagina de inicio: La página principal de un sitio Web y la primera pantalla que ve un visitante cuando se conecta a ese sitio; normalmente dispone de enlaces a otras páginas, tanto en ese mismo sitio como a otros sitios.

PSK (Phase Shift – Keying – Codificación por Cambio de Face).

Política: Reglas de gobierno a nivel empresarial/organizativo que afectan a los recursos Informáticos, prácticas de seguridad y procedimientos operativos.

Protocolo de Oficina Postal Versión 3 (POP3) : POP3 (Post Office Protocol Version 3) es netamente un protocolo para la administración de correo en Internet. El Protocolo de oficina de correos - Versión 3 (POP3) está destinado a permitir que una estación de trabajo acceda dinámicamente a un maildrop en un host servidor de forma útil y eficiente. Esto significa que el protocolo POP3 se usa para permitir a una estación de trabajo recobrar correo que el servidor tiene almacenado.

Proxy: Un agente software que actúa en beneficio de un usuario. Los proxies típicos, aceptan una conexión de un usuario, toman una decisión al respecto de si el usuario o cliente IP es o no un usuario del proxy, quizás realicen procesos de autentificación adicionales y entonces completan una conexión entre el usuario y el destino remoto.

Protocolo: Reglas para la comunicación.

Protocolo asincrono: Conjunto de reglas para la transmisión asíncrona.

Protocolos bases del TCP/IP: El componente del protocolo TCP/IP que está instalado en su sistema operativo es una serie de protocolos interconectados llamados los protocolos base del TCP/IP. Todas las demás aplicaciones y demás protocolos en el grupo de protocolos TCP/IP se apoyan en los servicios básicos proporcionados por los siguientes protocolos: IP, ARP, ICMP, IGMP, TCP, y UDP.

Protocolo de Conversión de Dirección (Address Resolution Protocol, ARP): es responsable de la conversión de las direcciones de la capa de Internet a las direcciones de la capa de la interfase de red, tales como las direcciones de hardware.

Protocolo IP SEC: IPSec utiliza dos mecanismos que garantizan la seguridad, uno es Authentication Header (AH) que autentifica cada paquete y asegura la integridad de los datos ya que detecta cualquier alteración durante la transmisión; el otro es el Encapsulating Segurity Payload (ESP) que encripta y desencripta los datos utilizando algoritmos estándar como DES 56bit y 3 DES a 168 bits.

Protocolo de oficina postal versión 3 (POP3): POP3 (Post Office Protocol Versión 3) es netamente un protocolo para la administración de correo en Internet. En algunos nodos menores de Internet normalmente es poco práctico mantener un sistema de transporte de mensajes (MTS). Por ejemplo, es posible que una estación de trabajo no tenga recursos suficientes (espacio en disco, entre otros) para permitir que un servidor y un sistema local asociado de entrega de correo estén residentes y continuamente en ejecución. De forma similar, puede ser caro (o incluso imposible) mantener una computadora personal interconectada a una red tipo IP durante grandes cantidades de tiempo (el nodo carece el recurso conocido como "connectivity").A pesar de esto, a menudo es muy útil poder administrar correo sobre estos nodos y frecuentemente soportan un user agent (UA) (agente de usuario) para ayudar en las tareas de manejo de correo. Para resolver el problema, un nodo que sí sea capaz de soportar un MTS ofrecerá a estos nodos menos dotados un servicio de maildrop. Se entiende por maildrop, el "lugar" en el sistema con el MTS donde el correo es almacenado para que los otros nodos puedan trabajar con él sin necesidad de mantener su propio MTS.

PROTOCOLOS TCP/IP: El TCP/IP (Transfer Control Protocol / Internet Protocol) es un grupo de protocolos estándares de la industria diseñados para grandes redes que incluyen los enlaces de las redes de área amplia (wide area network, WAN). El TCP/IP fue desarrollado en 1969 por la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de los Estados Unidos (Department of Defense Advanced Research Projects Agency, DARPA), el resultado de un experimento para compartir recursos llamado la Red de la Agencia de Proyectos de Investigación Avanzada (Advanced Research Projects Agency Network, ARPANET). El propósito del TCP/IP fue proporcionar enlaces de redes para comunicación de alta velocidad

Radiofrecuencias: La sección del espectro electromagnético definido como comunicación de radio se divide en ocho rangos, denominados bandas, cada una de ellas reguladas por las autoridades gubernamentales. Estas bandas se clasifican desde frecuencia muy baja (VLF, Very Low Frecuency) a frecuencia extremadamente alta (EHF, Extremely High Frecuency).

RAS (Remote Server Access) : Forma de comunicarse remotamente a las instalaciones dentro de una LAN por medio de troncales digitales y una PSTN.

Red de Área Extensa (WAN): Una red dispersada geográficamente que conecta dos o más LANs; normalmente implica líneas telefónicas dedicadas de alta velocidad o satélites.

Red de Área Local (LAN): Estaciones de trabajo y computadoras conectados en un área de trabajo específica en la misma ubicación general.

Red digital de servicios integrados (RDSI): son las siglas de la Red Digital de Servicios Integrados. La diferencia más importante entre una conexión RDSI y un módem es que en lugar de convertir los datos en una onda eléctrica, el sistema transporta la información en su propio código. De este modo consume menos ancho de banda, lo que significa que RDSI puede transmitir

archivos de mayor tamaño a mayor velocidad. Un enlace RDSI de alta velocidad puede gestionar velocidades de hasta 2 millones de bits por segundo. Suficiente para transmitir una película VHS en tiempo real.

Redundancia: Un mecanismo de detección de errores que satisfaga estos requisitos sería enviar dos veces cada unidad de datos. El dispositivo receptor sería entonces capaz de hacer una comparación de cada unidad de datos. Cualquier discrepancia indicaría un error y se podría corregir mediante un mecanismo apropiado.

Reflexión: Cuando el ángulo de incidencia se hace mayor que el ángulo crítico, se produce un fenómeno denominado reflexión (o más exactamente, reflexión completa, porque algunos aspectos de la reflexión siempre coexisten con la refracción). En este caso, ya no pasa nada de la luz al medio menos denso, porque el ángulo de incidencia es siempre igual al ángulo de reflexión.

Refracción: La luz se propaga en línea recta mientras se mueve a través de una única sustancia uniforme. Sí un rayo de luz que se propaga a través de una sustancia entra de repente en otra (más o menos densa), su velocidad cambia abruptamente, causando que el rayo cambie de dirección. Este cambio se denomina refracción. Una paja que sobresale de un vaso de agua parece estar torcida, o incluso rota, debido a que la luz a través de la que la vemos cambia de dirección a medida que se mueve del aire al agua. La dirección en la que se refracta un rayo de luz depende del cambio de densidad que encuentre. Un rayo de luz que se mueva de una sustancia menos densa a un medio más denso se curva hacia el eje vertical. Los dos ángulos formados por el rayo de luz en relación al eje vertical se denominan I, para incidente y R, para refractado.

Router: Un dispositivo que conecta dos redes; opera como un bridge pero también puede seleccionar rutas a través de una red.

Ruteadores (Routers): Son dispositivos inteligentes que trabajan en el nivel de red del modelo de referencia OSI, por lo que son dependientes del protocolo particular de cada red. Envían paquetes de datos de un protocolo común, desde una red a otra. Convierten los paquetes de información de la red de área local (LAN), en paquetes capaces de ser enviados mediante redes de área extensa (WAN). Durante el envío, el ruteador examina el paquete buscando la dirección de destino y consultando su propia tabla de direcciones, la cual mantiene actualizada intercambiando direcciones con los demás ruteadores para establecer rutas de enlace a través de las redes que los interconectan. Este intercambio de información entre ruteadores se realiza mediante protocolos de gestión propietarios.

Satélites geosincrónicos: se llaman así por moverse a la misma velocidad que la tierra de forma que parezca que está fijo en un cierto punto. Debido a que la velocidad orbital depende de la distancia desde el planeta, solamente hay una órbita que puede ser geosincrónica. Esta órbita se produce en el plano ecuatorial y está aproximadamente a 36.000 kilómetros de la superficie de la tierra. Pero un único satélite geosincrónico no puede cubrir toda la tierra
SD Send Data (Envío de Datos)

Señal: Ondas electromagnéticas propagadas a través de un medio de transmisión.

Señales Analógicas: Forma de onda continua que cambia ligeramente con el tiempo.

Señales Descompuestas: Una señal periódica descompuesta en dos ondas senosoidales

Señales Digitales: Es una señal de tiempo discreto, cuyos valores pertenecen a un conjunto finito

Señales aperiódicas: Señal que no exhibe un patrón o repetición cíclica.

Señales Periódicas: Señal que exhibe un patrón repetitivo.

Servicios de la RDSI: La RDSI puede ser la infraestructura soporte de los servicios de telecomunicación ya establecidos y de aquellos nuevos que, por su mayor capacidad, pueda ofrecer frente a las redes convencionales. Los servicios que en la RDSI se contemplan se dividen en dos categorías básicas

Servicios portadores: Estos servicios ofrecen al usuario RDSI, mediante una serie de interfaces normalizadas, una capacidad de transporte de información, independientemente de su contenido y aplicación, entre dos equipos terminales. Atendiendo a cómo se transmite esta información, podemos clasificarlos en:

Servidor: Un nodo de red que proporciona servicios a PCs clientes; por ejemplo, acceso a archivos, centro de impresión o ejecución remota.

Servidor de aplicaciones: servidor que contiene todas o la mayoria de las apliaciones de una empresa.

Servidor DHCP: El protocolo utilizado en un servidor DHCP, es el protocolo de configuración dinámica de estación (DHCP;Dynamic Host Configuration Protocol) que proporciona una configuración dinámica, en la cual el administrador no necesita especificar una dirección IP en particular.

Servidor DNS (servidor de nombres) : Servidor que se utiliza para identificar una entidad, los protocolos TCP/IP utilizan direcciones IP, que identifican de forma única la conexión de una PC a Internet. Sin embargo, la gente prefiere utilizar nombres en lugar de direcciones.
Por lo tanto, es necesario un sistema con un servidor que puede proyectar un nombre en una dirección y de forma inversa una dirección en un nombre.

El protocolo que utiliza un servidor DNS es el sistema de nombres de dominio (DNS; Domain Name System) es un protocolo que se puede utilizar en plataformas diferentes.

Servidor de Impresión: Una computadora de aplicación específica que gestiona las impresoras y solicitudes de servicios de impresión; permite que múltiples usuarios compartan una impresora en red.

Servidores proxy: Un servidor proxy es una aplicación que media en el tráfico que se produce entre una red protegida e Internet. Los proxies se utilizan a menudo, como sustitutorios de routers controladores de tráfico, para prevenir el tráfico que pasa directamente entre las redes.

Servidores Seguros: Se entiende por Servidor Seguro un servidor de páginas web que establece una conexión cifrada con el cliente que ha solicitado la conexión, de manera que nadie, salvo el servidor y el cliente, puedan tener acceso a la información transmitida de forma útil. El uso de servidores seguros es un elemento imprescindible en todos aquellos servicios que utilicen información confidencial, como operaciones bancarias on-line, compras por Internet, acceso a servidores de datos sensibles, etc.

Servidor SMTP (correo electrónico): El servidor de red más popular es el de correo electrónico (e-mail). El protocolo que soporta el correo electrónico en Internet es el protocolo sencillo de transferencia de correo electrónico (SMTP; Simple Mail Transfer Protocol). Por medio de este servidor se envían mensajes a otros usuarios de computadoras basadas en direcciones de correo electrónico. El servidor SMTP ofrece el intercambio de correo electrónico entre usuarios de la misma empresa o de diferentes computadoras.

Sistema abierto: Es un modelo que permite que dos sistemas diferentes se puedan comunicar independientemente de la arquitectura subyacente.

SHF: Las ondas de frecuencia super alta (SHF, Súper High Frecuency) se transmiten usando principalmente propagación por visión directa y algo de propagación espacial. Los usos del SHF incluyen las microondas terrestres y satélite y la comunicación radar.

Sincronización: Para realizar la sincronización se transmite una señal que se activa y desactiva, o que varia en función de unas convenciones especificadas. Como la base de tiempos se transmite mediante los cambios de dicha línea, se puede informar así al dispositivo receptor de que debe examinar los datos en un tiempo determinado.

Sistema de archivos de RED (NFS): NFS (Network File System; NFS) es un sistema distribuido para archivos, este es para las redes heterogéneas, con este protocolo, el usuario solo ve un directorio cuando esta dentro de la red, claro que tiene ramas dentro pero no puede ver mas arriba de el nivel en el que se entra, tal ves los archivos dentro de esta estructura del directorio ni siquiera están en la misma computadora.

Sistema Operativo en Red (NOS): Software que administra los recursos de una red; normalmente proporciona servicios para compartir archivos e impresoras, correo electrónico, seguridad, etc.
Software de Conexión Remota: software especial que se utiliza para enlazar un VPN Gateway con un usuario remoto.

SONET: Es un estándar de comunicación entre redes con el fin de generar compatibilidad.

Secure Socket Layer (SSL): Secure Socket Layer es un sistema de protocolos de carácter general diseñado en 1994 por la empresa Nestcape Communcations Corporation, y está basado en la aplicación conjunta de criptografía simétrica, criptografía asimétrica (de llave pública), certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet.

Switch: Los conmutadores o switches tienen la funcionalidad de los concentradores a los que añaden la capacidad principal de dedicar todo el ancho de banda de forma exclusiva a cualquier comunicación entre sus puertos. Esto se consigue debido a que el conmutador no actúa como repetidor multipuerto, sino que únicamente envía paquetes de datos hacia aquella puerta a la que van dirigidos.

TCP: es un servicio de entrega confiable, orientado a conexiones. Los datos son transmitidos en segmentos. Orientado a conexiones significa que una conexión debe establecerse antes de que el servidor intercambie datos. La confiabilidad es lograda asignando un número de secuencia a cada segmento transmitido. Se utiliza una confirmación para verificar que los datos fueron recibidos por el otro servidor. Para cada segmento enviado, el servidor que recibe debe regresar una confirmación (acknowledgment, ACK) dentro de un periodo específico de bytes recibidos. Si una ACK no es recibida, los datos son retransmitidos.

Tecnología de túnel: Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos, a esto se le conoce como encapsulación, además los paquetes van encriptados de forma que los datos son ilegibles para los extraños El servidor busca mediante un ruteador la dirección IP del cliente VPN y en la red de tránsito se envían los datos sin problemas.

Teletrabajo: Una solución que lleva las computadoras a los usuarios, en vez de los usuarios a las computadoras. Si su equipo de trabajo utiliza diariamente la computadora, ya no hay ninguna necesidad de someterles al estrés, pérdida de tiempo e incomodidad que supone el traslado a una oficina remota.

Tipos de máscaras de subred: Las máscaras de subred son frecuentemente expresadas en notación decimal punteada. Una vez que los bits son establecidos para las porciones de identificador de red e identificador de servidor, el número de 32 bits resultante es convertido a notación decimal punteada. Note que aunque esté expresado en notación decimal punteada, una máscara de subred no es una dirección IP.

Topologías: La topología o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio. Existe un número de factores a considerar para determinar cual topología es la más apropiada para una situación dada. Existen tres topologías comunes.

Topología tipo anillo: Las estaciones están unidas unas con otras formando un círculo por medio de un cable común. El último nodo de la cadena se conecta al primero cerrando el anillo. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Con esta metodología, cada nodo examina la información que es enviada a través del anillo. Si la información no está dirigida al nodo que la examina, la pasa al siguiente en el anillo. La desventaja del anillo es que si se rompe una conexión, se cae la red completa.

Topología tipo estrella: La red se une en un único punto, normalmente con un panel de control centralizado, como un concentrador de cableado. Los bloques de información son dirigidos a través del panel de control central hacia sus destinos. Este esquema tiene una ventaja al tener un panel de control que monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red.

Topología tipo bus: Las estaciones están conectadas por un único segmento de cable. A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo. Los nodos en una red de "bus" transmiten la información y esperan que ésta no vaya a chocar con otra información transmitida por otro de los nodos. Si esto ocurre, cada nodo espera una pequeña cantidad de tiempo al azar, después intenta retransmitir la información.

Topologías híbridas: El bus lineal, la estrella y el anillo se combinan algunas veces para formar combinaciones de redes híbridas.

Transformada de Fourier: Técnica matemática que reduce una señal periódica en una serie de señales seno mas sencillas.

TR Terminal Ready (Terminal Lista) Informa que hay un Software activo que reconoce el Módem.

Transporte. Encargada de encapsular los datos a transmitir (de usuario)

Troncal: Camino principal de transmisión de una red.

UHF: Las ondas de frecuencia ultra alta (UHF, Ultra High Frecuency) siempre se usan en propagación de visión directa. Los usos para el UHF incluyen la televisión UHF, los teléfonos móviles, la radio celular, los buscadores y los enlaces de microondas. La comunicación con microondas comienza en la frecuencia 1 Ghz de la banda de UHF y continúa hasta las bandas SHF y EHF.

UDP: El UDP proporciona un servicio de datagrama sin conexión que ofrece entrega no confiable, de mejor esfuerzo de los datos transmitidos en los mensajes. Esto significa que la llegada de los datagramas no está garantizada; ni que la entrega de los paquetes esté en la secuencia correcta. El UDP no se recupera de la pérdida de datos utilizando retransmisión.
El UDP es utilizado por aplicaciones que no requieren confirmación de la recepción de los datos y que típicamente transmiten pequeñas cantidades de datos en un momento dado. El servicio de nombres de NetBIOS, el servicio de datagramas de NetBIOS y el Protocolo Simple de Administración de Redes (Simple Network Management Protocolo, SNMP) son ejemplos de servicios y aplicaciones que utilizan el UDP. La tabla 4.9 describe los campos clave en la cabecera UDP.

Unión Internacional de Telecomunicaciones (UIT) : La Unión Internacional de Telecomunicaciones conocida en ingles como ITU (International Telecomunication Union; ITU)) Es una agencia especializada del Sistema de las Naciones Unidas dedicada al sector de las Telecomunicaciones y cuya sede esta en Ginebra Suiza; Esta unión esta compuesta por gobiernos, compañías privadas, instituciones industriales y científicas que cooperan para un uso racional de las telecomunicaciones.

URL (Uniform Resource Locator): El modo estándar de escribir la dirección de un sitio específico o parte de una información en el Web

Velocidad de señalización: Velocidad de señalización, es una referencia a la velocidad expresada en bauds o baudios (razón o velocidad de señalización) con el que un módem puede transmitir datos. Indica el número de bps transmitidos, lo que la velocidad de transferencia mide realmente es el número de sucesos (eventos), o cambios de señal, que se producen en 1 segundo.

Velocidad de señalización real (Throughput): Define la cantidad de datos que pueden enviarse a través de un módem en un cierto período de tiempo. Un módem de 9600 baudios puede tener un throughput distinto de 9600 bps debido al ruido de la línea (que puede ralentizar) o a la compresión de datos (que puede incrementar la velocidad hasta 4 veces el valor de los baudios).

Velocidad de la luz: 300.000 Kilómetros/segundo (aproximadamente, 186.000 millas/segundo)

VLF : Las ondas de frecuencia muy baja (VLF, Very Low Frecuency) se propagan como ondas de superficie, habitualmente a través del aire, pero algunas veces a través del agua del mar. Las ondas VLF no sufren mucha atenuación debido a la transmisión, pero son sensibles a los altos niveles de ruido atmosférico (calor y electricidad) activo en bajas altitudes. Las ondas VLF se usan principalmente para radio-navegación de largo alcance y para comunicación submarina.

VHF: La mayoría de las ondas de frecuencia muy alta (VHF, Very High Frecuency) usan propagación de visión directa. Los usos del VHF incluyen la televisión VHF, la radio FM, la radio AM de los aviones y la ayuda de navegación de los aviones.

VPN: Las redes privadas virtuales crean un túnel o conducto dedicado de un sitio a otro. Las firewalls o ambos sitios permiten una conexión segura a través de Internet. Las VPNs son una alternativa de coste útil, para usar líneas alquiladas que conecten sucursales o para hacer negocios con clientes habituales. Los datos se encriptan y se envían a través de la conexión,

protegiendo la información y el password. La tecnología de VPN proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privada a través de Internet. Instalando VPNs, se consigue reducir las responsabilidades de gestión de un red loca

VPN Gateway: Dispositivo que controla el trafico de entrada y salida entre uno o mas usuraos y la VPN que utilizan para conectarse a una LAN. Esta LAN usualmente se constituye sobre Internet a través de conexión segura en ella los datos se encriptan y se envían a través de la conexión.

B.2.2 Firewalls de Nokia

Nokia IP350

High Speed Performance
- Optimized for Check Point NG
- Standard 256MB RAM (512 Max)
- 350 Mbps for NG FW-1
- 60 Mbps 3DES VPN
- IDS for 10/100 Ethernets

Flexible Connectivity
- 4 Integrated 10/100 Ethernet Ports
- 2 Option Slots for Dual WAN
  - WAN Connection Backup
- 2 Type II PCMCIA Modem Slots

Rapid Serviceability
- Slide Out Access Tray

Small- and Medium-Enterprise Security Platform

NOKIA

Nokia IP380

High-speed Performance
- Optimized for Check Point NG
- Standard 256MB RAM (1024 Max)
- 600 Mbps for NG FW-1
- 90 Mbps 3DES VPN
- 130 Mbps 3DES VPN W/ Accelerator
- IDS to Support 100mbps Line Speed

Real-world Traffic Flexibility
- Up to 8 Ethernet Ports
- 4 Integrated 10/100 Ethernet Ports
- 2 Type II PCMCIA Modem Slots
- 2 Option Slots
  - Dual 10/100 Mbps Ethernet or WAN
- 1 Internal PMC Slot for the Nokia VPN Encryption Accelerator

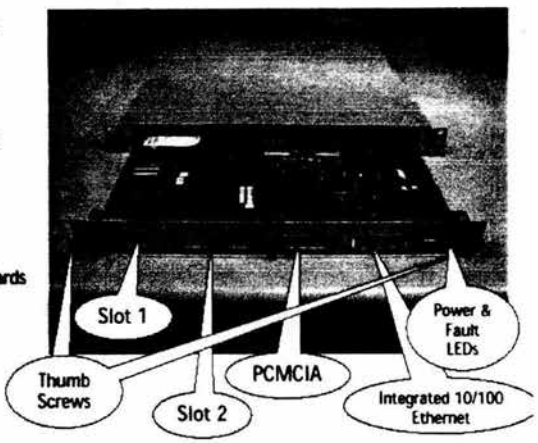
Easily Serviceable
- Slide Out Access Tray

Medium-Enterprise Security Platform

NOKIA

Nokia IP350 and IP380
Advanced Architecture

- Motherboard on Slide-out Tray
  - 1 RU Form Factor
  - Easily Serviceable
  - Auto Power Disconnect
  - Console Port
  - Auxiliary Port
  - FRU'able Internal Components
    - External Facing Interface Cards in Slot 1 & 2
    - Hard Drive
    - Memory DIMMs
    - VPN Card (IP380 Only)



NOKIA

IP350 & IP380 OS and Applications

- IP350 and IP380 Run With IPSO 3.5.1
  - Not Backward Compatible With Older IPSO Versions
  - Customers Cannot Down-grade Factory Ship Software
- Checkpoint NG FP2 Support
  - No Support for Check Point 4.1 Code Series
- ISS Real Secure 6.5 Support
  - IP350 Can Be Deployed to Support 10/100 Ethernet
  - IP380 Can Support 100 Mbps Sensor Rates, Full Duplex (200 Mbps)

CHECK POINT NG NEXT GENERATION

NOKIA

B.5 HOJAS TÉCNICAS DE LOS SERVIDORES

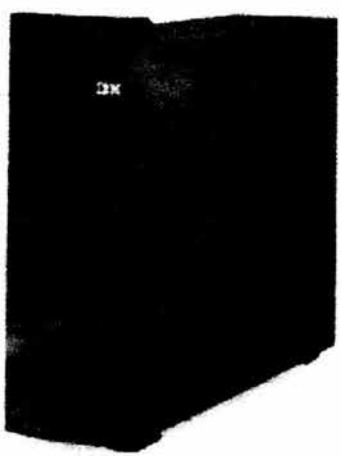
B.5.1 Servidores de IBM.

XSeries 225

Tower with 4U rack capability via optional rack-mount

kit
- Intel Xeon processors at up to 2.8GHz with high-performance 533MHz front-side bus speed
- 512MB standard/8GB maximum PC2100 DDR Chipkill memory
- Up to 6 Ultra320 hot-swap hard disk drives and 880GB max storage on select models
- Hot-swap redundant power models help improve availability
- IBM Director, Remote Deployment Manager and the Remote Supervisor Adapter provide proactive remote management for distributed environments

xSeries 225 overview

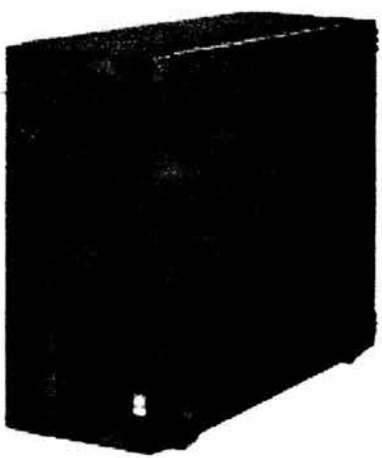


IBM @server xSeries

xSeries 235

5U tower with rack capability via optional rack-mount kit kit
• Up to two Intel® XeonTM processors up to 2.8GHz with high-performance 533MHz front-side bus speed
• 512MB standard/12GB maximum PC2100 DDR ChipkillTM memory
• Up to 1.3TB Ultra320 SCSI storage, no hard disk drive standard
• Hot-swap redundant power and cooling, integrated hard disk drive mirroring and Active PCI-X slots help provide 24/7 availability and data protection

xSeries 235 overview



IBM @server xSeries

B.5.2 Servidores de DELL.

PowerEdge 600SC

- **Costo de Implementación Bajo** - El modelo PowerEdge 600SC es un servidor accesible diseñado para su fácil instalación, excelente funcionamiento, corrección de problemas y capacidad de expansión. El servidor PowerEdge 600SC es la plataforma perfecta para las empresas pequeñas o para los servidores con aplicaciones de grupo de trabajo que requieren de poco soporte de sistemas.

Protección de Datos - Sabemos que el respaldo de datos es una actividad esencial para que las empresas funcionen correctamente. El servidor 600SC soporta soluciones de respaldo en cinta de alta capacidad ya sea con unidades de respaldo en cinta internas IDE (PowerVault™ 100T IDE) o SCSI (PowerVault 100T DDS-4 o PowerVault 110T DLTVS80.

Mayor Tiempo en Funcionamiento - Ordene su sistema con un controlador RAID y establezca redundancia de datos en una solución eficiente para la administración del almacenamiento interior. El mantenimiento del servidor se simplifica con el chasis PowerEdge 600SC al que se le puede dar servicio sencillamente. Entre otras características de disponibilidad se encuentran la memoria ECC y el fácil acceso a componentes internos.

Fabricación de acuerdo a las especificaciones del cliente, Dell Facilita las Cosas - Cada servidor PowerEdge 600SC está fabricado para satisfacer las necesidades de nuestros clientes con una entrega oportuna. Además, usted puede comprarnos un sistema operativo para servidor y nuestros ingenieros expertos lo instalarán por usted. Más aún, para ayudarle en los procesos de instalación e inicio del servidor entregado, ofrecemos una variedad de servicios de instalación y soporte de software (sírvase consultar la sección Servicio y Soporte para mayor información). El servidor PowerEdge 600SC se entrega con el CD Dell Server Assistant para facilitar su instalación y con el sistema Dell OpenManage™ para facilitar la administración integración de la línea de servidores ¡sin cargo adicional!

ESPECIFICACIONES TÉCNICAS.

Un solo procesador Intel® Pentium® 4 de 1.80 GHz o más
Un solo procesador Intel® CeleronTM de 1.70 GHz o más
Bus Frontal
Bus Frontal de 400 MHz
Caché
Pentium 4: Caché L2 de 512 KB
Celeron: Caché L2 de 128 KB
Conjunto de Chips
ServerWorks® Grand ChampionTM SL
Memoria
SDRAM ESS DDR-200 de 128 MB hasta 4 GB
Ranuras de Expansión
5 Ranuras PCI en total
4 de 64 bits y 33 MHz (Soporta tarjetas 3.3V)
1 de 32 bits y 33 MHz (Soporta tarjetas 3.3V)
Controladores
Tres canales integrados IDE para un máximo de seis dispositivos IDE
Controlador 39160 Ultra3 SCSI opcional
Controladores RAID
Controlador RAID IDE CERC ATA-100 opcional (Nivel RAID 0, 1, 5)
Controlador RAID PERC 3/SC opcional (Nivel RAID 0, 1, 5)

Bahías
4 bahías de 1" sin capacidad hot-swap
2 bahías frontales de 5.25" que pueden alojar un CD y/o un DVD-ROM y un TBU
1 bahía estándar de 3.5" para disco floppy
Estándar: 48X EIDE CDROM
Opcional: 16X DVD ROM
Unidades de Disco Duro
Elija entre unidades SCSI o IDE: Unidades de Disco IDE 7,200 RPM: 20 GB1, 40 GB, 80 GB, 120 GB
Unidades de Disco SCSI 10,000 RPM: 18 GB, 36 GB, 73 GB
Capacidad Máxima de Almacenamiento Interno
Un máximo de 480 GB de almacenamiento interno (IDE)
de Respaldo en Cinta Opciones
PowerVault 100T, IDE, TR5, 10 GB
PowerVault 100T, IDE, Travan40, 20/40 GB
PowerVault 100T, SCSI, DDS4, 20/40 GB
PowerVault 110T, SCSI, DLTVS80, 40/80 GB
Comunicaciones
NIC Gigabit Intel integrado
Intel Pro1000XT opcional
Intel Pro 100S opcional
Broadcom 5703 opcional
Módems internos y externos 56K V.90 opcionales
Dispositivos de Captura
Mouse Logitech y Microsoft
Teclados Chicony USB y NMB Rubberdome PS/2
Puertos
2 USB 1.1, 1 paralelo, 1 serial, 1 de video, 1 NIC, 1 mouse PS/2, 1 teclado PS/
Abastecimiento de Energía
Abastecimiento de energía única de 250W
Auto-interruptor de 110/220 Voltios

Sistema de Enfriamiento
Tecnología de enfriamiento activa con tres ventiladores para distribuir la carga enfriadora equitativamente

Chasis
Chasis de torre - 17" (43.1 cm) altura X 8" (20.3 cm) ancho X 19.5" (49.5 cm) profundidad
Peso aproximado: 37 lb. (16.8 kg)

Gráficos
Controlador integrado ATI-Rage XL con 8MB de memoria SDRAM (no tiene capacidad de crecimiento)

Administración
Los dispositivos de administración de sistemas integrados (LM-81 y MAX1617) detectan eventos en el sistema como fallas en ventiladores o problemas de temperatura o voltaje.
El software de administración supervisa los Ventiladores (Ventilador Posterior del Sistema, Ventilador Frontal del Sistema), Voltajes (al centro del CPU, +1.5, +2.5, +3.3, +12 y +5 voltios), Temperaturas (temperatura del CPU) y estado de la memoria.
El software de administración puede leer los registros de incidentes y mostrarlos en la página de Registro de Hardware dentro del software de administración. El usuario también puede definir Acciones de Alerta cuando los censores rebasen los umbrales establecidos.
La opción de recuperación automática permite al sistema reiniciarse o apagarse cuando se quede estático. La opción de apagado térmico, en caso de estar habilitada, puede activar el apagado del sistema operativo o apagado del sistema cuando la temperatura del CPU rebase el umbral establecido. El software funcionará únicamente si la temperatura del CPU es mayor a los límites establecidos durante una cantidad específica de tiempo.

Software
Software Opcional
Microsoft® Windows® 2000 Server
Microsoft Windows® 2000 Small Business Suite
Red Hat® Linux 7.3
Novell® NetWare® Versión 6.0 soportado, no instalado de fábrica
Dell Tape Backup Software por Veritas® Backup ExecTM , Computer Associates® ARCserve® , y TapeWare (IDE)

PowerEdge 2600

El conjunto de chips **Intel®** E7500 está diseñado para soportar a la familia de procesadores de 32 bits Intel de la siguiente generación, tecnología de memoria DDR y el sistema avanzado PCI-X bus I/O. El modelo E7500 soporta micro arquitectura Intel NetBurst™

Incluye **un controlador RAID Ultra320/LVD SCSI de doble canal y alto desempeño opcional** con **caché respaldado con batería de 128 MB** para ofrecer el mejor desempeño posible y protección de datos.

Todos los servidores Dell PowerEdge cuentan con los CDs de administración de sistemas **Dell OpenManage™** para facilitar la instalación, manejo, supervisión y administración de su servidor ¡sin costo adicional!

Con un máximo de **2 procesadores Intel Xeon™** , **584 GB** de capacidad de almacenamiento interno con modalidad hot-plug, **7 ranuras PCI** (6 PCI-X) y **6 ranuras PC2100 DDR SDRAM DIMM**, ¡usted como usuario tendrá espacio suficiente!

Chasis **individual de torre** o rack **5U** que no requiere de herramienta, lo que ofrece **mayor facilidad de servicio** y conservación de espacio de racks.

Sistema de enfriamiento estándar, **redundante y con capacidad hot-plug**, así como **sistema de encendido redundante, hot-plug opcional** para ofrecer mayor disponibilidad y facilidad de servicio.

Ofrece soluciones de administración remota al proporcionar soporte a agentes del software **Dell OpenManage** y **Embedded Server Management III** (ESM III), así como la tarjeta procesador opcional **Embedded Remote Access** (ERA/O) la cual es una solución de hardware que proporciona soporte a administración remota sin requerir una sola ranura

ESPECIFICACIONES TÉCNICAS

Hasta 2 procesadores Intel® Xeon® de 1.80 GHz, 2.0 GHz, 2.20 GHz, 2.40 GHz, 2.60 GHz y 2.80 GHz que incorporan los avances tecnológicos en servidores de doble procesador con micro arquitectura NetBurstTM y tecnología Hyper-Threading

Bus Frontal

Bus frontal de 400 MHz que permite un mejor rendimiento en comparación con las velocidades de los buses frontales de sistemas anteriores

Cache

Caché L2 de 512K para todas las velocidades de los procesadores

Conjunto de Chips

Conjunto de chips Intel E7500

Memoria

6 sockets DDR DIMM que soportan hasta un máximo de 6 GB de memoria principal
128 MB / 256 MB / 512 MB / 1 GB PC2100 DDR en pares para intervalos

Ranuras de Entrada y Salida

7 ranuras de expansión: 2 PCI-X de 64 bits y 133 MHz (Soportan tarjetas 3.3v)
4 PCI-X de 6 bits y 100 MHz (Soporta tarjetas 3.3v)
1 PCI de 32 bits y 33 MHz (Soporta tarjetas anteriores 5v o tarjetas universales)

Controladores

Controlador dual integrado PCI Ultra320 LVD SCSI LSI Logic 53C1030

Controladores RAID

PERC4/Di (Controlador RAID U320 de doble canal con caché de 128 MB respaldado por batería)
PERC3/DC (Controlador RAID PCI de doble canal)
PERC3/QC (Controlador RAID PCI de cuatro canales)

Bahías de Disco

Bahías estándar internas para disco duro que soportan hasta seis unidades de disco SCSI U160 o U320 de 1.0" con plano divisorio Dell y capacidad hot-plug
2 unidades de disco adicionales que se pueden instalar en las bahías de medios
Hasta 24X max. IDE CD-ROM estándar u 8X DVD-ROM/24X CD-ROM opcionales
Unidad para diskettes de 1.44 MB y 3.5" estándar

Discos Duros

(Funcionalidad hot-plug que requiere la incorporación de un controlador RAID) Hasta 8 unidades de disco SCSI con capacidad hot-plug de 1" (6+2)
Unidades de disco SCSI Ultra 160 y Ultra 320 de 10,000 y 15,000 RPM disponibles

Capacidad Máxima de Almacenamiento Interno

Hasta 584 GB de capacidad de almacenamiento interno

Opciones de Almacenamiento Externas

Almacenamiento NAS PowerVaultTM
Almacenamiento SCSI PowerVault
Almacenamiento en Canal de Fibra PowerVault
Dell | Productos EMC

Opciones de Respaldo en Cinta

Interno: PowerVault 100T DDS 4; PowerVault DLT VS80; PowerVault 110T LTO; PowerVault 110T SDLT; PowerVault 110T DLT7000
Externo: PowerVault 112T, PowerVault 120T DLT1 Autoloader, PowerVault 136T y PowerVault 122T VS-80

Comunicaciones

NIC Gigabit individual integrado
Para Mayor Disponibilidad y soporte Contra Fallas NIC: Intel PRO\100 S opcional
NIC de puerto doble Intel PRO\100+ opcional
NIC Gigabit Intel opcional (cobre)
Intel PRO\1000F opcional (fibra)

Dispositivos de Captura

Mouse Logitech y Microsoft
Teclados Chicony y NMB Rubberdome

Puertos USB

Puertos duales para Bus Serial Universal (USB)

Abastecimiento de Energía

Abastecimiento de energía individual o dual de 730W con capacidad hot-plug

Sistema de Enfriamiento

Dos ventiladores redundantes con capacidad hot-plug

Chasis

Torre o rack 5U (el chasis de rack 5U ayuda a conservar el espacio en racks)
Chasis de Torre: 17.5" (44.45cm) altura x 9" (22.86cm) ancho x 24.5" (62.23cm) profundidad
Peso: Aproximadamente 100 lb. (totalmente cargado)

Gráficos

Controlador integrado ATI-Rage XL con 8 MB en memoria SDRAM (no tiene capacidad de crecimiento)
Administración
Controlador integrado ESM III
Tarjeta de administración opcional ERA/O

Software

Software Opcional
Microsoft® Windows® 2000 Server (instalado de fábrica)
Microsoft Windows 2000 Advanced Server (instalado de fábrica
Microsoft Windows NT® Server, Versión 4.0 (validado mas no instalado de fábrica)
Microsoft Small Business Server 2000
Red Hat® Linux 7.2 (no instalado de fábrica - incluido en el empaque)
Novell® NetWare® Versión 6.0 (no instalado de fábrica)
Dell OpenManageTM PowerSuites para Veritas® Backup ExecTM
Dell Tape Backup Software por Veritas Backup ExecTM y Computer Associates® ARCserve®

PowerEdge 4600

- **Construido para entregar velocidad y potencia** - La tecnología de procesador del PowerEdge 4600 - Xeon™ la generación más nueva de Intel® - brinda características tales como microarquitectura NetBurst™ con bus de sistema de 400 MHz, memoria caché de 512 KB L2, velocidades de procesamiento superiores a 2,2 GHz y el nuevo conjunto de instrucciones Streaming SIMD Extensions 2 (SSE2), que añade 144 instrucciones nuevas a las tecnologías MMX™ y SSE. Con tanto espacio disponible en frecuencia y potencia de proceso, el servidor PowerEdge 4600 es ideal para aplicaciones "ávidas" de memoria o ancho de banda, por ejemplo explotación datos (Datamining), previsión financiera, investigación, seguridad y medios de comunicación.

- **Optimizado para el rendimiento** - El chipset del PowerEdge 4600 -el nuevo ServerWorks GC-HE- tiene espacio disponible para hasta doce DIMM 200 (PC1600) DDR registrados con capacidades de 128 MB hasta 1 GB y arquitectura de memoria interfoliada de cuatro vías. El diseño incluye también un algoritmo ECC de 128 bits que realza la confiabilidad del sistema, pues corrige errores de cuatro bits y detecta errores de ocho bits. El chipset apoya la tecnología "chipkill" para mantener la integridad de datos del sistema, incluso en caso de falla de un chip DRAM en la celda de memoria. Cada controlador PCI-X de doble canal tiene su propia conexión dedicada de 1,6 GB/s bidireccional con el North Bridge para atender el tráfico máximo generado por los buses PCI-X que controla.

- **Máxima expandibilidad** - El PowerEdge 4600 tiene capacidad para 10 discos duros, es decir, una capacidad interna total de almacenamiento de 730 GB, con 7 ranuras PCI (seis PCI-X) y 12 GB de memoria. Dos controladores Ethernet integrados (uno Gigabit) y dos controladores SCSI integrados ofrecen espacio disponible, pues la característica está incorporada en el servidor mismo.

- Todos los servidores Dell PowerEdge se entregan con los discos compactos Dell OpenManage™ para instalar, monitorear y manejar su servidor ¡sin pago adicional!

ESPECIFICACIONES TÉCNICAS

Hasta 2 procesadores Intel® XeonTM de 1.80 GHz, 2.0 GHz y 2.20 GHz, 2.60 GHz y 2.80 GHz

Bus Frontal (FSB)

Bus frontal de 400 MHz con velocidad interna de datos superior a las velocidades de los anteriores "legacy" FSB de solo 133 MHz

Memoria Caché

20 KB de memoria caché de Nivel 1 (12 KB de memoria caché para instrucciones y 8 KB de memoria caché para reescritura bidireccional de datos)

512 KB de memoria caché de Nivel 2 (a velocidad máxima del procesador)

Chipset

El chipset ServerWorks Grand Champion High End (GC-HE) utiliza interfoliado tetradireccional de la memoria y una arquitectura de bus PCI de cinco elementos paritarios para entregar un rendimiento E/S máximo

Memoria

512 MB - 12 GB de SDRAM ECC DDR (doble velocidad de datos) de 200 MHz

Con interfoliado tetradireccional de la memoria para entregar un desempeño superior (requiere añadir DIMM en grupos de cuatro de igual capacidad)

Ranuras de Expansión

Enchufable en caliente (Hot-Plug): 6 PCI-X de 64 bits/100 MHz (apoya tarjetas 3,3 V solamente); Legado: 1 x PCI de 32 bits/33 MHz (apoya tarjetas 5V o Universal)

Controladores de Unidad

Adaptec® AIC-7899 Ultra3 (Ultra160)/LVD SCSI integrado, de doble canal, para entregar una de las tecnologías SCSI de alto desempeño más rápidas actualmente disponibles

Adaptec AIC-7890 Ultra-2/LVD SCSI integrado, de un solo canal, dedicado a los dispositivos de cinta internos

Controladores RAID

Controlador PowerEdge Expandible RAID integrado, Versión 3, de doble canal (PERC 3/Di) hasta con 128 MB de memoria caché respaldada por batería (Optional RAID Enabler Kit)

- Ofrece RAID de nivel 0, 1, 5 y 10
- Dos canales con alto grado de flexibilidad: dobla las unidades del chasis principal, dobla las unidades del chasis para medios de grabación y del chasis principal, con un canal interno y otro externo, o enruta ambos externamente y los conecta a un almacenamiento externo

Controlador PowerEdge Expandable RAID opcional, Versión 3, de doble canal (PERC 3/DC)

Controlador PowerEdge Expandable RAID opcional, Versión 3, de cuatro canales (PERC 3/QC)

Chasis para Unidades de Discos

Bahías para unidades de discos enchufables en caliente (Hot Plug): ocho en chasis para unidades de 2,54 cm (1")

Bahías periféricos: Tres chasis de media altura, de 13,34 cm (5,25") -uno ocupado por la combinación CD/DVD-ROM/disquetera; dos disponibles para unidades de cintas ó dos para unidades de discos de 2,54 cm (1") enchufables en caliente

CD-ROM IDE de hasta 24X o DVD estándar

Disquetera estándar de 8,89 cm (3,5") con capacidad para 1,44 MB

Unidades de Discos Duros

Discos duros SCSI de 18 GB, 36 GB y 73 GB (de 2,54 cm, 1") con velocidad de rotación de 10.000 RPM Ultra3 (Ultra160) enchufables en caliente

Discos duros SCSI de 18 GB y 36 GB (de 2,54 cm, 1") con velocidad de rotación de 15.000 RPM Ultra3 (Ultra160) enchufables en caliente
Discos duros de canal de fibra (10.000 RPM), de 18 GB, 36 GB y 73 GB (externos solamente)

Opciones para Resguardo en Cinta

Resguardo en cinta: opción para unidades de cinta tanto internas como externas, autocargadores (Autoloaders) y bibliotecas (Libraries). La máxima tecnología de cinta que incluye: DDS4, DLT1, SDLT y LTO

Comunicaciones

NIC Broadcom® Gigabit integrado y NIC Intel® 10/100/1000. Los NIC integrados apoyan PXE y funciones cooperativas como respaldo y equilibrio de cargas (Load Balancing)
Adaptador Intel® PRO/100+ Dual-Port Server
Adaptador Intel® PRO/100S Server (con encriptamiento IP SEC)
Broadcom NetXtreme 10/100/1000 (Cat-5 Copper Cabling)
Intel PRO/1000 XT
Intel PRO/1000 F
Módem de 56 K1 (interno o externo) modem

Dispositivos de Entrada

Teclado estándar de Windows®
Mouse Dell estilo PS/2

Puertos

2 puertos USB, 2 PS/2, 1 para video, 1 paralelo, 2 seriales, 2 SCSI y 2 RJ-45

Energía

Tres fuentes de alimentación estándares no redundantes, de 300 Watt cada una
Opcional: una cuarta fuente de alimentación de 300 W para redundancia en corriente directa
Interruptor estándar integrado de corriente alterna, que provee redundancia en alimentación CA (dos cordones de corriente pueden conectarse a dos tomacorrientes distintos

Chasis

Configuración en torre (Tower): 44,45 cm (17,5") de alto x 31,14 cm (12,26") de ancho x 70,08 cm (27,59") de profundidad
Configuración en Rack (6U): 27,43 cm (10,8") de alto x 48,01 cm (18,9") de ancho x 70,08 cm (27,59") de profundidad
Peso: 52,16 kg (115 lb)

Gráficas

Controlador ATI-Rage XL integrado con 8 MB de SDRAM

Administración

Pantallas ID y LCD activas, que monitorean el estado de salud del sistema y ayudan a diagnosticar las fallas de componentes
Monitoreo de fallas de voltaje, ventilador y temperatura para asegurar la notificación apropiada en caso de problemas potenciales
Rastrea los errores de memoria corregidos por la memoria ECC
La característica Automatic Server Recovery vuelve a arrancar automáticamente el sistema si el sistema operativo se bloquea

Correo electrónico o radiolocalización a través de Dell OpenManageTM mantiene informados a los administradores sobre los posibles problemas del servidor antes de que dichos problemas alcancen un nivel crítico

Características de administración de activos permiten a los clientes inventariar la configuración del servidor, el CPU, la memoria y la información del disco, lo que ayuda a rastrear el sistema y a mantenerlo al día

Umbrales de sistema operativo definibles por el usuario para afinar el sistema y reducir el congestionamiento en el desempeño

El CD Dell OpenManage Server Setup incluido en cada servidor permite poner en marcha la máquina, operarla y aportar sus recursos rápidamente al resto de la infraestructura de tecnología de la información

Software

Software Opcional

Novell® NetWare® Versión 5.1 y 6.0

Microsoft® Windows NT Server Versión 4.0

Microsoft Windows 2000 Server y Advanced Server

Red Hat® Linux 7.2

Dell OpenManage PowerSuites para Veritas® Backup ExecTM

Dell OpenManage PowerSuites para Computer Associates® ARCserve®

BIBLIOGRAFÍA

Libros:

-Andrew S. Tanenbaum. 1996 Redes De Ordenadores México: Prentice-Hall Hispanoamericana.

-Mischa Schwartz. 1994 Transmisión de información, modulación y ruido. México McGraw-Hill de México.

-Uyless Black. 1997 Redes de computadores (Protocolos, normas e interfaces). Mexico. Alfaomega Grupo Editor.

-Comer, Douglas E. Internetworking with TCP/IP , vol. 1. Prentice Hall, 1995.

-Forouzan. Behrouz. Introduction to Data Communications and Networking. MacGraw- Hill. 1998

-Perlman, Radia . Interconnections: Bridges and Routers. Addison- Wesley. 1992

- Forouzan Behrouz Transmisión de Datos y redes de comunicaciones, 2ª Edición. Mc Graw Hill 2002

-Faynberg, Gabuzda, Lu. 2000. Converged Networks and Services. New York: John Wiley & Sons, Inc.

-Harry Newton, 2000. Newton´s Telecom Dictionary. New York: CMP books.

-Lawrence M. Thompson. 1991. Industrial Data Communications. Research Triangle Park: ISA

-John G. van Bosse. 1998. Signaling in Telecommunication Networks. New York: John Wiley & Sons, Inc.

-James Chellis. 1997. Networking Essentials. Alameda: Sybex Inc.

-Douglas E. Corner. 1999. Computer Networks and Internets. New Jersey: Prentice-Hall.

-Julie Bort. 1997. Building an Extranet. New York: John Wiley & Sons, Inc.

-Ana Martos Rubio. 1998 Así son las Intranets. Madrid: McGraw-Hill Interamericana de España.

-Gregory B. White. 1996. Computer System and Network Security. Boca Raton: CRC Press, Inc.

Referencias electrónicas:

http://www.monografias.com

http://www.cisco.com

http://www.nortelnetworks.com

http://www.cofetel.gob.mx

http://support.aventail.com

http://www.webopedia.com

http://www.iec.org/online/tutorials/

http://www.lacompu.com.mx

http://www.rad.com

MODEMS

http://www.modems.com/

http://www.modemhelp.org

http://www.intel.com/support/faxmodem/4304.htm

http://www.hylafax.org/Modems-PeterChen/04compproto.html

ISDN

http://www.isdnshop.com/isdn-basics.html#isdn

http://www.ralphb.net/ISDN/

http://www.rware.demon.co.uk/isdn.htm

DSL

http://pssi-us.com/DSLInfo.html

EIA / TIA

http://www.eia.org

http://www.tiaonline.org