UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE INGENIERIA

"Sistema de Seguridad para controlar el acceso remoto a la Red Financiera de una Institución Bancaria"

T E S I S

PARA OBTENER EL TITULO DE

INGENIERO MECÁNICO ELECTRICISTA

P R E S E N T A N :

AVILA GALICIA APOLINAR ERNESTO
GARCIA YEVENES MENDEZ JORGE
MAZAS OLIVER NEFTALI
MORALES CONTRERAS SERGIO
VALDIVIESO PEREZ OSCAR

ASESOR: M.I. LAURO SANTIAGO CRUZ

CIUDAD UNIVERSITARIA, MÉXICO, D. F. SEPTIEMBRE 2003

DEDICATORIAS

Este trabajo está dedicado a mis padres; Isaías Avila Mercado, María de la Luz Galicia Segura como un homenaje y agradecimiento por todo el apoyo recibido, por enseñarme a luchar y seguir adelante, por su capacidad de entrega, pero sobre todo por enseñarme a ser responsable, gracias a ustedes he llegado a esta meta y a ser la persona que soy hoy en día. A mis hermanos Arturo y Alejandro, por creer en mi y apoyarme para terminar mi carrera profesional. A mi familia “Gracias por formar parte de mi vida”.

Ernesto Avila Galicia

Este trabajo se los dedico a: Mis padres, que siempre me apoyaron y se sacrificaron por mpi para obtener los estudios que ahora tengo, a mis hermanos que nunca dudaron de mí, a mis amigos que me alentaron a seguir en la carrera y me apoyaron en esta, a mi novia por apoyarme y alentarme a terminar mis estudios y obtener así mi Título Universitario, a todos ellos gracias por dedicarme un poco de su tiempo este trabajo es para ustedes.

Sergio Morales Contreras

Dedicado a mis padres por todo su apoyo, pues sin él no hubiera sido posible la conclusión de mis estudios ni la realización de este trabajo. Así mismo, a mis hermanos por la confianza que me brindaron. Gracias.

Oscar Valdivieso Pérez

A Dios
Quien me ha inspirado y sustenta todos los días
Al recuerdo de mi Padre, A mi Madre
Quien me ha impulsado y a quien debo este trabajo
A Silvia, Jorge Aarón y Stephanie
Quienes me han brindado apoyo incondicional
En todas las cosas que emprendo
A Eva, Juan, Luz María,
José, Juan y Sergio
Quienes me han animado a dar este importante paso

Jorge García Yévenes Méndez

Este trabajo se lo dedico a la persona que me dio la vida y que siempre ha estado al tanto de mí, apoyándome en todo, que ha sido mi ejemplo a seguir y me ha alentado a salir adelante. Sin su ayuda no hubiera podido concluir este trabajo Ana María Oliver Tenorio.

A la memoria de mi padre Ubaldo Mazas Cruz, por la persona que compartiré el resto de mis días y a Saúl. A mis hermanos y a mis amigos, que siempre han confiado en mí, y que han estado conmigo en las buenas y en las malas. A todos ellos gracias por ser parte de mi vida.

Neftalí Mazas Oliver

ÍNDICE TEMÁTICO

LISTA DE FIGURAS

LISTA DE TABLAS

PRÓLOGO

El principal factor que nos motivó a la realización del presente trabajo de investigación, fue la necesidad que tenía la Institución Bancaria de proteger la información que maneja a través de las redes públicas y privadas. Esta necesidad de proteger datos e información es de vital importancia hoy en día, ya que la información que se transmite desde sus oficinas centrales a las sucursales e Intermediarios Financieros es confidencial y se debe evitar que caiga en manos de personas no deseadas. De igual manera un factor motivante es el incremento en los costos y la complejidad de los medios de protección en los sistemas de detección de intrusos en una red, siendo éste un aspecto crítico para mantener un alto nivel de protección en la Red Financiera. En el presente trabajo procuramos innovar tecnológicamente el equipo a usar y los medios existentes para brindar la seguridad adecuada haciendo hincapié en los costos y comparaciones tecnológicas de diversos fabricantes.

Se ha puesto gran cuidado en la organización del presente trabajo, incluyendo figuras y tablas que soportan y ayudan a complementar el texto. Se parte de un levantamiento de información de la Red Financiera para conocer las carencias que presenta y así poder definir las partes más vulnerables. A partir de este punto se definen posibles soluciones que cubran las deficiencias y mejoren la comunicación y seguridad. Finalmente se presentan ejemplos de configuraciones y gráficas que describen las tasas como: utilización de ancho de banda y cargas, que se obtienen durante las pruebas.

Es importante mencionar el formato de algunas palabras que manejamos en este trabajo, como son los tecnicismos en inglés y en español. Las siglas aparecerán en itálicas junto con su descripción únicamente la primera vez que se mencionan, por ejemplo: *LAN (Local Area Network / Red de Area Local)*. Si aparecen posteriormente, el formato será en texto normal

La estructura del trabajo está conformada por 6 capítulos dentro de los cuales se maneja una breve nota introductoria de cada capítulo al inicio. Al final se presenta un apéndice que incluye aspectos de cableado estructurado.

En el presente trabajo de Investigación tratamos los siguientes temas: En el capitulo 1 se presenta una breve introducción que brinda un panorama general sobre las telecomunicaciones, su evolución y la importancia que han adquirido actualmente. En el capítulo 2 se brindan los conceptos teóricos necesarios para la realización del presente trabajo. En el capítulo 3 se determinan las necesidades y los requerimientos que deben ser reforzados o sustituidos en la Red Financiera, así como las posibles soluciones que la propuesta incluye, con base en un análisis del estado actual de la Institución. En el capítulo 4 se desarrolla la solución que se aplicará a la Red Financiera, para corregir las deficiencias detectadas en el capítulo previo. En el capítulo 5 se describe la implementación del sistema, estableciendo la configuración requerida en cada dispositivo que conforma la Red, y así mismo se presentan las pruebas desarrolladas y las gráficas del comportamiento de los enlaces. Finalmente, en el capítulo 6 se describen los resultados y las conclusiones a las que se llegó después de poner en marcha el proyecto respecto a los objetivos iniciales, así como los problemas presentados y posibles mejoras a futuro.

CAPÍTULO 1

INTRODUCCIÓN

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

1.1. Antecedentes Históricos

Desde los tiempos más remotos el ser humano ha buscado la mejor forma de comunicarse con otros de su misma especie, aún cuando éstos se encuentren en lugares lejanos. La historia de la comunicación está marcada por los adelantos tecnológicos de cada época y lugar.

Uno de los adelantos tecnológicos más interesantes de este siglo, es la unión de la ingeniería de las telecomunicaciones con la industria de las computadoras. Por sí solas, ambas industrias han producido muchos cambios en nuestra sociedad. No obstante, éstas se complementan mutuamente y, combinadas, aumentan el poderío de cada una.

En el mundo de las computadoras, la distribución a gran distancia de la información se lleva a cabo en su mayoría mediante las telecomunicaciones. Se envían datos a través de las líneas telefónicas y por medio de satélites a lugares lejanos.

La mayor influencia sobre las telecomunicaciones la tuvo la Segunda Guerra Mundial; en esta época la humanidad ya se encontraba en la frontera de la revolución tecnológica. Muchos de los sucesos que condujeron a la conclusión de la guerra, estuvieron relacionados con la disponibilidad de información oportuna, o con la intercepción ingeniosa de información del enemigo. Los requerimientos de comunicaciones instantáneas, seguras y privadas de esa época fueron determinantes para que las comunicaciones sean lo que son hoy en día.

Con el inicio de la era tecnológica se dispuso del telégrafo, como un medio con el cual fue posible establecer una comunicación a distancia e instantánea por medio de códigos y claves de sonido. Posteriormente la comunicación humana se vio beneficiada con la invención del teléfono, permitiendo el uso de la voz; más adelante vino la radio, la televisión y con ello las computadoras.

Es de vital importancia tener, administrar y transmitir información, ya que toda la humanidad se ve y se seguirá viendo afectada e influida por quienes tienen, administran y transmiten este recurso, razón por la cual a esta época se le han impuesto los calificativos de "sociedad de la información" o de "revolución electrónica", éste último debido a la facilidad con que se transmite la información por medio de los sistemas modernos basados en dispositivos electrónicos.

1.1.1. Historia de las Redes de Computadoras

La aparición de la computadora *ENIAC (Electronic, Numeric, Integrator and Calculator / Integrador y Computador Numérico Electrónico)* estructurada por John Mauchly y John Eckert, y puesta en funcionamiento en 1945, marca el inicio de nuestra era computacional. Se trataba de una máquina electrónica programable y universal. La computadora pesaba más de 30 toneladas, contenía más de 18,000 tubos electrónicos y ocupaba más de 150 metros cuadrados del piso.

En esta época, las computadoras eran de gran tamaño, muy caras, con altos consumos de energía y baja velocidad de procesamiento de información. Además presentaban dificultad en la posibilidad de almacenamiento y en la presentación de instrucciones.

Los primeros intentos para intercambiar información entre computadoras comerciales fue manual, empleando una cinta magnética o una pila de tarjetas perforadas, las cuales necesitaban ser insertadas a la otra computadora mediante la intervención humana, es decir, su funcionamiento no era automático. Más tarde, este proceso se perfeccionó y se logró transmitir información mediante cables conectando 3 o más computadoras, surgiendo así las redes. Esta comunicación se establecía a muy baja velocidad y además había un gran inconveniente, las computadoras que formaban la red tenían que funcionar a la perfección porque a la menor falla de cualquiera de ellas la red dejaba de operar y era necesario desconectarla para dejar funcionando a las demás.

Fue en esta época que las computadoras comenzaron a ser más comunes en las empresas (aunque su precio seguía siendo considerablemente alto), lo que condujo a intentar hacer más flexibles y potentes a estos equipos, logrando incrementar su producción.

Para llegar a los niveles de comunicación actuales se han dedicado años de investigación y perfeccionamiento en la transmisión de datos. Fue en 1969 cuando la *ARPA (Advanced Research Projects Agency / Agencia de Proyectos de Investigación Avanzada)*, del Pentágono, creó la primera red llamada *ARPAnet*, la cual constaba sólo de cuatro computadoras conectadas: una en la Universidad de California, en los Ángeles, otra en el Instituto de Investigaciones de Stanford, una más en la Universidad de California, en Santa Bárbara y la última en la Universidad de UTAH.

En 1974 los investigadores Vint Cerf y Robert Kahn redactaron un documento titulado *"A protocol for Packet Network Internetworking" (Un Protocolo para Interconectividad de Paquetes en una Red)*, donde explicaban cómo podría resolverse el problema de comunicación entre los diferentes tipos de computadoras.

A mediados de los 80's ocurren dos avances importantes en la tecnología:

- **El avance de los microprocesadores.** Inicialmente eran dispositivos de 8 bits, pero pronto surgieron de 16, 32 y hasta 64 bits. Su velocidad de procesamiento fue cada vez mayor y su consumo de energía así como su precio disminuyeron notablemente.

- **Surgimiento de las redes.** Esto permitió que cientos de computadoras fueran conectadas entre sí, de tal manera que pequeñas cantidades de información podían ser transferidas en fracciones de segundo.

Como resultado de estas dos tecnologías surgen los Sistemas Distribuidos que permiten, entre otras cosas, compartir recursos como impresoras, carpetas de archivos y bases de datos. Así mismo, al conectar dos computadoras en red se requiere manejar más recursos, como son: la transferencia de información, direccionamiento, detección y corrección de errores, sincronización y coordinación de la transmisión.

Con el surgimiento de las Redes *LAN (Local Area Network / Redes de Área Local)* disminuyó el alto costo de los medios de procesamiento de datos. La interconexión de redes provee la base de aplicaciones tales como el *E-mail (Electronic-Mail / Correo Electrónico)* y la transferencia de archivos; útiles para incrementar la productividad y la competitividad.

Con el desarrollo de las minicomputadoras y de las redes *WAN (Wide Área Network / Red de Área Extendida)*, se crean los sistemas de redes. Las minicomputadoras ofrecen un camino para acceder a los servicios desde una central de datos, facilitando la distribución y el procesamiento de los mismos. Las redes *DECnet (Digital Equipment Corporation Network / Red de la Corporación Equipo Digital)* son típicas de esta era. Sin embargo, las aplicaciones permanecen separadas e independientes y utilizan diferentes protocolos de comunicación.

En 1982 se creó el protocolo *TCP/IP (Transmition Control Protocol / Internet Protocol │ Protocolo de Control de Transmisión / Protocolo de Internet)* basándose en los estudios efectuados por Vint Cerf y Robert Kahn. Este protocolo es un sistema de comunicación muy sólido y robusto bajo el cual se integran todas las redes. Fue adoptado de inmediato como estándar por el Departamento de Defensa de los Estados Unidos, quien este mismo año se separó de ARPAnet y creó una red propia llamada *MILnet (Red Militar)* gracias al protocolo TCP/IP se incrementó notablemente el número de redes locales de agencias gubernamentales y de universidades que participaban en el proyecto, originando así, la red de redes más grande del mundo. Los nuevos organismos que se fueron integrando dieron a esta red el término *Internet*, tal y como ahora se le conoce mundialmente.

Las aplicaciones militares que dieron origen a las redes finalmente se separaron y se permitió el acceso a la red a todo aquel que lo requiriera, sin importar de que país proviniera, siempre y cuando fuera para fines académicos o de investigación, por tal razón Internet tuvo su etapa de desarrollo fundamentalmente dentro de las Universidades. Hasta este momento la velocidad de transferencia entre nodos era de 56 *kbps (kilobits por segundo)*.

En lo que se refiere a México, en 1987 se pusieron en operación los enlaces digitales por fibra óptica, siendo éste el medio más adecuado para la transmisión de señales luminosas. Fue en este mismo año cuando el *ITESM (Instituto Tecnológico y de Estudios Superiores de Monterrey)*, en el campus Monterrey, logró una conexión a BITnet a 9600 *bps (bits por segundo)*, a través de líneas conmutadas y por medio de una línea privada analógica de 4 hilos. En 1989 lo hizo el ITESM, se conectó a Internet al enlazarse por medio de la Universidad de Texas en San Antonio, por la misma línea privada. La *UNAM (Universidad Nacional Autónoma de México)* accedió a Internet por

medio de una conexión vía satélite de 56 kbps con el *NCAR (National Center for Atmospheric Research / Centro Nacional de Investigación Atmosférica)* de Boulder, Colorado, siendo éste el segundo nodo de Internet en México. Después se interconectaron ambas universidades mexicanas usando líneas privadas analógicas de 9600 bps, velocidad suficiente para proveer correo electrónico, transferencia de archivos y acceso remoto.

Poco a poco se fueron incorporando a Internet otras instituciones educativas mexicanas como son: Universidad de Chapingo en el Estado de México, el Centro de Investigación de Química Aplicada de Saltillo, y el Laboratorio Nacional de Informática Avanzada de Jalapa, Veracruz, los cuales se conectaban al ITESM para salir a Internet. Para esta época, en México ya existía un organismo llamado RED-MEX, donde se discutían las políticas, estatutos y procedimientos que habrían de regir y dirigir el camino del control de la red de comunicación de datos de México.

Tiempo más tarde surgió otro organismo denominado MEXNET, que reunía a representantes legales de cada institución, el cual incluía a varias universidades del país. Dicha organización, en 1992, establece una salida de 56 kbps al *Backbone (cable de comunicación principal)* de Internet.

En 1993 el *CONACYT (Consejo Nacional de Ciencia y Tecnología), el ITAM (Instituto Tecnológico Autónomo de México)* y la *UAM (Universidad Autónoma Metropolitana)* se conectaron a Internet mediante un enlace satelital al NCAR, estableciéndose como el primer *NAP (Network Access Point / Punto de Acceso a la Red)*, al intercambiar tráfico entre dos diferentes redes. A finales de este año en México ya se contaba con distintas redes: MEXnet, Red UNAM, Red ITESM, BAJAnet y Red total CONACYT entre otras. En el mismo año, Internet se abre en el ámbito comercial en México, con lo cual se inicia una nueva era de desarrollo para nuestro país, que beneficia a todas las personas, empresas o instituciones que deciden participar en la proyecto desde sus inicios, ya que hasta entonces sólo instituciones educativas y de investigación tenían acceso a la súper carretera de la información.

Fue en 1994, con la fundación de la *RTN (Red Tecnológica Nacional)*, integrada por MEXnet y CONACYT, que se generó un enlace a 2 *Mbps (Megabits por segundo).*

A finales de 1995 se crea *NIC-México (Names Internet Control / Control de Nombres en Internet),* que se encarga de la coordinación y administración de los recursos de Internet asignados al país, como son la administración y delegación de los nombres de dominio bajo ***".***mx***"***. En 1996 se registran cerca de 17 enlaces *E1 (formado por 32 canales de 64 kbps)* contratados con Telmex para uso privado. Así mismo, se consolidan los principales *ISP (Internet Service Provider / Proveedores de Servicios de Internet)* en el país, de los casi 100 ubicados a lo largo y ancho del territorio nacional. Para el año de 1997 existen más de 150 ISP's, ubicados en los principales centros urbanos: Cd. de México, Guadalajara, Monterrey, Chihuahua, Tijuana, Puebla, Laredo, Saltillo y Oaxaca, entre otros.

Actualmente Internet es utilizado por instituciones educativas y gubernamentales, empresas privadas y personas de todo el mundo, entre quienes se llevan a cabo intercambios constantes de información, dando origen a la llamada globalización de la comunicación. Hasta el día de hoy, gracias a Internet, se puede recibir información al instante desde cualquier parte del mundo, agilizando y facilitando de esta forma el proceso comunicativo a distancia. La integración de los servicios y la privatización de Telmex pretenden garantizar el desarrollo de una red de telecomunicaciones más moderna, impulsando el progreso económico de México. Así mismo, se abre la puerta a una revolución tecnológica que multiplica las formas posibles de acceso a la telefonía, así como la modificación de sus costos.

1.2. Necesidad de Tener Redes Seguras

La necesidad de proteger datos e información de una infraestructura es de vital importancia hoy en día, ya que la información requerida tiende a ser confidencial y se trata de evitar que caiga en manos de personas no deseadas. Esto ha incrementado el costo y la complejidad de los medios de protección y de los sistemas de detección de intrusos en una Red; siendo éste un aspecto crítico para mantener el alto nivel de seguridad de un sistema. Por otro lado, los mecanismos de protección deben asegurar continuamente al negocio y minimizar el impacto del costo de la intrusión.

La amenaza es verdadera, la cantidad de acontecimientos no autorizados de seguridad en la información aumentó en el año 2000. Según un estudio reciente, hay un aumento del 70% en los incidentes de seguridad en las organizaciones examinadas. Este dato esta por encima del 42% señalado en 1996. La mayoría de los expertos de la seguridad sienten que estos números están creciendo innecesariamente, pues hay muchas maneras para que las organizaciones eviten presentar incidentes. Muchas organizaciones también carecen de técnicas para detectar y para reaccionar a eventos que afecten la seguridad de la red.

Un elemento que nos ayuda a reforzar la seguridad en el acceso entre una red externa y una interna, sin disminuir el rendimiento, es el *Firewall (Barrera de fuego),* el cual contiene elementos de hardware y software que le permite establecer parámetros de seguridad y controlar el acceso a recursos de la red, así como a servicios públicos.

Para tener un acceso remoto seguro, es recomendable la autentificación y la encripción para proteger de forma fácil y segura toda la información proporcionada. Para proveer privacidad de información confidencial, los datos en tránsito se encriptan sobre enlaces de comunicación públicos o privados, lo que proporciona beneficios tales como una alta seguridad, elección de algoritmos, administración de mensajes de servicios de red y protección contra las amenazas a la seguridad en el comercio electrónico. Para un amplio rango de aplicaciones, se proporciona amplitud y profundidad que conjuntamente protegen a los servidores del sistema, a las terminales de los usuarios finales y a la infraestructura entre ellos. Uniéndolos todos en una solución integral se elevará el servicio a uno de los más respetados niveles profesionales. Así, los requerimientos fundamentales son:

- Seguridad en servidores centrales.
- Seguridad de escritorio y usuarios finales.
- Seguridad en redes.

Hace falta hardware y software de vanguardia que contribuya con inapreciables niveles de seguridad, realización y funcionamiento, que se apegue a los estándares de redes existentes de protección contra intrusos y además que provea rangos de seguridad y de servicio como el direccionamiento de red y de puerto, así como filtros, integración y servicios de autentificación. Estos equipos también deberán contar con servicio de seguridad para voz y datos entre cliente-servidor.

La integración de servicios de acceso remoto y las capacidades propuestas para conectar un sitio a otro, deben extender el ambiente de las redes de trabajo e incluir el acceso de clientes vía remota o satelital.

1.3. Redes Alternas

La conectividad inalámbrica es lo nuevo en el mundo de las redes de computadoras, las redes inalámbricas involucran la conexión de *laptops (computadoras portátiles)*, *desktops (computadoras de escritorio)*, teléfonos celulares, servidores, etc.

La conectividad inalámbrica trae consigo el potencial de brindarle a los usuarios una conexión a Internet y sus servicios en cualquier lugar y en cualquier momento. Una red inalámbrica es como cualquier otra red, es decir, conecta las computadoras a las redes, pero sin la necesidad de cables. Este tipo de red puede proveer acceso a otras computadoras, bases de datos, e Internet. Para las redes LAN inalámbricas, el hecho de no tener cables, les permite a los usuarios contar con movilidad sin perder la conexión.

Si clasificamos las redes por su alcance geográfico, tenemos dos tipos de redes inalámbricas:

- Redes WAN inalámbricas.
- Redes LAN inalámbricas.

Una WAN es una red de computadoras que abarca una área geográfica relativamente extensa, típicamente permiten a múltiples organismos como oficinas de gobierno, universidades y otras instituciones conectarse en una misma red. Las WAN tradicionales hacen estas conexiones generalmente por medio de líneas telefónicas. Por medio de una WAN Inalámbrica se pueden conectar las diferentes localidades utilizando conexiones satelitales, o por antenas de radio microondas. Estas redes son mucho más flexibles, económicas y fáciles de instalar. En la actualidad, la forma más común de implementación de una red WAN es por medio de Satélites, los cuales enlazan una o más estaciones base, para la emisión y recepción. Los Satélites utilizan

una banda de frecuencias para recibir la información, luego amplifican y repiten la señal para enviarla en otra frecuencia.

Para que la comunicación satelital sea efectiva, generalmente se necesita que los satélites permanezcan estacionarios con respecto a su posición sobre la tierra, si no es así, las estaciones en tierra los perderían de vista. Para mantenerse estacionario, el satélite debe tener un periodo de rotación igual que el de la tierra, y esto sucede cuando el satélite se encuentra en la órbita geoestacionaria a una altura de 35,784 km.

Comunidades de usuarios con intereses comunes, instituciones y empresas, se verán beneficiadas por la conectividad que ofrecerán las redes celulares de datos de la próxima generación.

Nuevos productos, servicios y actividades derivadas de estas tecnologías impulsarán cambios radicales en la manera en que se trabaja hoy en día. Nuevos negocios basados en estas tecnologías saldrán al mercado, y se verá de una vez por todas la utilidad de tener Internet en cualquier lugar y en cualquier momento.

Las redes LAN inalámbricas permiten conectar una red de computadoras en una localidad geográfica, para compartir archivos, servicios, impresoras, y otros recursos. Usualmente utilizan señales de radio, las cuales son captadas comúnmente por tarjetas *PCMCIA (Personal Computer Memory Card International Association / Asociación Internacional de Tarjetas de Memoria para Computadoras Personales)* conectadas a laptops o a *slots (ranuras, conector en el que pueden insertarse tarjetas y ampliaciones a la Tarjeta Principal)*, *PCI (Peripheral Component Interconnect / Interconexión de Componentes Periféricos)* para PCMCIA en computadoras de escritorio. Estas redes soportan generalmente tasas de transmisión entre los 11 Mbps y 54 Mbps; tienen un rango entre 30 y 300 metros, con señales capaces de atravesar paredes.

Redes similares pueden formarse con edificios, o vehículos. Esta tecnología permite conectar un vehículo a la red por medio de un transmisor en una laptop, al punto de acceso dentro del edificio. Estas tecnologías son de gran uso en bibliotecas, unidades móviles como ambulancias para los hospitales, etc.

Las redes LAN inalámbricas ofrecen muchas ventajas sobre las LAN's *Ethernet* convencionales, como son: movilidad, flexibilidad, escalabilidad, velocidad, simplicidad, y costos reducidos de instalación. Son una solución para edificios que por su arquitectura, o su valor histórico, no pueden ser perforados para instalar cableado estructurado.

En los Estados Unidos, muchas bibliotecas han implantado con éxito redes LAN inalámbricas a costos mucho más bajos de lo que saldría implantar redes físicas, y además les permiten el acceso a la red en cualquier lugar de la biblioteca a todos sus usuarios. En México se tiene al Tecnológico de Monterrey como pionero en este tipo de servicios.

1.4. Las Redes de Datos y los Sistemas Financieros

El mundo de las finanzas emplea muchos archivos cuya información cambia constantemente. Entre los primeros sistemas de computadoras de tiempo real se contaron los de los bancos de ahorros, cuyos cajeros empleaban máquinas para poner al corriente las cuentas de los clientes. Una computadora central manejaba los registros de todas las cuentas y la máquina los actualizaba en las ventanillas de cada cajero. La información que se necesitaba sobre cada cuenta se transmitía automáticamente a los cajeros. A menudo el sistema suministraba información a la administración a petición de la misma.

El éxito de ese pequeño principio ha iniciado un cambio que puede extenderse a toda la comunidad financiera y que podrá revolucionar finalmente a todo el sistema actual. Se llevarán a cabo muchas transacciones financieras sin emplear cheques o dinero en efectivo, como ocurre actualmente con las transacciones con tarjetas de crédito. El cliente del banco deberá identificarse de algún modo ante una terminal de telecomunicación y los detalles de la transacción se anotarán con el teclado en la misma terminal. Los datos llegarán a la computadora que contenga los registros de la persona que paga y los de la que recibe el pago, y se acreditarán y cargarán los registros correspondientes. De ese modo, las transacciones financieras se efectuarán mediante la transmisión de datos sin necesidad de documentos, o por lo menos, esos papeles serán externos en el sistema, y no internos como ocurre actualmente y sólo servirán para informar al usuario sobre las transacciones que se hayan efectuado.

Podemos imaginar que en un futuro, el valor del crédito de un individuo se almacenará, en un archivo al que se pueda tener acceso en tiempo real remotamente. Uno de los problemas de esa Red Financiera es la identificación adecuada de cada individuo. Actualmente una tarjeta de crédito reconocida es un medio de identificación para algunos. Sin embargo, esas tarjetas sólo se conceden a individuos que se consideran como confiables.

En este capítulo se ofreció un aspecto general de la evolución de las redes de datos, su desarrollo dentro de México, y las grandes posibilidades que nos proporcionan para implementar infraestructuras confiables y seguras. Sin lugar a duda, los avances tecnológicos llevarán a obtener mejores recursos, pero también crearán nuevas necesidades.

Para entender mejor los términos que se manejan en el uso de las redes y de los dispositivos utilizados en particular, en el siguiente capítulo se definirán aspectos generales.

CAPÍTULO 2

CONCEPTOS BÁSICOS

En el presente capítulo se definen los conceptos más importantes en relación con las redes de computadoras: en su composición, topología y aspectos fundamentales de su funcionamiento, así como los protocolos que utilizan. Se detallan las redes de alta velocidad y equipos de seguridad. Finalmente se describen los tipos de comunicación y el sistema de cableado estructurado que compone una red.

2.1. Redes de Computadoras

Una red de computadoras es un conjunto de terminales, nodos, servidores y elementos de propósito especial que interaccionan entre sí con la finalidad de intercambiar información y compartir recursos.

Anteriormente (aunque existen todavía) la información se almacenaba en los llamados *Mainframes (computadora central)* que poseen una gran rapidez y de costo muy alto, capaces de controlar al mismo tiempo a cientos o miles de usuarios, así como cientos de dispositivos de entrada y salida. En un Mainframe, diferentes terminales se conectaban a él, con la finalidad de recibir y guardar información y conectarse a los recursos. El problema con este tipo de "red" es que se basaba en un sistema centralizado, es decir, en el Mainframe se concentraba toda la información, teniendo por limitante la capacidad de almacenamiento de datos. (*Figura 2.1.*)

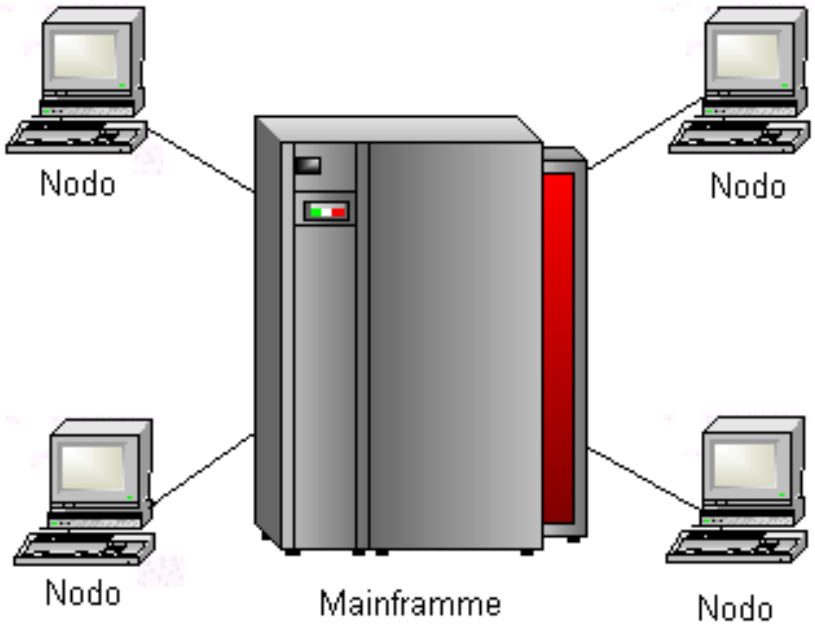

Figura 2.1. Esquema de funcionamiento de un Mainframe.

Por otro lado, con la utilización de un Mainframe, el fallo del mismo provocaba el fallo de todo el sistema, lo cual traía consecuencias muy graves para las organizaciones.

Con la introducción de las diferentes clases de redes de computadoras y tecnologías, surgió la posibilidad de utilizar diferentes servidores que, como su nombre lo indica, proveen servicios a un conjunto de nodos denominados clientes. De esta forma, no existe limitante en cuanto a almacenamiento de información, ya que nuevos servidores pueden ser instalados como lo indica la *Figura 2.2*, dando así, la facilidad en la expansión de las redes.

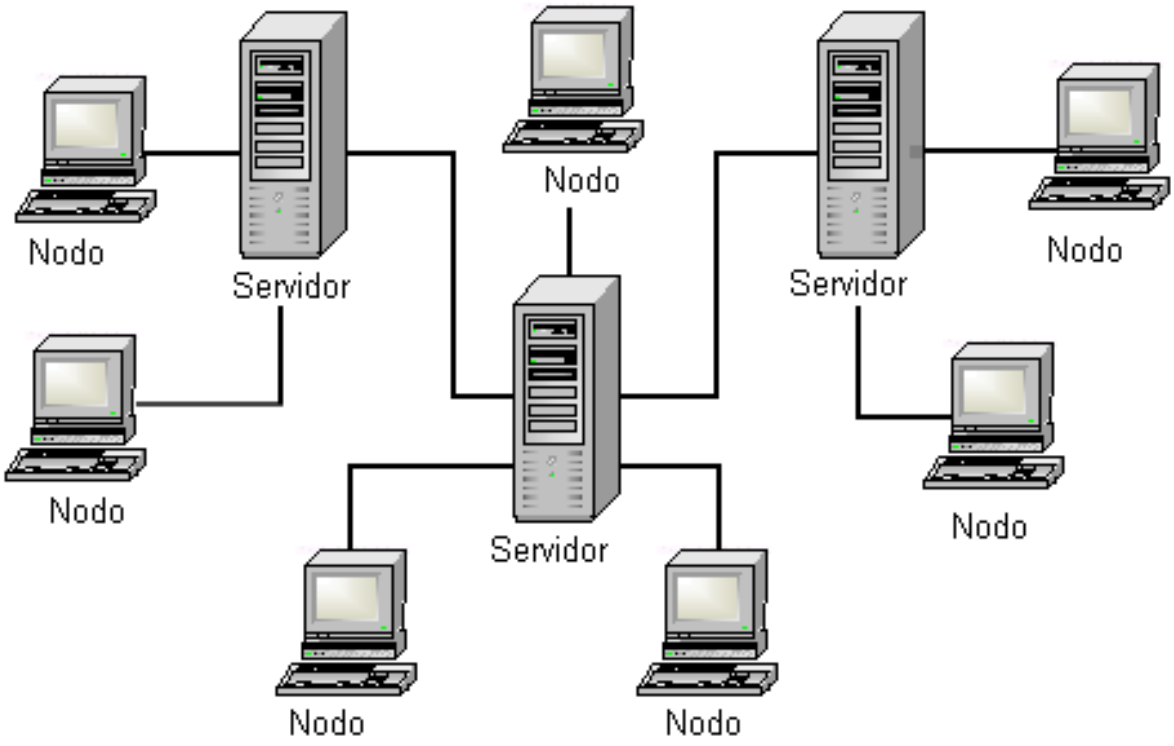

Figura 2.2. Esquema de interconexión Cliente – Servidor.

Otra nombre que suele darse a las redes de computadoras es el de sistema distribuido, donde la existencia de múltiples computadoras independientes es transparente para el usuario, el cual puede teclear una orden para ejecutar un programa y éste se ejecutará sólo en su computadora. La tarea de seleccionar un mejor procesador y colocar los resultados en el lugar apropiado, corresponde al sistema operativo y a la red.

En un sistema distribuido, el usuario no está consciente de que existen múltiples procesadores. El sistema se ve como un único procesador virtual.

Las razones principales que se pueden tomar en consideración para la utilización de una red de computadoras son:

Integridad: hacer de un sistema de varios elementos una sola herramienta, en donde se utilicen las características y las aptitudes de cada uno de la mejor forma posible.

Flexibilidad: facilidad en su uso, intercambio ágil de datos en cualquier momento y posibilidad de crecimiento.

2.2. Comunicación Entre Redes

La comunicación entre redes puede darse de tres maneras diferentes: por un solo canal (medio donde se transmite la información) y en una sola dirección a la vez (*Simplex*); por un solo canal y en ambas direcciones (*Half-Duplex*), al mismo tiempo y por dos canales (*Full-Duplex*). En nuestro caso utilizaremos solamente la comunicación Full-Duplex, aunque los equipos pueden configurarse para utilizar la comunicación Half-Duplex.

En una comunicación Half-Duplex existe un solo canal que puede transmitir en los dos sentidos pero no simultáneamente, las estaciones se tienen que turnar. Esto es lo que ocurre con las emisoras de radioaficionados. (*Figura 2.3.*)

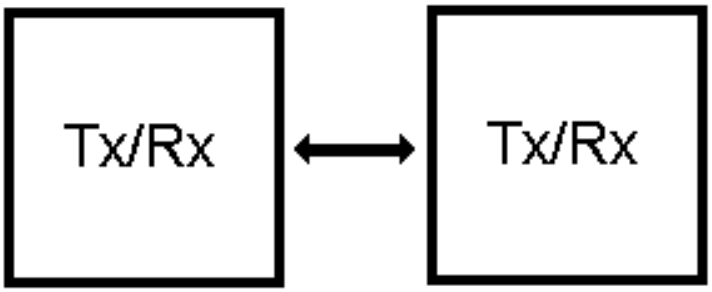

Figura 2.3. Comunicación Half-Duplex.

En una comunicación Full-Duplex existen dos canales, uno para cada sentido. Ambas estaciones pueden transmitir y recibir a la vez. Por ejemplo, el teléfono. (*Figura 2.4.*)

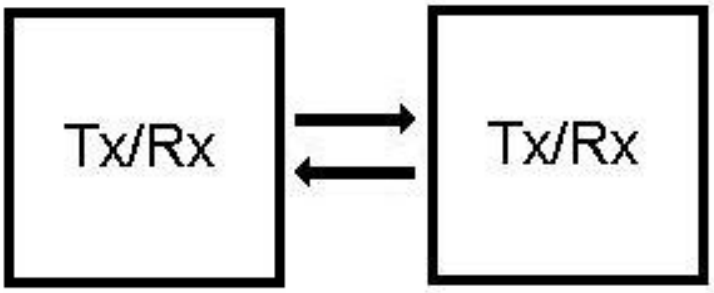

Figura 2.4. Comunicación Full-Duplex.

2.3. Modelo de Referencia OSI

El modelo de referencia *OSI (Open Systems Interconnection / Interconexión de Sistemas Abiertos)* fue un intento de la *ISO (International Standard Organization / Organización Internacional de Normas)* para la creación de un estándar que siguieran los diseñadores de nuevas redes. Se trata de un modelo teórico de referencia, únicamente explica lo que debe hacer cada componente de la red sin entrar en los detalles de la implementación.

El modelo divide a las redes en 7 capas, cada una de éstas debe tener una función bien definida y relacionarse con sus capas inmediatas, mediante interfaces también bien definidas.

En la *Figura 2.5,* se muestra el modelo OSI de 7 capas, y se definen las ventajas que tiene su uso.

- Reduce la complejidad
- Estandariza las interfaces
- Facilita el diseño modular

Figura 2.5. Modelo OSI de 7 capas, ventajas de su uso.

Capa Física

Se encarga de la transmisión de bits (un bit es un 1 o 0) a través de un medio guiado (un cable) o un medio no guiado (inalámbrico). Esta capa define, entre otros aspectos, lo que transmite cada hilo de un cable, los tipos de conectores, el voltaje que representa un 1 y el que representa un 0. La capa física será diferente dependiendo del medio de transmisión (cable de fibra óptica, cable par trenzado, enlace vía satélite, etc.) No interpreta la información que está enviando: sólo transmite 1's y 0's.

Capa de Enlace de Datos

Envía *Frames (tramas)* de datos entre hosts o routers de una misma red. Agrega secuencias de bits que envía a la capa física, escribiendo ciertos códigos al comienzo y al final de cada Frame. Esta capa fue diseñada originalmente para enlaces punto a punto, en los cuales hay que aplicar un control de flujo para el envío continuo de grandes cantidades de información. Para las redes de difusión (redes en las que muchos ordenadores comparten un mismo medio de transmisión) fue necesario diseñar la llamada subcapa *MAC (Media Access Control / Control de Acceso al Medio)* de Direccionamiento (Address), que determina el tipo de dispositivo para conectarse al medio y el tipo de Frame para comunicarse con otros dispositivos.

Posee también una subcapa *LLC (Logic Link Control / Control de Enlace Lógico)* que utiliza para comunicarse con las capas de red y con las capas superiores, y es responsable de tomar los bits de la capa física y reensamblarlos en su Frame original. Maneja la notificación de error pero no lo corrige, la topología de la red y el control de flujo, también llamado *Windowing (ventaneo de datos),* donde se define el número de

datos o Frames que pueden ser enviadas sin recibir notificación por parte del usuario final, de que la información fue bien recibida.

Capa de Red

Se encarga de encontrar el mejor camino para enviar datos de un lugar a otro dentro de la red. Maneja el envió de paquetes utilizando el direccionamiento del origen y el destino, atravesando tantas redes intermedias como sean necesarias. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente. Su misión es unificar redes heterogéneas, todos los host tendrán un identificador similar al nivel de la capa de red (en Internet son las direcciones IP) independientemente de la topología que se tenga en la capa inferior (Token Ring con cable coaxial, Ethernet con cable de fibra óptica, etc.).

Capa de Transporte

Únicamente se preocupa de la transmisión origen-destino. Podemos ver esta capa como una canalización fiable que une un proceso de un host con otro proceso de otro host. Un host puede tener varios procesos ejecutándose, por ejemplo uno para mensajería y otro para transferir archivos. No se preocupa del camino intermedio que siguen los fragmentos de los mensajes. Segmenta los paquetes, los etiqueta para que después puedan ser reensamblados en el orden correcto en que se recibieron, utiliza el control de flujo, la detección y corrección de errores en la recepción, de forma que los datos lleguen correctamente de un extremo a otro.

Capa de Sesión

Se encarga de iniciar, controlar y finalizar las comunicaciones. Además proporciona servicios mejorados a la capa de transporte como por ejemplo, la creación de puntos de sincronismo para recuperar transferencias largas fallidas.

Capa de Presentación

Esta capa provee de una representación de los datos en forma codificada y asegura que los datos que arriban desde la capa de red puedan ser utilizados por la aplicación. Codifica los datos en un sistema convenido entre emisor y receptor, con el propósito de que tanto textos como números sean interpretados correctamente. Una posibilidad es codificar los textos según la tabla *ASCII (American Standard Code for Information Interchange / Código Americano Normalizado para el Intercambio de Información)* y los números en complemento a dos.

Capa de Aplicación

Aquí se encuentran los protocolos y programas que utiliza el usuario para comunicarse en la red. Invoca programas que acceden servicios en la red. Interactúan con uno o más protocolos de transporte para enviar o recibir datos, en forma de

mensajes o bien en forma de flujos de bytes. Uno de estos protocolos es el Método de contención.

Método de Contención

Un protocolo de contención se utiliza generalmente en enlaces síncronos punto a punto para comunicarse, y es un protocolo de Intercambio Estándar, con las siguientes configuraciones de dispositivos:

- Computadora a computadora.
- Computadora a terminal de entrada remota de trabajos.
- De terminal a otra terminal.

En la *Tabla 2.1*, se muestran algunos comandos de control utilizados en este método.

Comandos de Control	Significado
ACK	Paquete de Confirmación (Datos Recibidos)
DLC	Control de Enlace de Datos
ENQ	Envío de Pregunta
EOT	Fin de Transmisión
ETB	Fin de Transmisión de Bloque
ETX	Fin de Texto
NACK	Paquete de Confirmación Negativa (Datos no Recibidos)
RTS	Envío de Solicitud de Transmisión
SOH	Indica el Principio de la Cabecera
STX	Indica el Principio de Texto
SYN	Indica Comunicación Sincronizado respecto a un Reloj

Tabla 2.1. Comandos de control para el método de contención.

Con un protocolo de contención, el enlace permanece activo sólo 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, enviando los comandos (SYN-SYN-SYN-SYN-ENQ), y espera confirmación (SYN-SYN-SYN-SYN-ACK) por parte del otro extremo y entonces puede comenzar la transferencia de datos. Si el dispositivo no recibe la confirmación durante un cierto tiempo *(Time Out / Tiempo Terminado)*, vuelve a realizar la petición.

Si sucede que los dispositivos conectados al mismo enlace realizan simultáneamente muchas peticiones, entonces ambos dispositivos ignorarán la petición del otro, pues con un protocolo Half-Duplex un dispositivo está 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 tiempo de espera, 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 un comando ACK) o confirmado negativamente (con un comando NAK) por el dispositivo receptor. Los bloques confirmados negativamente serán retransmitidos por el extremo emisor.

El comando 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. La *Figura 2.6,* muestra una operación de transferencia de datos típica utilizando un protocolo de contención.

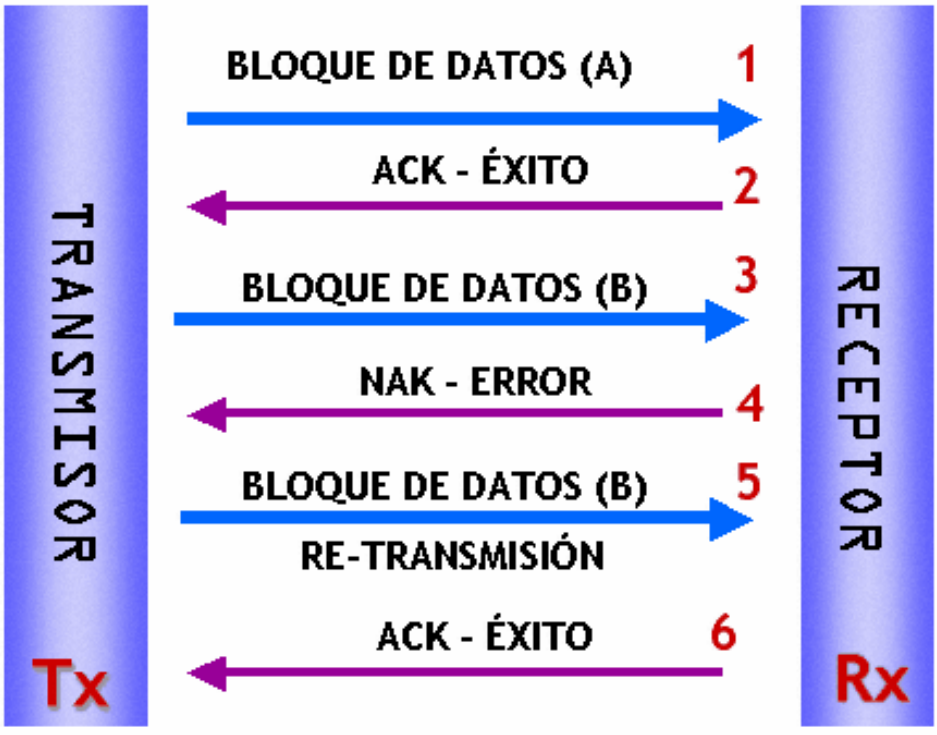

Figura 2.6. Ejemplo de Transferencia de Datos con un Protocolo de Contención.

Esta capa tendrá que ser adaptada para cada tipo de computadora, de tal forma que sea posible el envío de un correo electrónico, conexión a Internet, transferencia de archivos usando *FTP (File Transfer Protocol / Protocolo de Transferencia de Archivos)*, etc.

Métodos de Acceso

Adicionalmente a las 7 capas del sistema OSI, existen subcapas que controlan el acceso al medio, es decir, cuando dos computadoras quieren mandar información al mismo tiempo por el mismo medio, deben ponerse de acuerdo, ya que si no lo hicieran, la información de una chocaría con la de la otra. A esto se le llama colisión. Para evitar las colisiones se crearon los Métodos de Acceso. Se tienen dos métodos de acceso principalmente: CSMA/CD Y EL CSMA/CA.

CSMA/CD

El método de acceso *CSMA/CD (Carrier Sense Múltiple Access with Collision Detection / Acceso Múltiple por Detección de Portadora con Detección de Colisiones)* es utilizado en la arquitectura Ethernet.

El CSMA/CD funciona de la siguiente manera: cuando una computadora desea mandar información, primero escucha el cable de la red, para revisar que no se esté usando en ese preciso momento (detección de portadora). Esto se oye muy sencillo, pero el problema reside en que dos o más computadoras al escuchar que no se está usando el cable pueden mandar exactamente al mismo momento su información (acceso múltiple), y como solamente puede haber uno y sólo un mensaje en tránsito en el cable se produce una colisión. Entonces las computadoras detectan la colisión y deciden reenviar su información a un intervalo al azar; es importante que sea al azar, ya que si ambas computadoras tuvieran el mismo intervalo fijo se produciría un ciclo vicioso de colisiones y reenvíos (detección de colisiones). Así, por ejemplo, al detectar la colisión una computadora se espera tres milisegundos y la otra cinco milisegundos, siendo obvio que una computadora reenviará en primer lugar y la otra esperará a que el cable esté de nuevo sin tránsito.

Evidentemente que en una misma red Ethernet, al haber muchas computadoras tratando de enviar datos al mismo tiempo y/o al haber una transferencia masiva de datos, se crea un gran porcentaje de colisiones y utilización. Si se pasa del 1% de colisiones, y/o 15% de utilización de cable, ya se dice que la red está saturada. Además, las señales de este tipo de red tienden a degradarse con la distancia debido a la resistencia, la capacidad u otros factores. Inclusive la señal todavía se puede distorsionar por las interferencias eléctricas exteriores generadas por los motores, las luces fluorescentes y otros dispositivos eléctricos. Cuanto más se aumenta la velocidad de transmisión de los datos, más susceptible es la señal a degradarse. Por esta razón, las normas de Ethernet especifican los tipos de cables, los protectores y las distancias del mismo, la velocidad de transmisión y otros detalles para trabajar y proporcionar un servicio relativamente libre de errores en la mayoría de los entornos.

CSMA/CA

La norma IEEE 802.11 especifica el denominado *CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance / Acceso Múltiple por Detección de Portadora con Anulación de Colisiones)*.

Según este método, una computadora que está preparada para transmitir información, debe sensar el medio antes de hacerlo. Si se determina que el medio está libre, la computadora puede empezar el proceso de transmisión. Si por el contrario, el medio se determina ocupado, la estación espera un tiempo aleatorio, antes de volver a intentar la transmisión. El tiempo aleatorio es seleccionado de manera uniforme en un intervalo definido por los valores 0 y *CW (Contest Window /Ventana de Contienda)*. El parámetro CW varía en función del número de intentos que contabiliza una computadora para la transmisión de un paquete determinado.

Encapsulado de los Datos

Los paquetes de datos de cada capa suelen recibir nombres distintos. En la Capa Física se denominan **Bits**, en la Capa de Enlace de Datos se habla de **Frames**; en la Capa de Red de **Packets (Paquetes) o Datagramas**, en la Capa de Transporte se utiliza el término **Segmento**, y por ultimo en las Capas superiores formadas por la Capa de Sesión, Presentación y Aplicación se maneja el nombre de **Datos**. Para que cada Paquete reciba este nombre pasa por un proceso denominado encapsulado. Este proceso en los datos tiene la siguiente secuencia:

1. **Dato:** La información del usuario contenida en las Capas superiores 7, 6 y 5 es convertida en Datos y es enviada a la Capa 4.

2. **Segmento:** En esta Capa los Datos son convertidos en Segmentos y se les asigna un identificador (TCP) para pasarlos a la Capa 3.

3. **Paquete:** La Capa 3 recibe los Segmentos y los transforma en Paquetes o Datagramas, anexándoles un *Encabezado* (*Header*, IP) y los pasa a la Capa 2.

4. **Frame:** En esta Capa al Paquete recibido se le anexa un Header al inicio (LH) y un *Delimitador* (*Trailer*, LT) al final construyendo un Frame. A la estructura formada por: Header–Dato–Trailer (Control de datos cuando se encapsulan para su transmisión) se le conoce como encapsulado y es enviada a la capa 1.

5. **Bits:** El Frame recibido de la capa 2 se convierte en una serie de 1’s y 0’s, los cuales son enviados al medio de Transmisión.

En la *Figura 2.7,* se muestra el proceso de encapsulado descrito anteriormente.

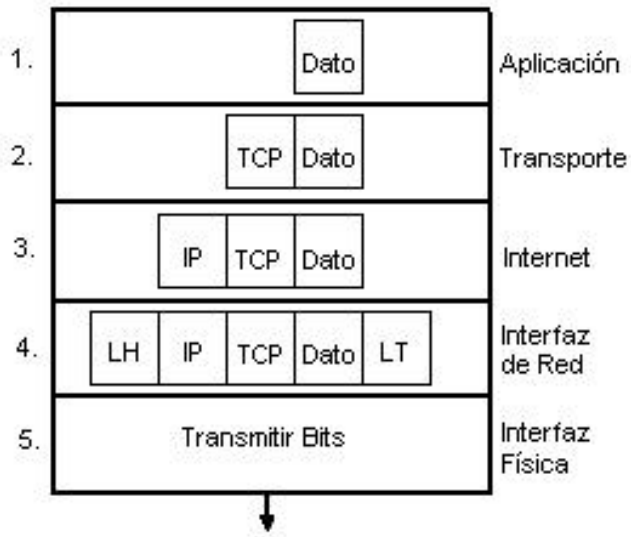

Figura 2.7. Encapsulado de Datos.

2.4. Topologías de Red

La topología de una red es el arreglo físico en el cual los dispositivos de la red, como son las computadoras, las impresoras, los servidores, los hubs, los switches, los bridges, etc., se interconectan entre sí, sobre un medio de comunicación.

Existen varias topologías de red básicas (bus, estrella, anillo y malla), pero también existen redes híbridas que combinan una o más topologías en un mismo arreglo. Para nuestro caso utilizaremos una red híbrida de bus, estrella y anillo, que puede ser comúnmente empleada en una Arquitectura Ethernet, Token Ring, etc.

2.4.1. Topología de bus

Una topología de bus está caracterizada por un cable principal con dispositivos de red interconectados a lo largo del mismo por medio de conectores. Las redes de bus son consideradas como topologías pasivas (en donde las computadoras sólo escuchan el tráfico en el medio de comunicación). Cuando están listas para transmitir, se aseguran que no haya nadie más transmitiendo en el bus y entonces envían sus paquetes de información. Las redes de bus están basadas en la contención, esto significa que cada computadora debe contender por un tiempo de transmisión. Típicamente emplean la arquitectura de red Ethernet.

Las redes de bus generalmente utilizan cable coaxial como medio de comunicación, las computadoras se conectan al bus mediante un conector *BNC (British Network Conector / Conector Británico para Red)* en forma de T. Y en cada extremo de la red se pone un terminador (si se utiliza un cable de 50 ohms, se debe poner un terminador de 50 ohms.). En la *Figura 2.8,* se pueden observar diferentes tipos de Conectores.

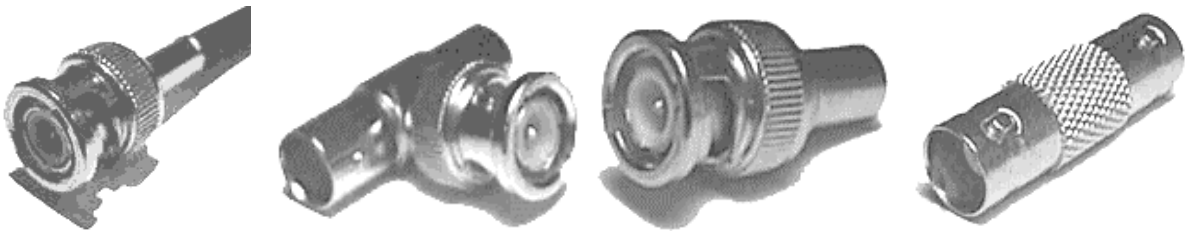

Figura 2.8. BNC, T, Terminador y de Unión respectivamente.

Las redes de bus son fáciles de instalar y de extender, pero son muy susceptibles a quebraduras, cortos en el cable y fallas de los conectores. Un problema físico en la red, tal como un conector T averiado, puede dejar inoperable toda la red. La *Figura 2.9,* muestra esta topología.

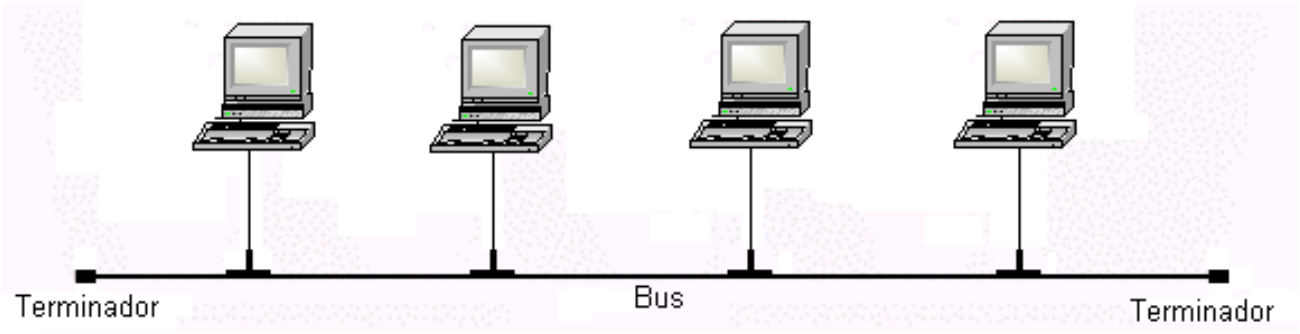

Figura 2.9. Topología de Bus.

2.4.2. Topología de Estrella

En una topología de estrella, las computadoras en la red se conectan a un dispositivo central conocido como hub o a un conmutador de paquetes conocido como switch. Cada computadora se conecta con su propio cable (Generalmente par trenzado con un RJ-45, véase Apéndice A) que se muestra en la *Figura 2.10,* a un puerto del hub o del switch como los que aparecen en la *Figura 2.11,* este tipo de red sigue siendo pasivo, y también utiliza el método de contención.

Figura 2.10. Cable de par trenzado y un conector RJ-45.

Figura 2.11. Ejemplos de Hubs y Switches Cisco respectivamente.

Debido a que la topología estrella utiliza un cable de conexión para cada computadora, es muy fácil de expandir, sólo dependerá del número de puertos disponibles en el hub o switch, aunque se pueden conectar hubs o switches en cadena para así incrementar el número de puertos. La desventaja de esta topología es la centralización de la comunicación, ya que si el hub o switch falla, también fallará toda la red. Esta topología se muestra en la *Figura 2.12.*

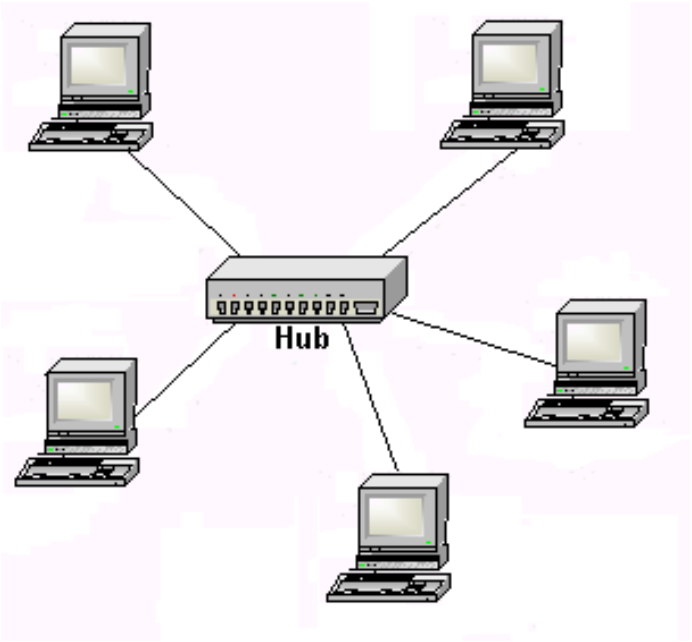

Figura 2.12. Topología de Estrella.

2.4.3. Topología de anillo

Una topología de anillo conecta a las computadoras una tras otra sobre el cable en un círculo físico. El acceso al medio de la red es otorgado a una computadora en particular por medio de pequeños formatos de Frames llamados Token. Esta topología mueve información sobre el cable en una dirección y es considerada como una topología activa (se va pasando el Token o estafeta de una a otra, y todas participan, actualizando al Token). Las computadoras en la red retransmiten a la siguiente computadora los paquetes que reciben.

El Token circula alrededor del anillo y cuando una computadora desea enviar datos (origen), espera al Token y se posesiona de él. La computadora entonces envía los datos sobre el cable. La computadora destino envía un mensaje a la computadora origen para indicar que fueron recibidos correctamente. La computadora origen crea un nuevo Token y los envía a la siguiente computadora, empezando el ritual de paso de Token (Token Passing) nuevamente. *La Figura 2.13,* muestra la topología de anillo.

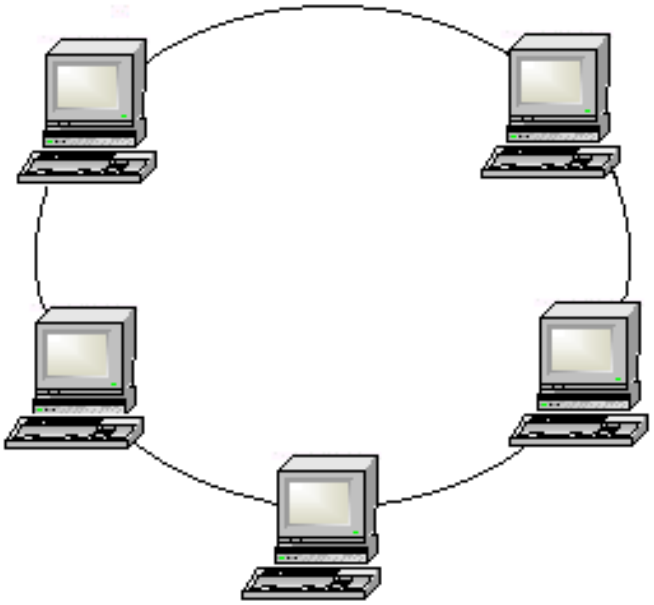

Figura 2.13. Topología de Anillo.

2.5. Redes LAN, MAN y WAN

Las redes de acuerdo a la cobertura geográfica pueden ser clasificadas en LANs, MANs, y WANs.

2.5.1. Redes de Área Local

Una LAN conecta varios dispositivos de red en una área de corta distancia (decenas de metros), delimitadas únicamente por la distancia de propagación del medio de transmisión: coaxial (hasta 500 metros), par trenzado (hasta 90 metros) ó fibra óptica (Ver Apéndice A), espectro disperso e infrarrojo (decenas de metros).

Una LAN podría estar delimitada también por el espacio en un edificio, un salón, una oficina u hogar, pero a su vez podría haber varias LANs en estos mismos espacios. Estas redes se basan en el protocolo TCP/IP, también se puede concebir una LAN como una subred.

Las LANs comúnmente utilizan las arquitecturas Ethernet, Token Ring, *FDDI (Fiber Distributed Data Interface / Interfaz de Datos Distribuidos en Fibra)* para

conectividad, así como protocolos tales como AppleTalk, Banyan Vines, *DECnet (Digital Equipment Corporation Net / Red de la Corporación de Equipo Digital),* IPX, etc.

2.5.2. Redes de Área Metropolitana

Una Red *MAN (Metropolitan Area Network / Red de Área Metropolitana)* es una colección de LANs dispersas en una ciudad (decenas de kilómetros). Una MAN utiliza tecnologías tales como *ATM (Asynchronous Transfer Mode / Modo de Transferencia Asíncrona)*, *Frame Relay (Retransmisión de Frames), xDSL (Digital Subscriber Line / Línea de Suscripción Digital), WDM (Wavelength Division Modulation / Modulación por División de Longitud de Onda)*, y herramientas *ISDN (Integrated Services Digital Network / Red Digital de Servicios Integrados)*, *E1* (Banda Ancha que permite la transmisión de datos a 2.048 Mbps), *T1* (Línea Arrendada con la compañía telefónica que permite la transmisión de datos a 1.544 Mbps), *PPP (Point to Point Protocol / Protocolo de Punto a Punto)*, etc., para conectividad a través de medios de comunicación tales como cobre, fibra óptica, y microondas.

2.5.3. Redes de Área Amplia

Una *WAN (Wide Area Network / Red de Área Amplia)* es una colección de LANs distantes geográficamente en cientos de kilómetros una de otra. Un dispositivo de red llamado router es capaz de conectar LANs a una WAN.

El propósito de una conexión WAN es la transmisión de datos entre dos redes distantes, tan eficientemente como sea posible el enlace WAN es típicamente más lento que el enlace LAN.

Existen diferentes protocolos para proveer la conexión serial entre dos redes; uno de ellos es el protocolo *SLIP (Serial Line Internet Protocol / Protocolo de Internet con Línea Serial)*, esté protocolo permite la conexión entre una red y un nodo remoto.

El protocolo PPP es la siguiente generación del SLIP, pero trabaja en la capa física y enlace de datos. PPP incluye mejoras como son encripción, control de errores, seguridad, y direccionamiento IP dinámico. PPP, además de utilizar el Frame de datos, utiliza otros tipos de Frame como son: *LCP (Link Control Protocol / Protocolo de Control del Enlace)* que es utilizado para establecer y configurar la conexión, y *NCP (Network Control Protocol / Protocolo de Control de Red)* que se utiliza para seleccionar y configurar los protocolos en la capa de Red.

Las WAN utilizan comúnmente tecnologías ATM, Frame Relay, X.25, E1/T1, *GSMC (Global System for Mobile Communications / Sistema Global para Comunicaciones Móviles), TDMA (Time Division Multiplex Access / Acceso Múltiple por División de Tiempo), CDMA*, xDSL, PPP, etc., para conectividad a través de medios de comunicación tales como fibra óptica, microondas, celular y vía satélite.

2.6. Redes de Alta Velocidad

En los últimos años han cobrado gran importancia las redes de alta velocidad, lo mismo que su utilización, principalmente en los sistemas distribuidos locales y metropolitanos, así como los mecanismos a través de los cuales se puede garantizar la calidad del servicio que se entrega a través de las redes de computadoras (Por Ej. ATM).

2.6.1. Frame Relay

Frame Relay es un protocolo de redes WAN que trabaja en la capa Física y en la capa de Enlace de Datos del modelo OSI. Es una red de acceso múltiple, lo cual significa que más de dos mecanismos se pueden conectar a la misma red.

Una de las características de Frame Relay es que envía Frames de tamaño variable entre dispositivos conectados a la misma red. Utiliza el concepto de *Paquetes Conmutados (Paket Switching)* y de banda compartida, es decir que todos los dispositivos conectados a la misma línea arrendada comparten su ancho de banda.

Frame Relay utiliza la conexión orientada, lo que implica que debe existir un reconocimiento previo entre emisor y receptor antes de enviar la información.

En la *Figura 2.14,* se muestran algunos conceptos de conectividad utilizados para Frame Relay , donde la línea arrendada conecta al router (también llamado *DTE (Data Terminal Equipment / Equipo Terminal de Datos)* o R1, R2, etc.) con el switch (llamado *DCE (Data Communications Equipment / Equipo de Comunicación de Datos)*) más cercano. A dicha conexión se le llama *Enlace de Acceso (Access Link)*. Se utiliza el protocolo *LMl (Local Management Interface / Interfaz de Administración Local)* entre el router y el switch. El protocolo LMI es usado para asegurar que dicho enlace trabaje correctamente.

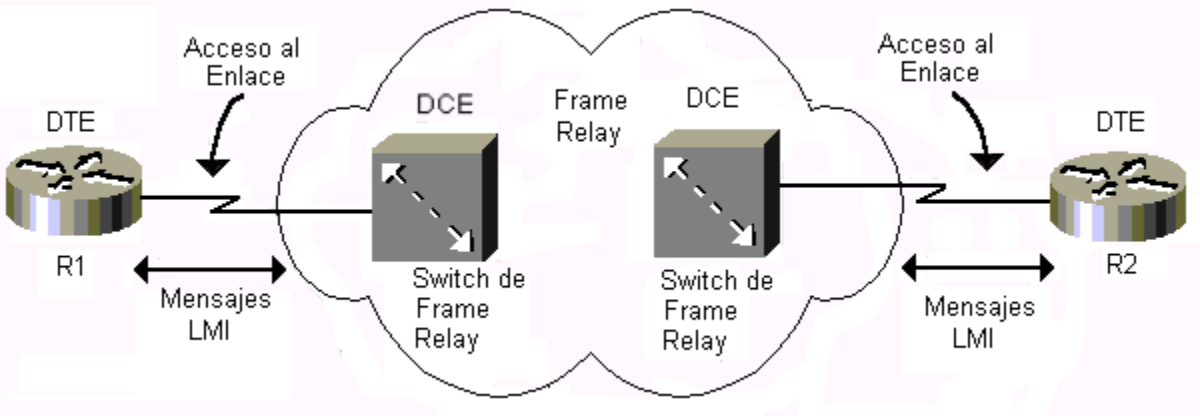

Figura 2.14. Componentes Básicos de una Red de Frame Relay.

El camino lógico entre un par de routers (DTEs) es llamado *VC (Virtual Circuit / Circuito Virtual)*, el cual se representa con tres líneas paralelas como se muestra en la *Figura 2.15.*

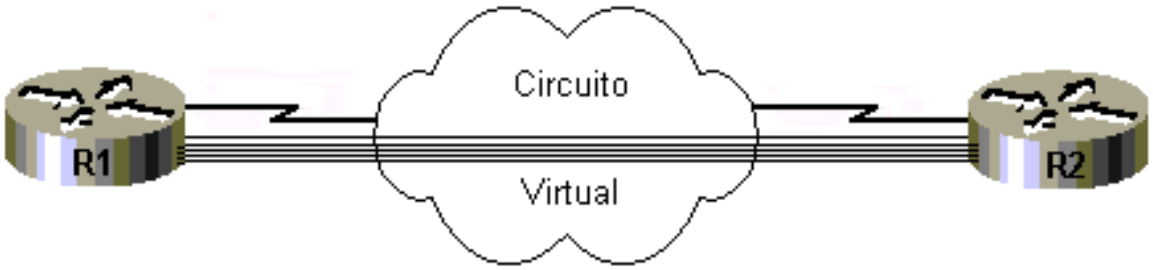

Figura 2.15. Conexiones Lógicas asociadas a un Circuito Virtual.

Comúnmente el proveedor de servicio configura previamente todos los detalles requeridos de un VC. A estas configuraciones de VCs se les llama *PVCs (Permanent Virtual Circuits / Circuitos Virtuales Permanentes)* a diferencia de los *SVCs (Switched Virtual Circuits / Circuitos Virtuales Conmutados)*, los cuales se actualizan dinámicamente cuando se necesita y es semejante a tener una conexión por modem.

Una red Frame Relay se comunica entre sí utilizando *FRADs (Frame Relay Access Devices / Mecanismos de Acceso para Transmisión de Tramas)* y *FRS (Frame Relay Switches / Conmutadores de Transmisión de Tramas)*, los cuales son conectados por medio de enlaces físicos tales como *DS0 (Digital Signal Level 0 / Especificación de Transmisión Digital sobre un Canal Simple de 64 kbps)*, T1 o E1.

Los FRADs son los dispositivos terminales, encargados de la conexión entre una LAN y una WAN de Frame Relay, utilizando los diferentes switches (FRS) de la red. Los switches FRS son los que realizan todo el ruteo de la información a través de la red.

Una característica primordial de Frame Relay es que no existe garantía de que los paquetes de datos lleguen a su destino correctamente. Los protocolos de transporte son los encargados de la detección y corrección de errores únicamente en los nodos terminales. Los switches únicamente dejan pasar la información. Esto es así, ya que Frame Relay supone que los enlaces físicos tienen un nivel muy bajo de error, de esta forma la comunicación es mucho más rápida.

El protocolo *LAPD (Link Access Procedure on the D Channel / Procedimiento de Acceso al Enlace en el Canal de Señalización D)* en Frame Relay, únicamente realizará la tarea de fragmentación y múltiplexaje de VCs, así como la detección de errores utilizando el método de *CRC (Cyclic Redundancy Check / Verificación de Redundancia Cíclica)*.

Si existe un error en la transmisión detectado por el CRC, el Frame es descartado automáticamente, sin aviso a ningún otro dispositivo de tal evento.

2.6.2. Redes basadas en X.25

Diversas tecnologías pueden ser empleadas para permitir un enlace de red WAN. X.25 es una de ellas, aunque la tendencia actual es más en enlaces como Frame Relay. X.25 se menciona ya que sirve como base para éste.

X.25 es una red para la transmisión de datos a grandes distancias. X.25 define la forma de conexión de equipos DTE, DCE y *PSE (Packet Switching Exchanges, Intercambio de Conmutación de Paquetes)* o simplemente switches.

X.25 es un protocolo que cubre las tres primeras capas del modelo de referencia OSI (Física, Enlace de Datos y Red), usa PVCs y SVC al igual que Frame Relay con velocidades de 9.6 a 256 kbps, utiliza Frames de tamaño variable como resultado de revisar los errores y retransmitir datos, su velocidad es considerada lenta, utiliza la conexión PPP entre DTE y DCE definiendo el formato de los paquetes e intercambio de mismos.

Los enlaces en X.25 son desarrollados utilizando PVCs, la cual es una conexión lógica permanente entre DTEs o SVCs, ambos se identifican por medio de un *LCN (Logical Channel Number / Número de Canal Lógico)*, el cual tiene definición local por cada nodo en la red X.25.

El PVC es solicitado por medio de un contrato previo sin la necesaria inicialización de llamadas, mientras que los SVC son requeridos mediante peticiones e inicializaciones.

2.6.3. Red Digital de Servicios Integrados

La Red Digital de Servicios Integrados (*RDSI*, o bien *Integrated Services Digital Network (ISDN)*) es un concepto ligado al de una red totalmente digital que, utilizando unos estándares universales de acceso, permite la conexión de una amplia gama de terminales como teléfonos, ordenadores, centrales *PBX (Private Branch Exchanges / Intercambios en un Rama Privada)*, etc., a los que la red proporciona una gran variedad de servicios entre los que se incluyen voz, datos e imágenes.

También podría considerarse la terna "voz, datos e imágenes" como poco significativa (a pesar de haberse convertido en un tópico), ya que al tratarse de una red digital de paquetes y de circuitos de *Banda Estrecha (BE)* poco importa el origen de la información codificada, como lo ilustra la *Figura 2.16.*

Es decir, la RDSI se presenta como la bandera de la *Red Digital Integrada (RDI),* aunque su oferta es diferente:

- Audio de 7 kHz de ancho de banda, en vez de los 3.1 kHz de la red telefónica actual.
- Canales digitales de 64 kbps de velocidad, en vez de las que se alcanzan utilizando módems, que difícilmente llegan a los 40 kbps.

- Mayor funcionalidad y servicios gracias al canal común de señalización.
- Un único y estandarizado método de acceso que da paso a toda una red de área extensa, con posibilidad de transferir información tanto en modo circuito como en modo paquete.

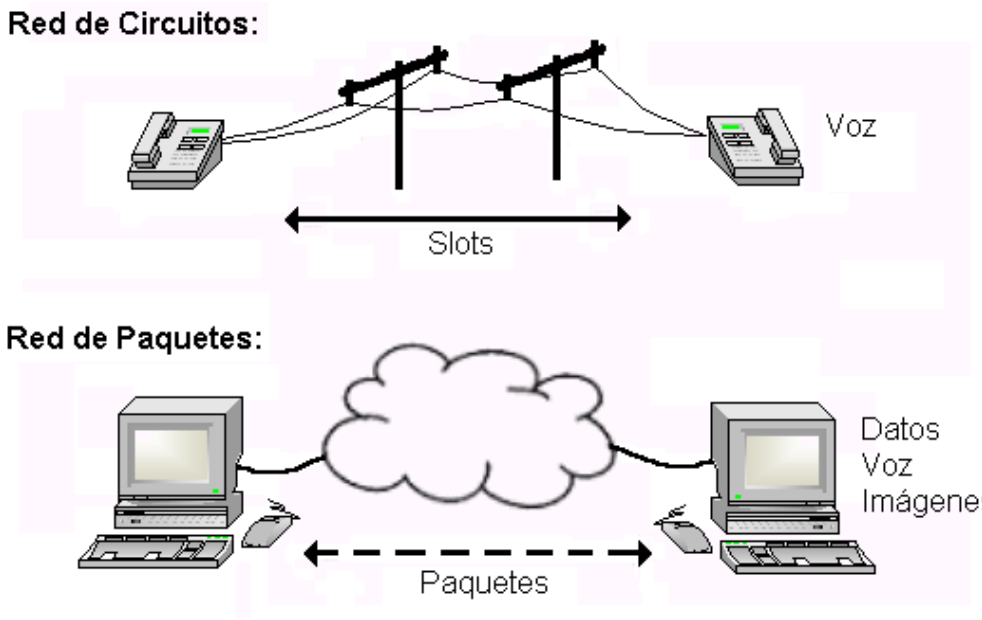

Figura. 2.16. Esquema de la RDSI-BE.

La RDSI de Banda Estrecha (RDSI-BE)

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

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

Es evidente que no existe una red universal donde podamos conectar indistintamente el teléfono, las terminales *X.25*, ni por supuesto un receptor de TV. Cada uno de estos dispositivos requiere un tipo específico de servicio, contratado, instalado y gestionado por separado. La RDSI pretende ser la gran integradora de los servicios que hasta ahora proporcionaban las compañías telefónicas; desde la red conmutada para voz, redes de paquetes, hasta los enlaces digitales punto a punto, pasando por la mayoría de redes especializadas en dar un solo servicio. La integración de las LAN y circuitos de TV quedan como objetivo para una futura RDSI en banda ancha. En principio, la RDSI convivirá y permitirá la conectividad con el resto de redes

públicas, aunque éstas progresivamente irán siendo integradas o sustituidas por la RDSI hasta llegar a constituirse en red única.

Para permitir la interconexión de las terminales actuales, que no soportan de forma nativa protocolos RDSI, se han diseñado los denominados *TA (Adapters of Terminal / Adaptadores de Terminal)*. Los TA garantizan de esta forma la conexión de la mayoría de recursos de comunicaciones existentes sin necesidad de cambios notables.

Configuración de Referencia para RDSI-BE

La configuración de referencia del acceso usuario-red está basada en dos elementos:

a) Grupos funcionales o TAs.
b) Puntos de referencia o interfaces de comunicación de los TAs.

Grupos funcionales

Se llaman grupos porque no intentan describir un TA específico, sino un conjunto genérico de equipos con sus funciones y responsabilidades, como se muestra en la *Figura 2.17.*

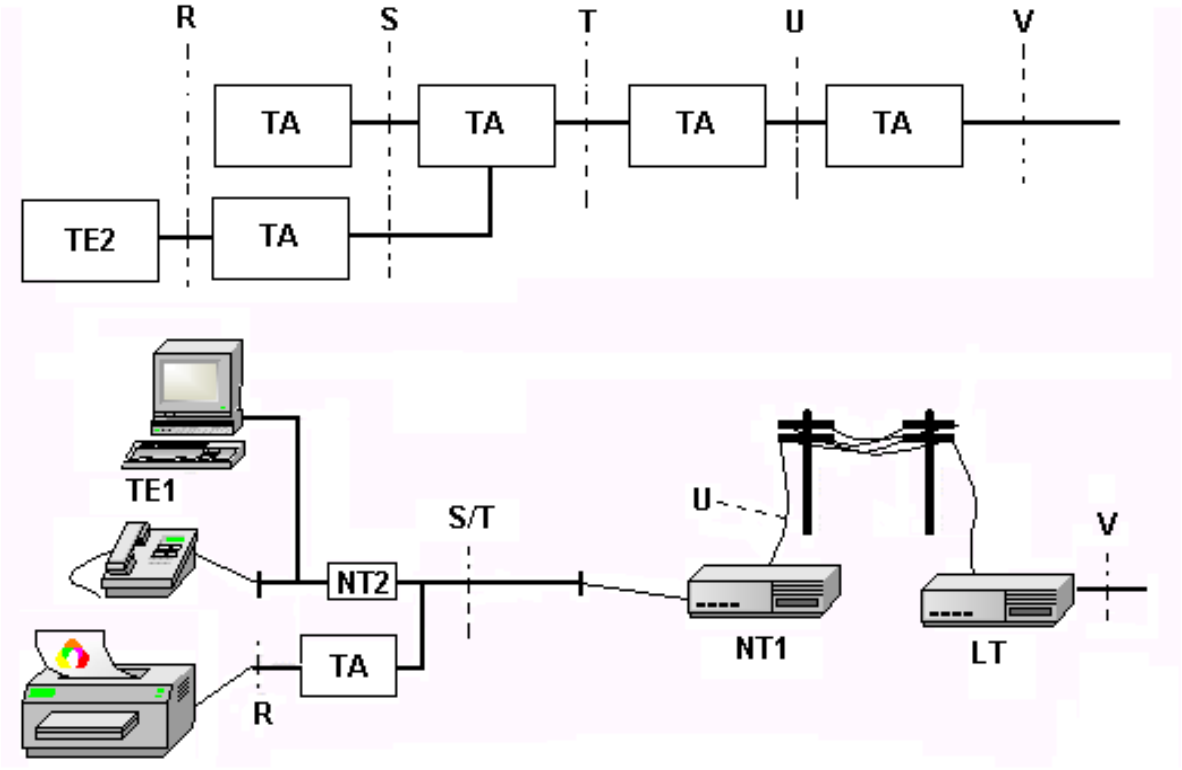

Figura. 2.17. Modelo genérico de configuración RDSI.

Las características correspondientes a cada grupo son:

- **NT1:** Terminación de Red 1. Localizado en casa del abonado, es el responsable de ejecutar funciones de bajo nivel. Presenta el final de la conexión física que supervisa el acceso a la red.
- **NT2:** Terminación de Red 2. Equipo de usuario que realiza las funciones de adaptación a los distintos medios físicos, así como de la señalización y multiplexaje del tráfico. Por ejemplo, una central PBX.
- **TE1:** Equipos Terminales 1. Son periféricos que integran de forma nativa los protocolos RDSI y pueden conectarse directamente a la interfaz *S* y *T*. Por ejemplo, un teléfono digital o una tarjeta adaptadora para PC.
- **TE2:** Equipos Terminales 2. Son aquellos periféricos que utilizan las actuales interfaces y protocolos no-RDSI. Precisan de un TA para poder acceder a la red. Por ejemplo, un teléfono analógico tradicional.
- **LT:** Terminación de línea. Su función es simétrica a la del NT1 pero localizado al lado de la central.
- **TA:** Adaptador de Terminal. Permiten la conexión de los TE1 a la RDSI actuando como conversor de protocolos *V.24* o *X.21* en la señalización RDSI.

Puntos de referencia

Los Puntos de referencia son las interfaces de comunicación entre los grupos funcionales. En la *Figura 2.17*. También se muestran los principales puntos de referencia, cuyas características son:

- **R:** Son todos los protocolos no-RDSI, como *V.24* o *X.21*, los que pueden ser incluidos en este apartado. Precisan adaptadores de terminal para conectarse.
- **S:** *Subscriber*, es el punto de acceso universal a la red para los terminales con RDSI nativo. Puede coincidir o incluir al punto *T.*
- **T:** Interfaz entre NT1 y NT2. Separa el bucle de abonado de la instalación propia del usuario.
- **U:** Interfaz entre LT y NT1 que las une.
- **V:** Interfaz dentro de la central. Pertenece a la implementación propia de la compañía operadora.

Canales RDSI

Se denomina canal, al medio a través del cual fluye la información y que es utilizado por los abonados para interactuar con otros usuarios. Hay definidos tres tipos de canales según su capacidad y funcionalidad.

Canal B: Es el canal básico del usuario. Transporta la información entre usuarios (datos digitales, voz digital codificada PCM, etc.) generalmente a 64 kbps (56 kbps en EE.UU.). En un canal B se pueden establecer cuatro tipos de conexiones:

- **Circuito conmutado:** El usuario realiza una llamada y se establece una conexión de circuito conmutado con otro usuario de la red

- **Paquetes conmutados:** El usuario se conecta a un nodo de conmutación de paquetes, intercambiando los datos con los demás usuarios vía X.25.

- **Modo de Frame:** El usuario se conecta a un nodo de retransmisión de Frames y los datos se intercambian con otros usuarios.

- **Semipermanente:** Es una conexión con otro usuario establecida anteriormente, y que no requiere un protocolo para iniciar una nueva llamada.

Canal D: Transporta la información de señalización entre el usuario y la red, que sirve para controlar las llamadas de circuitos conmutados asociadas a los canales B. Dependiendo de la configuración pueden tener una velocidad de 16 o 64 kbps.

Canal H: Usados para información de usuario a alta velocidad. Tienen por tanto la misma funcionalidad que los canales B, de hecho son agrupaciones de canales B con lo que conseguimos velocidades múltiplos de 64 kbps: 384 kbps (H), 1536 kbps (H1) y 1920 kbps (H2).

Ya hemos mencionado que el acceso a los servicios de la red se consigue a través del canal D (canal de señalización), mientras que los datos se transportan a través de los canales B. Todos ellos son: digitales, Full-Duplex e independientes entre sí.

Los tipos de canales mencionados se agrupan en estructuras de transmisión que se ofrecen como paquetes al usuario. En la *Figura 2.18*, podemos distinguir dos tipos de estructuras.

Aquí es descrita cada estructura:

- **Estructura de canal básico (Acceso básico):** consiste en dos canales B de 64 kbps y un canal D de 16 kbps. Es una configuración para entornos con bajo volumen de tráfico, y que puede satisfacer las necesidades de la mayoría de usuarios individuales, viviendas y pequeñas oficinas.
- **Estructura de canal primario (Acceso primario):** Destinado a entornos con alto volumen de tráfico, como oficinas con PBX digitales, LAN o bases de datos. En Europa proporciona 30 canales B de 64 kbps y un canal D de 64 kbps consiguiendo una capacidad de 2,048 Mbps. En EE.UU., en cambio, proporciona 23 canales B de 64 kbps y un canal D de 64 kbps para una velocidad de 1,544 Mbps.

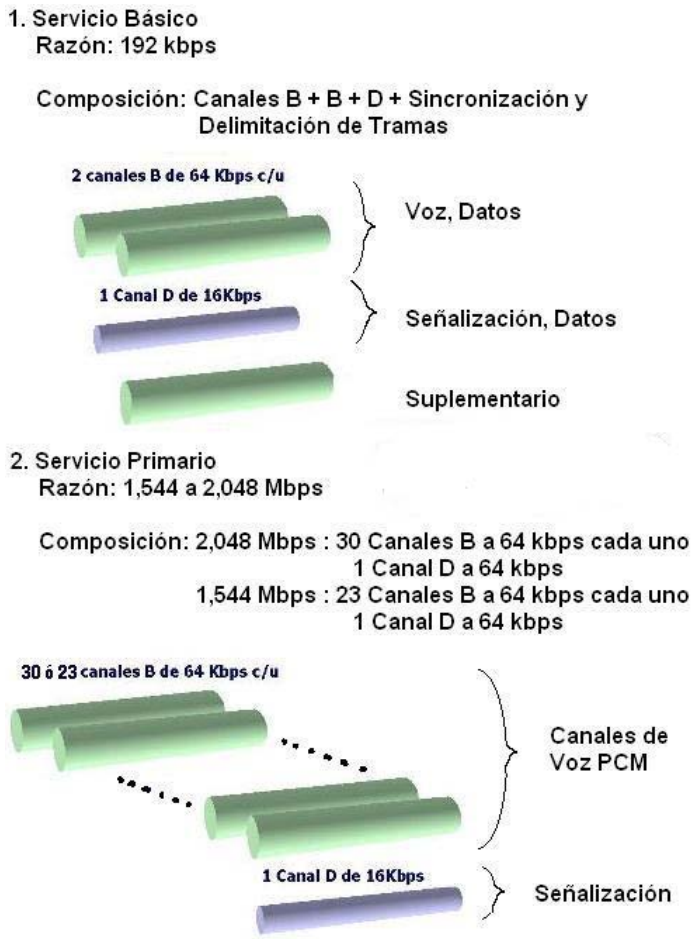

Figura 2.18. Estructuras del Servicio Básico y del Servicio Primario.

Para usuarios con menos requerimientos, se pueden usar menos canales B, proporcionando accesos no estandarizados (D, B+D, 6B+D, etc.).

También existen estructuras que incluyen **canales H**:

- **Estructura del canal H con interfaz de velocidad primaria:** Admite canales H a 384 kbps. Para 1,544 Mbps se usan las estructuras 3H+D y 4H, mientras que para 2,048 Mbps se usa la estructura 5H+D.
- **Estructura del canal H1 con interfaz de velocidad primaria:** La estructura del canal H1 consiste de un canal a 1536 kbps. La estructura del canal H2 consiste de un canal a 1920 kbps y un canal D a 64 kbps.
- **Estructuras con interfaz de velocidad primaria para mezcla de canales B y H:** Consta de uno ó ningún canal D más una combinación de canales B y H (3H+5B+D, 3H+6B, etc.).

Cuando en una estructura no hay ningún **canal D**, se supone que otro **canal D**, en otra interfaz primaria, en la misma posición de abonado, proporcionará cualquier señalización necesaria.

2.6.4. Modo de Transferencia Asíncrono

El manejo de Frames de longitud variable puede causar errores, además de que los dispositivos deben conocer el tamaño del Frame que llega antes de poder transmitirlo, provocando retraso de transmisión debido a los diferentes switches, generando así, retraso en toda la red.

ATM es la tecnología que se apoya en el método *Cell-Relay (Transmisión de Celdas)* para la transmisión de la información en forma de celdas de tamaño fijo, generando así, velocidades mayores de propagación.

Es una tecnología de transmisión de información, que puede estar montada sobre cable *UTP (Unshielded Twister Pair / Par Trenzado Sin Blindaje*) ver Apéndice A, enlaces E1, E3 (Banda ancha que permite la transmitir de datos a 34.368 Mbps) o en Fibra Óptica (ver Apéndice A).

Las celdas de ATM están formadas por 53 bytes de longitud fija, donde 48 bytes son usados para la información y 5 para el Header que indica la dirección destino.

Con este formato en Celdas de ATM se tendrá mayor velocidad de conmutación, el cual puede ser utilizado no únicamente para la transmisión de datos, sino de voz y video en tiempo real, permitiendo así el uso por ejemplo de videoconferencia.

Tanto ATM como Frame Relay, parten de la suposición de que los enlaces físicos son 100% confiables, por lo cual no tienen métodos de corrección de errores.

ATM se basa en los términos *UNI (User-Network Interface / Interfaz de Red-Usuario)* y *NNI (Network-Network Interface / Interfaz de Red-Red)* para definir el tipo de comunicación, si es entre interfaz y usuario-red ó entre interfaz y red-red respectivamente.

2.7. Protocolos de Comunicaciones

Un protocolo es un conjunto de reglas de comunicaciones entre dispositivos (computadoras, teléfonos, routers, switches, etc). Los protocolos gobiernan el formato, sincronización, secuencia y control de errores. Sin estas reglas, los dispositivos no podrían detectar la llegada de bits.

Pero los protocolos van más allá que sólo una comunicación básica. Suponiendo que se desea enviar un archivo de una computadora a otra. Se podría enviar todo el archivo de una sola vez, pero quién podría detener a los demás usuarios que están usando la LAN durante el tiempo que toma enviar dicho archivo. Adicionalmente, si un error ocurre durante la transmisión, todo el archivo tendría que enviarse de nuevo. Para resolver estos problemas, el archivo es partido en piezas pequeñas llamados paquetes agrupados de cierta manera. Esto significa que cierta información debe ser agregada al paquete para decirle al receptor donde pertenece cada grupo en relación con los otros.

Para mejorar la confiabilidad de la información, el paquete debe ser sincronizado y corregido. A la información útil (es decir el mensaje), junto con la información adicional se le conoce como protocolo.

Debido a su complejidad, la comunicación entre dispositivos es separada en pasos. Cada paso tiene sus propias reglas de operación y, consecuentemente, su propio protocolo. Esos pasos deben de ejecutarse en un cierto orden, de arriba hacia abajo en la transmisión y de abajo hacia arriba en la recepción. Debido al arreglo jerárquico de los protocolos, el término pila de protocolos (Protocol Stack) es comúnmente usado para describir esos pasos. Una pila de protocolos, por lo tanto, es un conjunto de reglas de comunicación, y cada paso en la secuencias tiene su propio subconjunto de reglas.

Existen dos tipos de protocolos de comunicación definidos como:

- **Protocolos de Ruteo (Routed Protocol)**. Son usados en los nodos para encapsular los datos en paquetes dentro de la capa de red, direccionando la información para que pueda transmitirse a través de la red. Apple Talk (protocolo de comunicación diseñado por Apple Computer), IP e *IPX (Internetwork Packet Exchange / Intercambio de Paquetes en la Internet)* son protocolos de ruteo. Cuando un protocolo no soporta una dirección en el nivel de red, entonces se trata de un protocolo de enrutamiento.

- **Protocolos de Enrutamiento (Routing Protocol):** Son los que usan los routers para construir y mantener las tablas de enrutamiento y enviar los paquetes de datos por la mejor ruta hacia sus redes destino. Los protocolos de enrutamiento permiten a los routers aprender sobre el estado de las redes que no están conectadas directamente a ellos. Esta comunicación se lleva a cabo continuamente, permitiendo que la información en la tabla de asignación sea actualizada con cada cambio que ocurra en la red.

2.8. Direccionamiento IP

Este protocolo utiliza direcciones de IP para identificar los host y direccionar los datos hacia ellos. Todos los host deben tener una dirección de IP única para las comunicaciones. El nombre de host se traduce a su dirección consultándolo en una base de datos de pares nombre-dirección.

Cuando se diseñaron las direcciones de IP, nadie había soñado que llegase a haber millones de computadoras en el mundo y que muchas de ellas necesitasen una dirección IP. Los diseñadores pensaron que tenían que satisfacer las necesidades de una modesta Comunidad de Universidades, Grupos de Investigación, Organizaciones del Gobierno y Militares. Eligieron un diseño que les parecía razonable para ese momento. Una dirección de IP es un número binario de 32 bits (4 octetos). Claramente, la dirección se eligió para que encajase convenientemente en un registro de 32 bits de una computadora.

La notación punto se inventó para leer y escribir fácilmente las direcciones de IP. Cada octeto (8 bits) de una dirección se convierte a su número decimal, y los números se separan por puntos. Por ejemplo, la dirección de ***blintz.med.yale.edu*** es un número binario de 32 bits que en la notación punto es:

10000010 10000100 00010011 00000001
130.132.19.31

El mayor número que puede aparecer en una posición corresponde al número binario 1 1 1 1 1 1 1 1 es el 255.

2.8.1. Formatos de Direcciones

Una dirección de IP tiene un formato de dos partes que son la dirección de red y la dirección local. (*Figura 2.19.*). La dirección de red identifica la red a la que está conectado el nodo. La dirección local identifica a un nodo en particular dentro de la red de una organización.

Figura 2.19. Formato de una dirección de IP.

Todas las computadoras deben tener una dirección de IP única en el rango de los sistemas con los que se comunican. Todo esto da como consecuencia a las clases de direcciones, que tienen las características que se muestran en la *Tabla 2.2.*

Clase	Tamaño de la Dirección de la Red (en octetos)	Primer Número	Número de Direcciones Locales
A	1	0 — 127	16.777.216
B	2	128 — 191	65.536
C	3	192 — 223	256

Tabla 2.2. Características de Clases de Redes.

La parte de red de una dirección de Clase A tiene una longitud de un octeto. Los tres octetos restantes de una dirección de Clase A pertenecen a la parte local (número de host) y se usan para asignar números a los nodos.

Existen muy pocas direcciones de Clase A y la mayoría de las organizaciones de gran tamaño han tenido que conformarse con un bloque de direcciones de Clase B de tamaño medio. La parte de red de una dirección de Clase B es de dos octetos. Los dos

octetos restantes de una dirección de Clase B pertenecen a la parte local y se usan para asignar números a los nodos.

Las organizaciones pequeñas reciben una o más direcciones de Clase C. La parte de red de una dirección de Clase C es de tres octetos. De esta forma sólo queda un octeto para la parte local que se usa para asignar números a los nodos. La *Figura 2.20.* Muestra el Formato en cada Clase. Es sencillo adivinar la clase de una dirección de IP. Basta con mirar el primer número de la dirección en formato de puntos.

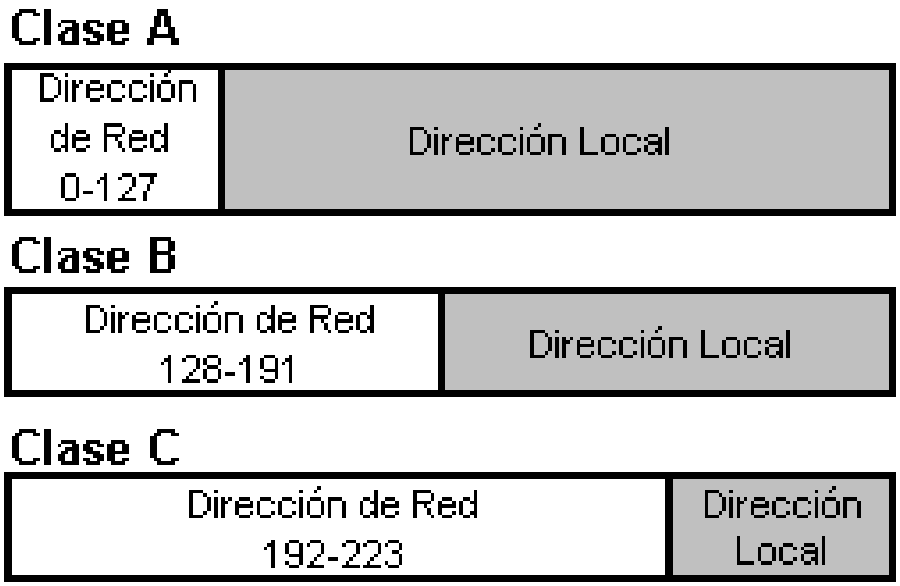

Figura 2.20. Formato de Direcciones en cada Clase de Red.

Además de las Clases A, B y C, existen dos formatos especiales de direcciones, la Clase D y la Clase E. Las direcciones de Clase D se usan para multienvío de IP. El multienvío permite distribuir un mismo mensaje a un grupo de computadoras dispersas por una red. Las direcciones de multienvío permiten realizar aplicaciones de conferencia. Estas direcciones empiezan con un número entre 224 y 239.

Las direcciones de Clase E se han reservado para uso experimental. Estas direcciones empiezan con un número entre 240 y 255.

2.8.2. Restricciones en las Direcciones

Se han reservado varios bloques de direcciones para su uso en redes que no se van a conectar a la Internet y que no van a necesitar conectividad con otra organización. Estas direcciones son:

10.0.0.0 — 10.255.255.255
172.16.0.0 — 172.31.255.255
192.168.0.0 — 192.168.255.255

Tenga en cuenta que puede haber muchas organizaciones que usen estos números. Si su compañía se fusiona con otra en algún momento, o decide comunicarse con los clientes o los proveedores mediante TCP/IP, puede haber conflictos de direcciones. Sin embargo, puede registrar una red de Clase C y usarla para las comunicaciones externas. Se puede obtener software de envío que mande la información entre ciertas computadoras y el mundo exterior usando una red registrada de Clase C.

2.8.3. Redes y Subredes

Una organización que tenga direcciones de red de Clase A o Clase B es muy probable que tenga una red de cierta complejidad constituida por muchas LAN y varios enlaces de WAN. Tiene sentido, entonces, dividir el espacio de estados de forma que coincida con la estructura de la red de acuerdo a una familia de subredes. Para ello, la parte local de la dirección se divide en una parte de subred y una parte de sistema de manera conveniente, como se muestra en la *Figura. 2.21.*

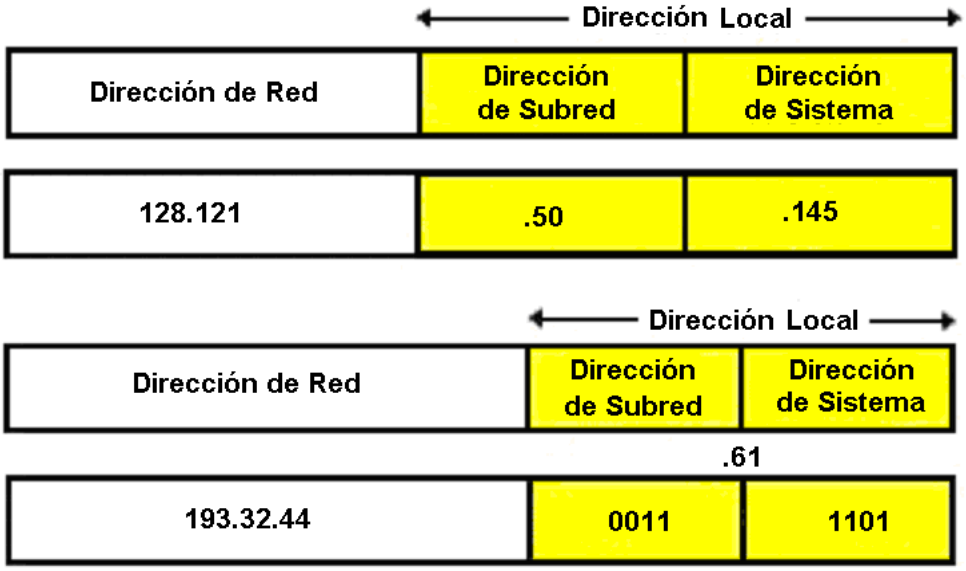

Figura 2.21. Identificación de la Red y Subred en la Dirección IP.

El tamaño de la parte de subred de una dirección y la asignación de números a subredes es responsabilidad de la organización que posee esa parte del espacio de direcciones. Las direcciones de subred suelen dividirse en bytes. Una organización con direcciones de Clase B, como por ejemplo 128.121 usará el tercer byte para identificar las subredes. Por ejemplo:

128.121.1
128.121.2
128.121.3

Entonces el cuarto byte se usará para identificar los host particulares de una subred.

Por otra parte, una organización con direcciones de Clase C sólo tiene un byte de espacio de direcciones. Podría elegir no realizar subredes o quizá usar 4 bits para direcciones de subred y 4 bits para direcciones de host, como se mostró en la *Figura 2.15*. En esta figura, las direcciones locales 61, se expresan en binario como 0011 1101. Los cuatro primeros bits identifican a una subred y los últimos cuatro bits identifican el sistema.

2.8.4. Máscaras de Subred

El tráfico se encamina hacia un host consultando las partes de red y subred de una dirección de IP. La parte de red de una dirección de Clase A, B o C tiene un tamaño fijo**.** Pero las organizaciones pueden decidir sus propios tamaños de subred. Se deben configurar los sistemas para que conozcan el tamaño de la parte de subred de la dirección.

El tamaño del campo de subred se almacena realmente en un parámetro de configuración llamado máscara de subred. La máscara de subred es una secuencia de 32 bits. Los bits que corresponden a los campos de red y subred de una dirección se ponen a 1 y los bits para el campo del sistema se ponen a 0.

Por ejemplo, si se usa el tercer byte de las direcciones que empiezan por 128.121 para identificar las subredes, la máscara es:

11111111 11111111 11111111 00000000

Normalmente las máscaras de subred se expresan en notación decimal con puntos. La máscara anterior se puede escribir como sigue:

255.255.255.0

A veces la máscara se escribe en Hexadecimal, como se muestra:

FF.FF.FF.00

Los host y routers conectados a una subred se configuran con la máscara de la subred. Suele ser común usar una única máscara de subred en toda una Internet de la organización. Hay excepciones a esta práctica, y algunas organizaciones usan varios tamaños diferentes de subred.

Por ejemplo, si una red tiene muchas líneas punto a punto, no sería conveniente usar los números de subred ya que sólo hay dos sistemas en cada subred punto a punto. Una organización podría decidir usar máscaras de 30 bits (255.255.255.252) para sus líneas punto a punto.

2.8.5. Protocolo de Resolución de direcciones

Antes de enviar un datagrama entre dos estaciones de una LAN, debe envolverse en un Frame con un Header y un Trailer. El Frame se envía a su tarjeta de interfaz de red cuya dirección física coincide con la dirección física de destino en el Header del Frame. Por tanto, para enviar un datagrama por una LAN, hay que descubrir cuál es la dirección física del nodo de destino.

Afortunadamente existe un procedimiento para descubrir automáticamente la dirección física. El *ARP (Address Resolution Protocol / Protocolo de Resolución de Direcciones)* ofrece un método de difusión para traducir automáticamente entre dirección de IP y dirección física.

Los sistemas de la red local usan ARP para descubrir información sobre su propia dirección física. Cuando un host quiere empezar a comunicarse con un socio local, busca la dirección de IP del otro en su tabla de ARP, que normalmente se mantiene en memoria. Si no existe una entrada para esa dirección de IP, el host difunde una solicitud de ARP que contiene la dirección IP de destino.

El host de destino reconoce su dirección de IP y lee la consulta. Lo primero que hace el host destino es actualizar su propia tabla de traducción de direcciones con la dirección física del origen. Es lógico ya que probablemente, el destino pronto empezará una conversación con el origen. El host destino envía de vuelta una respuesta que contiene su propia dirección de la interfaz hardware.

Cuando el origen recibe la respuesta, actualiza su tabla de ARP y ya está listo para transmitir datos por la LAN.

Una máquina puede enviar una solicitud ARP preguntando sobre su propia dirección IP. Los propósitos pueden ser:

- Detectar direcciones IP duplicadas.
- Forzar a que todos actualicen la entrada del cache correspondiente.

2.8.6. Protocolo de Resolución de direcciones inverso

Para ayudar a un nodo a descubrir su propia dirección de IP se diseñó una variante del ARP llamado *RARP (Reverse Address Resolution Protocol / Protocolo de Resolución de Direcciones Inverso)* El objetivo es que lo usen las estaciones de trabajo sin disco y otros dispositivos que necesiten obtener configuración de red de un servidor.

La estación que usa el protocolo RARP difunde una petición en la que indica su dirección física y solicita su dirección de IP. Un servidor de la red, configurado con una tabla de direcciones físicas y las correspondientes direcciones de IP responde a la petición.

El RARP ha sido superado por el protocolo *BOOTP (Protocolo de inicio)* y su versión mejorada, el *DHCP (Dynamic Host Configuration Protocol / Protocolo de Configuración Dinámica de Servidores)*. Estos protocolos son más potentes y se usan para conseguir un conjunto completo de parámetros de configuración de un sistema TCP/IP.

2.9. Servidor de Acceso Remoto

Un Servidor *RAS (Remote Access Service / Servicio de Acceso Remoto)* es una Computadora que permite a usuarios localizados fuera de una LAN, llamados usuarios remotos, o también a usuarios móviles, conectarse a la red corporativa a través de dispositivos del tipo Dial-up *(Conexión No Permanente)* como son los módems, RDSI, o a través de Internet con *VPN (Virtual Private Network / Red Privada Virtual)*.

Los clientes de acceso RAS pueden utilizar las herramientas básicas para el acceso a recursos. Por ejemplo, puede establecer una conexión a algún recurso de otra computadora, o conectarse a una impresora. Las conexiones pueden ser persistentes, es decir, que permanecen conectados al recurso hasta que explícitamente se desconectan. De esta manera, el recurso estará disponible mientras se esté conectado a la red. La convención universal de nombres es completamente soportada por el servicio de acceso remoto, así que la mayoría de los programas comerciales y aplicaciones a la medida podrán trabajar sin problema de manera remota, tal como si estuvieran dentro de la red.

2.9.1. Redes de Conexión No Permanente

En estas redes, un cliente RAS establece una conexión no-permanente. La conexión Dial-up a un puerto físico en un Servidor RAS utiliza el servicio de un proveedor de telecomunicaciones, como un teléfono analógico, RDSI o X25. Un ejemplo de una conexión Dial-up es cuando el cliente marca el número telefónico de un puerto del Servidor RAS, como se ve en la *Figura. 2.22.*

2.9.2. Redes Privadas Virtuales

Una *VPN (Virtual Private Network / Red Privada Virtual)* es la creación de conexiones seguras, punto a punto a través de una red privada o una red pública como lo es Internet. Un cliente de un VPN utiliza una clase especial de protocolos TCP/IP, llamados protocolos de túnel, para hacer una llamada virtual a un puerto virtual en el servidor de VPN. El mejor ejemplo de una VPN es cuando un cliente de VPN hace una llamada a Internet y luego establece una conexión al servidor a través de un software diseñado para este fin. El servidor contesta la llamada virtual, autentifica al usuario y transfiere datos entre el cliente de VPN y la red corporativa. (*Figura 2.23*)

Figura 2.22. Conexión Dial-up.

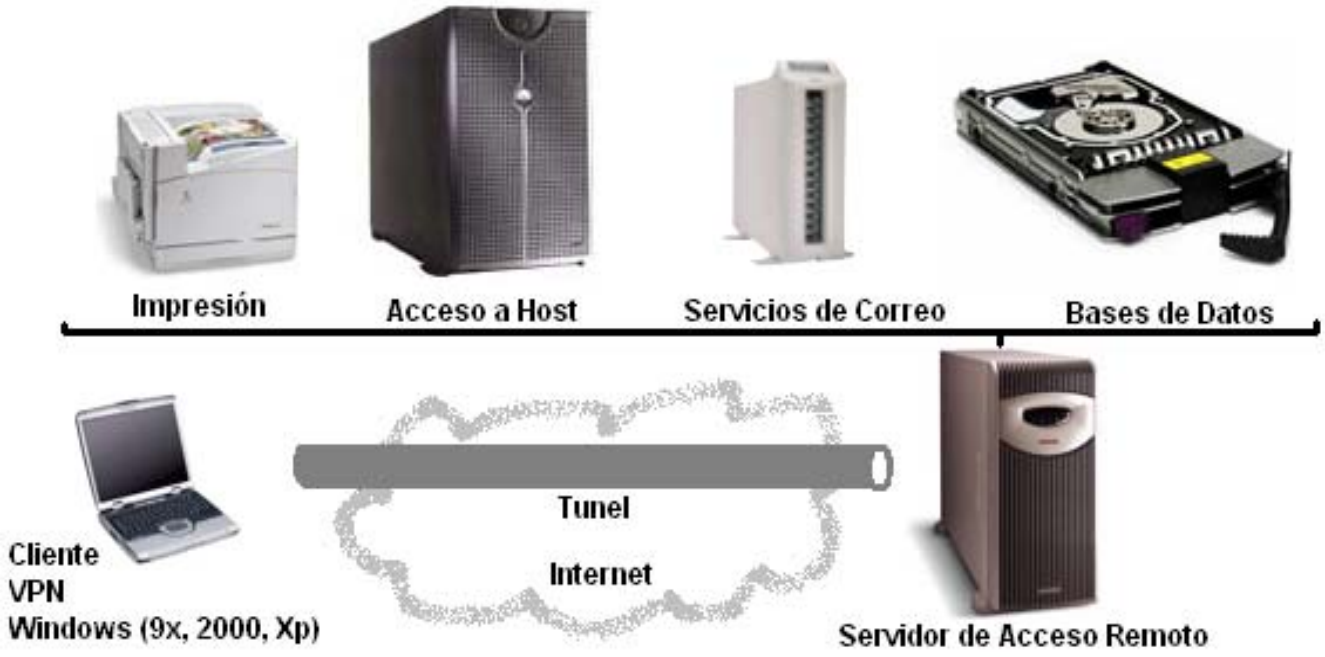

Figura. 2.23. Conexión VPN.

Las VPN son siempre virtuales, en contraste con las redes Dial-up, las cuales son conexiones directas. Las conexiones son indirectas entre un cliente VPN y el

servidor de red. Para asegurar la privacidad de la información, ésta debe viajar encriptada a través de la conexión.

2.10. Listas de Acceso

Las listas de acceso son herramientas de control. Estas listas son sumamente flexibles para filtrar el flujo de paquetes que viajan hacia las interfaces del router. Las listas de acceso son estados que especifican condiciones para el administrador que configura el router, de modo que este pueda manejar el tráfico a la salida de una manera ordenada. Básicamente existen dos tipos de listas de acceso: estándar y extendida.

- **Listas de Acceso Estándar**

Estas listas revisan la dirección fuente IP de los paquetes que pueden ser enviados. Permiten o bloquean la salida de un protocolo basados en las direcciones de red, subred y host. Si un paquete es bloqueado por una lista de acceso estándar todos los paquetes de datos son desechados.

- **Listas de Acceso Extendidas**

Este tipo de listas revisa la dirección fuente y destino del paquete, también el protocolo, el número de puerto, y otros parámetros. Los permisos se determinan a través del origen de los mismos y hacia donde tienen que ser enviados. Mediante estas listas se puede definir el tráfico necesario para inicializar una llamada.

Las listas de acceso se pueden identificar mediante un número de protocolo, el cual nos define el grupo de lista al que pertenece, estándar o extendida, También pueden existir nombres en vez de números para la lista de acceso, con lo cual se logra aumentar el rango de las mismas. El administrador de la red puede especificar sólo una lista de acceso por cada protocolo y por cada interfaz.

Las definiciones adoptadas para las listas de acceso son las que se presentan en la *Tabla 2.3.*

Tipo de Lista de Acceso	Rango
IP Estándar	1-99
Extendida	100-199
IPX Estándar	800-899
Extendida	1000-1099
Apple Talk	600-699

Tabla 2.3. Listas de Acceso.

2.11. Seguridad de la Información

La información es la base para el éxito en las empresas, por ello es que mantenerla segura es vital en la Red Financiera. Los aspectos fundamentales que debemos cuidar son la seguridad física y la seguridad durante la transferencia de la información, dentro de la organización y hacia los enlaces externos.

- **Seguridad Física**

El área donde se almacena la información del banco debe mantenerse protegida de cualquier clase de siniestro, como puede ser un terremoto, incendio, robo, etc.

El *Site (como normalmente se llama al sitio donde se encuentran los equipos de comunicaciones, servidores y respaldo de información)*, debe mantenerse protegido de personas que pudieran causarle daño o robarlo. Se deben tomar en cuenta una puerta con cerradura de alta seguridad (*Figura 2.24*), vidrios blindados, temperatura baja y con un sistema de energía que garantice el suministro necesario para trabajar sin interrupción. Se debe contar con personas que protejan esta área y que vigilen que nadie pueda extraer de manera ilegal el equipo o la información.

Figura 2.24. Chapa de seguridad.

Esta seguridad dependerá del presupuesto que la empresa asigne al área y del valor que le dé a la información que se almacena en este lugar. Un banco requiere, tanto por el valor de la información como por los reglamentos, implementar un ambiente altamente seguro en esta área.

También es importante hacer conciencia entre los empleados, que protejan sus equipos de trabajo de las personas que con mala intención pudieran extraer información, como pueden ser visitantes en horas de trabajo o personas externas a la empresa, etc. También es importante que no dejen papeles en las impresoras que pudieran tener información importante.

- **Seguridad en Redes**

Una red protegida debe validar los accesos que positivamente sean identificados como permitidos. Este acceso debe ser irrevocable. Nadie debe ser capaz de emular a alguien más y tampoco debe ser capaz de negar el envió de mensajes después de que se ha podido acceder a la Red.

A continuación se enlistan las partes esenciales para tener seguridad en la Red.

- **Establecer Inicio de Conexión.** Provee conexiones seguras, que son tan inmunes como es posible hacia los efectos de los intrusos que podrían estar escuchando la red.
- **Ruteadores Autentificados.** Una red debe empezar con dispositivos de seguridad confiables. Para eliminar el tipo de ataque conocido como intruso a mitad del camino, cada dispositivo de encripción de la red debe ser autentificado por cada dispositivo al cual enviará datos encriptados.
- **Políticas de Encripción.** Incluye una declaración de las redes que van a ser encriptadas y un límite de tiempo de sesiones de encripción.
- **Utilizar Llaves de Encripción Seguras**. Define los tipos de encripción a usar en una red segura. Las llaves de encripción son simplemente secuencias de números usados para convertir texto limpio en texto cifrado.

Por lo general, existen tres tipos de ataques que pueden potencialmente impactar en forma negativa un negocio:

- **Hurto de información.** Robo de información confidencial, tales como registros de clientes y empleados.
- **Sabotaje de información.** Cambios a la información, en un intento de dañar la reputación de una persona o empresa, como por ejemplo, elaborando cambios a los registros educativos y médicos de los empleados o publicando contenido malintencionado en su sitio Web.
- **Restricción del Servicio *DoS (Denial of Service / Negación del Servicio*).** Bloqueo de los servidores o red de su empresa, de forma que los usuarios legítimos no puedan acceder a la información o, para impedir la operación normal de su empresa.

Los ataques que normalmente se hacen en los sitios de Internet tienen, como principal objetivo, obtener información restringida, modificar o borrar información o dar

de baja los servicios que presta el sitio. Cada año se invierten grandes cantidades de dinero para prevenir o detectar accesos no autorizados.

Algunos de los métodos de ataque que utilizan estas personas son:

- **Ataque de fuerza bruta.** Un intruso intenta cualquier posible combinación de una llave, para acceder a la red.
- **Ataque de un intruso a mitad de camino.** Un intruso se sitúa entre dos host e intercepta el tráfico que pasa entre ellos.
- **Ataque de negación de servicio.** Un intruso intenta reducir la cantidad de datos que van o vienen de la red segura. Esta situación influye más en la disminución de la productividad de la red que en la seguridad de la misma.
- **Repeticiones de ataque.** Un intruso intenta reintroducir a intervalos de tiempo una llave descifrada, esperando que la red segura la utilice en alguna ocasión.
- ***Spoofing (Engaño)* de las direcciones de la red.** Un intruso busca y encuentra los pares de direcciones fuente y la utiliza como puerta de enlace *(gateway)* para romper las restricciones de control de acceso.

Ahora describiremos las diversas maneras de proteger los datos:

- **Seguridad al Transferir Información**

La seguridad al momento de transferir información, sobre todo en enlaces externos a través de Internet, es un tema que ha cobrado mucha fuerza en los últimos años, ya que hay personas llamadas *Hackers (así se les conoce a las personas que desean sustraer Información valiosa de algún lugar sin autorización para su beneficio)* o *Crackers (son individuos que gustan de corromper accesos por diversión)* que están constantemente buscando vulnerabilidades en las empresas para obtener beneficio propio o simplemente para causarles daño.

Otro aspecto que debemos recordar, es que los servidores de archivos, de bases de datos y de correo electrónico, entre otros, deben estar correctamente configurados de forma que cada usuario pueda ver únicamente su información, pero no la de los demás usuarios. En el caso de redes grandes, puede resultar interesante la división de departamentos en subredes, ya sea a través de routers, o a través de las facilidades que ahora brindan los sistemas operativos de red, con el fin de crear unidades de administración independientes. De esta manera, los usuarios de un departamento serán completamente independientes de los otros departamentos. En este esquema se utiliza un servidor de archivos para cada subred y un router con tantas tarjetas de red como departamentos, para interconectarlos.

En general, la seguridad de los datos debe proveer las siguientes políticas:

- Encripción de los datos para negar el acceso a la información de los Sites, a usuarios no autorizados.
- Una barrera para prevenir que el intruso pueda encontrar una forma de ataque.
- Una barrera para prevenir que alguien simule ser otra entidad y logre el acceso.
- Una firma para garantizar que el transmisor de datos es alguien permitido y no ficticio.
- Una firma para garantizar que el transmisor envió los datos y posteriormente no pueda negar el acceso a los mismos.
- Reducción y/o eliminación del ataque de negación de servicio.
- Generación dinámica de llaves de sesión, para forzar al intruso a descifrar la nueva llave periódicamente.
- Utilización de passwords de administrador y de usuario, determinando las prioridades en cada caso.

- **Firewalls**

La manera de protegerse de estos ataques es a través del llamado *Firewall (barrera de fuego)*, que es un equipo o programa que se dedica a verificar que solamente las personas autorizadas puedan pasar a través del enlace hacia o desde Internet. Cualquier intento de acceso que no esté previamente autorizado es desechado. Por ejemplo: se tiene un servidor web NT con el puerto 139 abierto (utilizado por *NetBIOS*, el cual es un Protocolo de Red), pero en el Firewall se cierra el puerto 139. Entonces, ningún usuario externo a la red podrá abrir una conexión al puerto 139 del servidor web, puesto que el Firewall la rechazará.

Importancia del Uso de un Firewall

La forma de proteger a la red privada a través de los Firewalls es que poseen capacidad de encripción de VPN, ya sea integrada o como característica opcional. Este recurso ofrece a las empresas una alternativa sencilla y rentable, en comparación con las líneas dedicadas tradicionales o el acceso remoto a través del módem. Al momento de implementar una VPN, todos los dispositivos deben soportar el mismo nivel de encripción.

Un Firewall constituye más que una puerta cerrada con llave al frente de su red. Es su servicio de seguridad particular. Un Firewall proporciona al administrador de la red: datos, información acerca del tipo y cantidad de tráfico que ha fluido a través del mismo y cuántas veces se ha intentado violar la seguridad. De manera similar a un sistema de circuito cerrado de TV, el Firewall no sólo bloquea el acceso, sino que también lo monitorea y nos ayuda a identificar a los usuarios que han intentado violar la seguridad.

Seguridad de Redes usando Firewalls

Uno de los puntos más importantes es la seguridad de los datos que se envían por la red pública y de las prioridades de acceso de los usuarios internos. El acceso a los servicios estará determinado a través de un enlace privado de Internet que tiene que ser autentificado por medio de los servidores de seguridad y el Firewall que nos permitirán validar la autentificación del usuario y su acceso a los servicios que proporciona el Proveedor.

Un Firewall es un sistema que permite ejercer políticas de control de acceso entre dos redes, por ejemplo: una red LAN privada y una red pública (como Internet). El Firewall define los servicios que pueden accederse desde el exterior y viceversa. Los medios a través de los cuales se logra esta función varían notoriamente, pero en principio, un Firewall puede considerarse como un mecanismo para bloquear y permitir el tráfico.

Un Firewall lleva a cabo tres funciones para proteger la red:

- Bloquea los datos entrantes que pueden contener el ataque de un hacker.
- Oculta la información acerca de la red, haciendo que todo parezca como si el tráfico de salida se originara del Firewall y no de la red. Utiliza *NAT (Network Address Translation / Traslación de Direcciones de Red),* para cambiar las direcciones públicas en direcciones privadas.
- Filtra el tráfico de salida, con el fin de restringir el uso de Internet y el acceso a localidades remotas.

Niveles de filtración

Un Firewall puede filtrar tanto el tráfico que sale como el que entra. Debido a que el tráfico que entra constituye una amenaza mucho mayor para la red, éste es inspeccionado de manera más estricta que el tráfico que sale. Al momento de evaluar productos de hardware y software de Firewall, es muy común escuchar acerca de tres tipos de filtración:

- La filtración que bloquea cualquier dato de entrada que no haya sido específicamente solicitado por un usuario de la red.
- La filtración basada en la dirección del Origen.
- La filtración basada en el contenido de la comunicación.

El Firewall inicialmente determina si la transmisión entrante ha sido solicitada por un usuario de la red y, de no ser así, la rechaza; posteriormente, cualquier dato que haya sido permitido se inspecciona cuidadosamente. El Firewall verifica la dirección de la computadora del remitente, con el fin de certificar que proviene de un sitio confiable, finalmente, se encarga de verificar el contenido de la transmisión.

Un hacker puede intentar obtener acceso a su red por diversos medios. Un intento de lograr acceso, por lo general, comienza con la recolección de información acerca de la red. Luego, esta información se utiliza para realizar un ataque con un propósito específico, ya sea para apoderarse de los datos o destruirlos. Un hacker puede usar un scanner de puertos, un software que permite ver la estructura de la red. Esto les permite averiguar cómo está estructurada la red y qué software se está ejecutando en la misma.

Una vez que el hacker tiene una idea de la estructura de la red, puede aprovecharse de todas las debilidades conocidas del software y utilizar las herramientas de piratería para ocasionar estragos en su ambiente. Es posible, inclusive, ingresar a los archivos de los administradores y dejar en blanco los discos, aunque una buena clave de acceso por lo general puede dificultar esta tarea. Afortunadamente, un buen Firewall es inmune a un escaneo de puertos y, a medida que se desarrollan nuevos escaners de puertos para evadir esta inmunidad, los fabricantes de Firewall producen actualizaciones para preservarla.

Firewall de filtración de paquetes

Un Firewall de filtración de paquetes verifica la dirección IP de donde proviene el tráfico entrante y rechaza cualquier tráfico que no coincida con la lista de las direcciones confiables. El Firewall de filtración de paquetes utiliza reglas para negar el acceso, según la información contenida en el paquete, como por ejemplo: el número del puerto TCP/IP, la dirección IP de la fuente/origen o el tipo de datos.

Un router común de una red puede filtrar el tráfico por dirección, pero los hackers tienen un pequeño truco llamado *spoofing (engaño)* de IP, con el cual los datos parecen provenir de una fuente confiable o incluso de una dirección de su propia red. Desafortunadamente, el Firewall de filtración de paquetes es propenso al spoofing de IP y son muy difíciles de configurar. Cualquier error en su configuración puede dejarlo vulnerable a los ataques.

Características y funciones adicionales de un Firewall

Además de las capacidades de seguridad estándares, se ha integrado una gran cantidad de características y funciones adicionales a los productos de Firewall; entre éstas figuran: soporte para servidores públicos de Web y correo electrónico (filtrado de contenido), que constituyen la llamada *DMZ (De-Militariced Zone / Zona Desmilitarizada).* Además, poseen otras funciones como soporte de encriptación de VPN y protección a través de antivirus.

Un Firewall que provee protección DMZ es una solución efectiva para empresas que ofrecen a sus clientes la posibilidad de conectarse a su red a partir de cualquier medio externo, ya sea a través de Internet o cualquier otra ruta. La decisión de optar por un Firewall con DMZ debe basarse en la cantidad de usuarios externos que acceden a la red y la frecuencia con la que lo hacen. Un Firewall con DMZ crea un área de información protegida en la red. Los usuarios externos pueden ingresar al área

protegida, pero no pueden acceder al resto de la red. Esto permite a los usuarios externos acceder a la información a la que tienen permiso, pero previene que obtengan información no autorizada.

Uno de los factores que deben tomarse en cuenta para la selección de un Firewall es, que entre más avanzado sea el nivel de encripción, mayor capacidad de procesamiento requerirá. Un pequeño número de proveedores ofrece ahora la aceleración de VPN por hardware, con el fin de optimizar el rendimiento del tráfico VPN.

Filtración de contenido

Un filtro de sitios Web o filtro de contenido extiende las capacidades del Firewall para bloquear el acceso a ciertos sitios Web. Con esta función adicional, se restringe el acceso de los empleados a sitios con contenido impropio.

Esta funcionalidad le permite definir categorías de material inadecuado y obtener un servicio que lista miles de sitios Web que incluyen dicho tipo de material. Como siguiente paso, se puede escoger el bloquear totalmente el acceso a estos sitios o permitir su uso, pero manteniendo un registro del mismo. Tal servicio debe actualizar automática y regularmente la lista de sitios Web que no pueden ser accedidos.

Protección a través de antivirus

Todos debemos preocuparnos seriamente por las amenazas de los virus, uno de los esquemas más nocivos de piratería de computadoras. Los usuarios pueden dañar rápidamente toda una red si, inadvertidamente, bajan material desconocido o diseminan virus peligrosos en las redes. Empresas de todo tipo y tamaño han perdido enormes cantidades de dinero, debido al impacto negativo en la productividad y los costos de reparación de la red causados por un virus. Los Firewalls no están diseñados para remover o limpiar virus, no obstante, pueden ayudar a detectarlos, lo cual es un factor esencial de cualquier plan de protección contra virus. Es importante observar que el Firewall sólo puede proteger la red a partir del dispositivo de WAN al cual está conectado.

Un servidor de acceso remoto, o una PC con un modem, puede servir como puerta de acceso a la red, el cual puede burlar las medidas de seguridad del Firewall. Lo mismo puede ocurrir cuando un empleado introduce un *diskette (disco flexible)* infectado con un virus en su PC. El lugar más apropiado para instalar el software antivirus es en la PC de cada usuario. No obstante lo anterior, un Firewall puede contribuir a la detección de virus, exigiendo que cada usuario que ingrese a Internet o baje correo electrónico, utilice, como mínimo, la última versión del software antivirus.

Selección del Firewall

Las funciones de un Firewall pueden implementarse ya sea como software o como complemento a su router o gateway. Alternativamente, la demanda de los dispositivos dedicados de Firewall está creciendo, principalmente debido a su facilidad

de uso, mejor rendimiento y bajo costo. Mencionaremos aquellos Firewall de mayor importancia:

Firewalls basados en routers firmware

Algunos routers proveen capacidades limitadas de Firewall. Éstas pueden incrementarse con software u opciones de firmware adicional. No obstante, es importante que tenga cuidado de no sobrecargar su router con servicios adicionales de Firewall. Además, es posible que algunas funciones de Firewall, como VPN, DMZ, filtración de contenido o protección a través de antivirus, no estén disponibles o sean muy costosas de implementar.

Firewalls basados en software

Por lo general, los Firewall basados en software son aplicaciones sofisticadas y complejas que se ejecutan en servidores dedicados UNIX o NT. Estos productos se tornan aún más costosos cuando usted suma los costos de software, sistema operativo, hardware de servidor y mantenimiento continuo requerido para soportar su implementación. Resulta esencial también que el administrador del sistema monitoree constantemente e instale las actualizaciones más recientes de seguridad y del sistema operativo, tan pronto como se encuentren disponibles. Sin estas actualizaciones que cubren los nuevos peligros de seguridad, el software de Firewall puede volverse totalmente inservible.

Dispositivos de Firewall dedicados

La mayoría de los dispositivos de Firewall son sistemas de hardware dedicados. Estos dispositivos son menos susceptibles a las fallas de seguridad inherentes de los sistemas operativos Windows NT o UNIX, gracias a que integran sistemas operativos desarrollados específicamente para utilizarse como Firewall. Estos Firewalls de alto rendimiento han sido diseñados para satisfacer los altos requerimientos de rendimiento o del procesador, exigidos por los Firewalls SPI. Debido a que no es necesario fortalecer el sistema operativo, por lo general, los dispositivos de Firewall son más fáciles de instalar y configurar que los productos de Firewall de software. Estos ofrecen potencialmente un nivel de instalación “Plug-and-Play”, requieren mínimo mantenimiento y una solución completa. También constituyen una solución rentable en comparación con otras implementaciones de Firewall.

- **Encripción de los Datos**

La encripción es un mecanismo que convierte información entendible a una serie de caracteres que ocultan el significado real; por ejemplo, cuando una palabra como “**Acceso**” es encriptada y enviada, las personas ajenas que quieran ver esta información, observarán una frase completamente distinta como por ejemplo, “**Bddftp**”. De esta forma no se da a conocer la información real. Sin embargo, cuando la frase

llega a su destino correcto, corre un mecanismo que invierte esa serie de caracteres a la información real, de tal forma que sólo el que envía y el que recibe la información pueden ver la frase real.

La encripción se relaciona principalmente con la palabra criptografía, del griego **Kripto**: Esconder y **Grafos**: Palabra.

La encripción puede salvaguardar los datos que viajan de un router a otro a través de una red insegura. El hecho de salvaguardar los datos ha tomado mucha importancia para las organizaciones a medida que las redes privadas son remplazadas por redes públicas. Por ejemplo, muchas organizaciones están utilizando actualmente Internet en lugar de líneas dedicadas con el objeto de ahorrar costos en sus operaciones.

Los datos que viajan a través de líneas de redes inseguras están expuestos, como ya se mencionó, a diferentes tipos de ataques. Estos datos pueden ser leídos, alterados o falsificados por cualquier persona que tenga acceso a la ruta que los datos tomen para llegar a su destino. Existe también la posibilidad de que un intruso pueda alterar los paquetes causando daño mediante la obstrucción, reducción o inutilización de las comunicaciones dentro de la organización. La vulnerabilidad de los datos de la red puede ser minimizada configurando la encripción en los routers.

La encripción de datos transforma información legible, llamada texto limpio, en una forma no legible llamada texto cifrado, para proveer seguridad en los intercambios de información. La encripción de datos es una de las mejores técnicas de seguridad disponible actualmente para la transferencia de información.

La encripción convierte los paquetes de información en datos sin sentido para cualquier persona o proceso, excepto para ella misma; de tal manera que la encripción pueda recuperar esos datos enviados a través de redes inseguras y no puedan ser interrumpidos o interceptados en una forma legible.

La encripción conjunta el uso de un algoritmo con una llave de encripción. Existen diferentes tipos de algoritmos, cada uno con sus fortalezas y debilidades, y cada uno impone restricciones en cuanto al tamaño mínimo y máximo de la llave de encripción.

La encripción transforma los datos de tal manera que los patrones reconocibles son movidos. Por ejemplo, en un mensaje simple de correo electrónico, al menos el 70% del mensaje consiste de espacios en blanco. El mecanismo de encripción seleccionado debe garantizar que todo el mensaje sea convertido de tal manera que dicho patrón de datos no pueda ser interpretado. Los espacios en blanco sucesivos deben ser convertidos en cualquier tipo diferente de datos.

No debe haber distinción entre frases o palabras que puedan dar una pista a un *hacker* del tipo de tráfico que esta siendo transmitido. Cualquier tipo de pista en los datos puede disminuir significativamente la seguridad de los mismos.

Existen muchos métodos de encripción, que van desde los sencillos (utilizados cuando queremos enviar un mensaje a alguna persona, pero no queremos que lo entienda el mensajero), hasta los complejos algoritmos que utilizan los Firewalls. Cada persona podría definir su método de encripción. En el ejemplo mencionado anteriormente, en donde encriptamos la palabra "**Acceso**" para quedar como "**Bddftp**", lo que se hizo fue poner el siguiente carácter en el alfabeto. Si se tiene una "**A**", se pone una "**B**"; para una "**c**", se pone una "**d**", y así sucesivamente.

Cuando se habla de privacidad o confidencialidad, se habla de mantener algo en secreto. La forma fundamental de mantener algo en secreto es usando la encripción, para transformar datos en algún formato ilegible, y la desencripción para convertir información encriptada nuevamente a su formato original, he aquí los mecanismos para encriptar los datos:

- Reconocimiento de routers de Encripción.
- Establecimiento de una Sesión de Encripción entre los routers.
- Encripción y Desencripción de Paquetes en la Red.
- Tecnología de Llaves-Públicas.
- Tarjeta ESA
- Niveles de Encripción

A la fecha, el nivel más avanzado de encripción públicamente disponible es el estándar 3DES de 168 bits que, según los expertos de seguridad, es inquebrantable.

Reconocimiento de routers de Encripción

Durante el inicio de cada sesión de encripción, los routers participantes intentan autentificarse uno al otro. Si cualquier router falla al autentificar al otro, la sesión de encripción no será establecida y no se permitirá el paso del tráfico encriptado. La autentificación en pares asegura que solamente el par de routers involucrados en la encripción, puedan intercambiar tráfico encriptado, previniendo de esta manera que algún router pueda ser engañado y comience a enviar tráfico encriptado hacia routers fraudulentos o ilegítimos.

La autentificación entre los routers ocurren durante el inicio de cada sesión de encripción. Pero antes de que los routers puedan autentificarse uno a otro, es necesario generar una llave *DSS (Digital Signature Standard / Firma Digital Estándar)* pública y privada para cada router y además intercambiarlas mutuamente. Después de esto, las llaves serán usadas cada vez que una sesión de encripción se lleva a cabo.

Establecimiento de una Sesión de Encripción entre los routers

Una sesión de encripción debe establecerse antes de que un router pueda enviar tráfico encriptado hacia el otro router de encripción; una sesión de encripción se establece siempre que un router detecta un paquete de IP que debe ser encriptado.

Para establecer una sesión de encripción, dos routers intercambian mensajes de conexión. Estos mensajes tienen dos propósitos: el primero es para autentificarse mutuamente. La autentificación es acompañada de marcas o firmas pegadas a los mensajes de conexión. Una marca o firma es una cadena de caracteres que es creada por cada router local, con base en su propia llave DSS privada, y es verificada por el router remoto usando la llave pública del router que anteriormente le envió. Una marca o firma es siempre única para el router transmisor y no puede ser falsificada por cualquier otro dispositivo. Una vez que la marca ha sido verificada, el router que la envió es autentificado. El segundo propósito de mensajes de conexión es generar una llave de sesión *DES (Data Encryption Standard / Encripción de Datos Estándar)* temporal, la cual es utilizada para encriptar los datos durante la sesión de encripción. Para generar la llave DES, los números del algoritmo de encripción *DH (Diffie-Hielman)* son usados para computar una llave común DES de sesión que es compartida entre ambos routers.

Después de que ambos routers son autentificados y la llave de sesión ha sido generada, los datos pueden ser encriptados y transmitidos. El algoritmo DES de encripción utiliza la llave para encriptar y desencriptar los paquetes de IP durante la sesión de encripción.

Una sesión de comunicación encriptada termina cuando los números DH y la llave DES son descartados. Cuando otra sesión de encripción es requerida, nuevos números DH y llaves DES serán generados. Tanto l*a* DES *como el* algoritmo *DH* son una herramienta eficiente para pasar grandes cadenas de datos encriptados.

Encripción y Desencripción de Paquetes en la Red

Actualmente la encripción y desencripción de paquetes de IP ocurre únicamente en los routers que se configuran para ello. Tales routers son considerados *como Peer Encrypting Routers (Par de Routers de Encripción)* o simplemente peer routers *(Par de routers)*.

Los routers que se encuentran en los saltos intermedios no participan en el proceso de encripción / desencripción. Frecuentemente los routers de encripción (peer routers) se sitúan en los bordes de las redes inseguras, de tal manera que provean la comunicación segura entre dos redes protegidas que están físicamente separadas.

El tráfico no encriptado que viene de la red protegida, entra a un peer router, se encripta y se envía a través de la red no protegida. Cuando el tráfico encriptado llega al peer router remoto, éste lo desencripta antes de enviarlo dentro de la red protegida.

Los paquetes son encriptados en la interfaz de salida de un peer router y desencriptados en la interfaz de entrada del otro peer router, localizado en un punto remoto.

Tecnología de Llaves-Públicas

La tecnología de *PK (Public Key / Llaves Publicas)* se basa en un par de llaves. Una llave se utiliza para encriptar y la otra para desencriptar. Cualquiera de las dos llaves puede ser utilizada para encriptar de tal manera que la otra llave será utilizada para desencriptar. Esto se conoce como un mecanismo asimétrico. Cada llave del par es utilizada únicamente en un solo sentido en el mecanismo de encripción. La misma llave no puede ser utilizada para desencriptar el mensaje. El hecho de marcar ó firmar un documento es fundamental para la tecnología de llaves públicas. Una marca o firma debe establecerse con base en una serie de políticas de seguridad acorde con las siguientes características:

- No debe perderse.
- Debe ser auténtica, de tal manera que convenza a los receptores del documento que el transmisor realmente marcó el documento.
- No debe ser reusable y debería ser parte del documento, de tal manera que otra persona no pueda manipularla.
- Un documento marcado debe ser inalterable. No puede ser descartado, es decir, una vez que se ha marcado y enviado, el transmisor no podrá posteriormente negar el envío del mensaje.
- La existencia de llaves electrónicas nos permite fortalecer la seguridad, ya que dichas llaves generan un grupo de números aleatorios que cambian dinámicamente.
- Un mecanismo de verificación de la llave se utiliza para establecer un enlace seguro con un host remoto, además se encripta el tráfico enviado hacia dicho host.

Los dos mecanismos PK y DES se combinan para crear una sesión de encripción y autentificación entre los dos host. DES es un mecanismo simétrico de encripción. Una llave simple de encripción (llamada llave de sesión) se utiliza tanto para encriptar como para desencriptar los datos. Esta llave debe ser generada por los routers participantes, teniendo cuidado de no enviar información significativa de la misma, de tal manera que un intruso pueda leerla y generar una llave con el mismo valor. El tráfico encriptado puede pasar libremente entre los routers. Cuando la sesión de encripción expira, una nueva sesión se debe establecer antes de que el tráfico encriptado pueda ser enviado.

La llave DSS privada no se comparte con ningún otro dispositivo. Sin embargo, la llave DSS pública se distribuye a todos los demás routers. Para intercambiar llaves entre dos routers es necesario ponerse de acuerdo con el administrador del otro router y ambos administradores de los routers deberán corroborar verbalmente estar de acuerdo que las llaves públicas fueron intercambiadas correctamente.

Cuando una sesión de encripción está siendo establecida, cada router utiliza la llave DSS pública de router de encripción para autentificarse mutuamente.

Tarjeta ESA

La tarjeta ESA *(Encryption Services Adapter / Adaptador de Servicios de Encripción)* provee el mecanismo de encripción basado en hardware.

Por el mecanismo de encripción, la tarjeta ESA utiliza tecnología PK basada en el concepto de *PE (Protected Entity / Entidad Protegida)* y hace uso del DES y del DSS para permitir el intercambio seguro de datos e información entre equipos similares dentro de la red.

La llave DSS de un router está compuesta de una llave pública y de una llave privada. Las llaves DSS pública y privada se almacenan en una parte de la memoria NVRAM del router, la cual no puede ser vista con comandos tales como: show configuration, show running-configuration o write terminal. Si se tiene un router con una tarjeta de encripción ESA, entonces las llaves DSS se almacenan en la memoria no manipulable de la tarjeta ESA.

Niveles de Encripción

Existen diferentes niveles donde se da la encripción:

- Encripción al nivel de Enlace.
- Encripción al nivel de Red.
- Encripción al nivel de aplicación.

Encripción a niveles de Enlace (capas 2 y 3)

La encripción en la capa de enlace provee protección extra al encriptar casi todo el paquete de datos o datagrama. Esto incluye los headers (encabezado) del protocolo. La única porción del datagrama que no es encriptada es la información del nivel del link (enlace entre dos paquetes de datos), que contiene información para acceder a las capas superiores. Este método protege tanto la información del protocolo como los datos y previene que un intruso obtenga información acerca de la estructura de red interna de una organización. La encripción de enlace de datos no permite el análisis de tráfico, así, una forma de ataque debe encriptar y desencriptar en cada salto y en cada trayectoria de la ruta seguida por los datos.

Encripción a niveles de Red (capas 3 y 4)

La encripción a nivel de red obliga a que los datos sean encriptados dejando los encabezados y el enlace con capas superiores sin encriptar. Este método asume que los datos del protocolo son sensitivos a la encripción, pero a la vez se despreocupa del análisis de tráfico de sus encabezados. La encripción a nivel de red requiere encriptar y desencriptar datos solamente una vez y los hace para las sesiones que necesita; sin embargo, los encabezados son enviados como texto el cual es factible de ser analizado.

Encripción al nivel de aplicación (capa 5, 6, 7)

La encripción a nivel de aplicación requiere que se modifique la aplicación para que se le incorpore una sesión de encripción, esto con el fin de proteger los datos que son enviados, sin esta encripción los curiosos podrían saber que tipo de datos se trataría.

De acuerdo a lo anterior, la encripción puede ser aplicada a diferentes niveles del encapsulado, como se muestra en la *Figura 2.25.* Para otorgar protección respecto a las diversas formas de ataque que existen (por ejemplo, protección de datos o análisis de tráfico) y también para permitir el paso de los datos a través de los diferentes dispositivos de red.

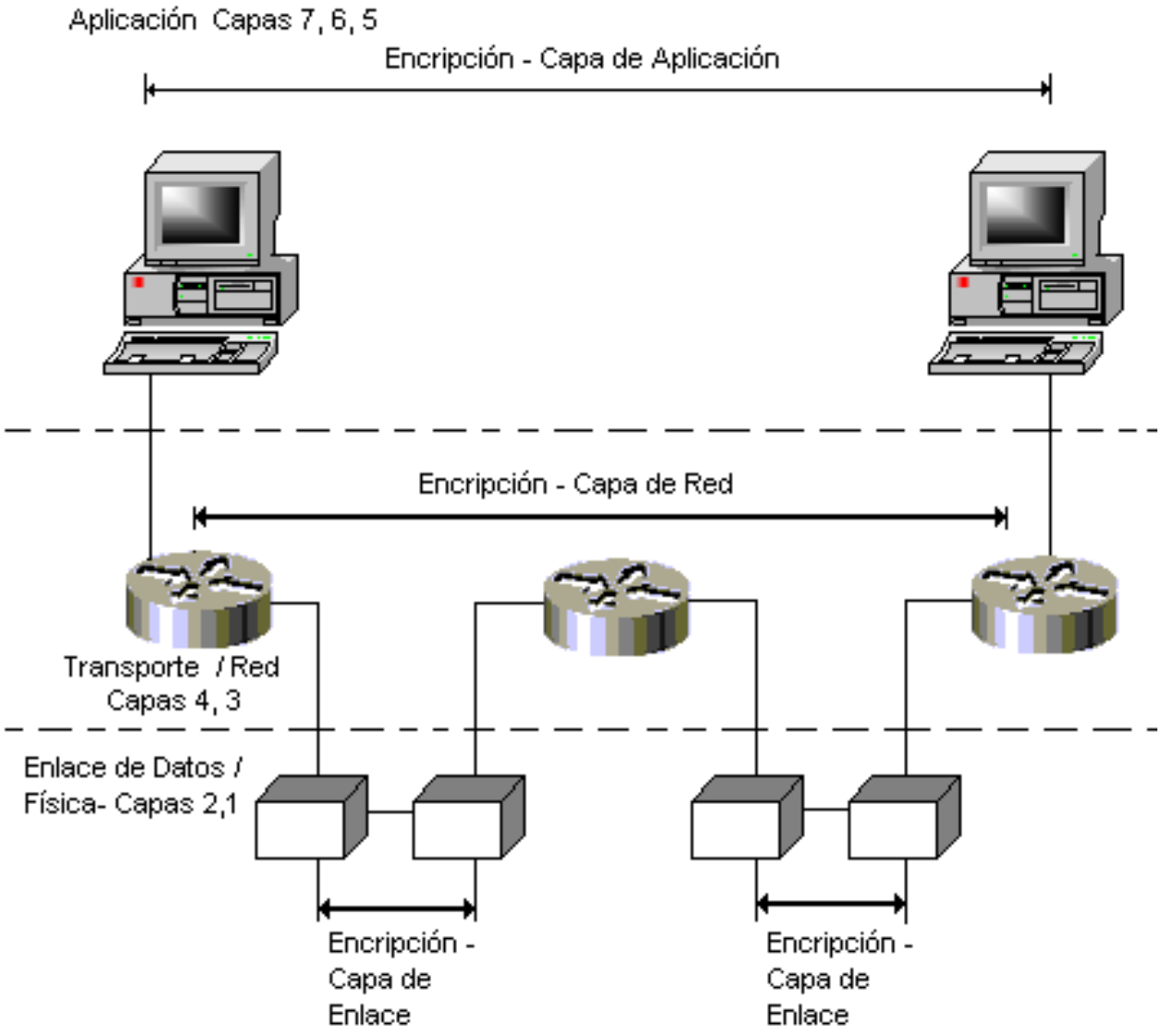

Figura 2.25. Encripción de datos.

La encripción es un arma muy eficiente para combatir la violación de la información, es un arma perfecta para obtener privacidad y seguridad, y por lo tanto no correr riesgos innecesarios. La encripción es una herramienta valiosa y ofrece un alto nivel de seguridad de la información, ya que permite el envío de información de un lugar a otro con la certeza de que, aunque alguien pudiera obtenerla, no sabría lo que significa.

Ninguna red es 100% segura. El mecanismo de encripción simplemente dificulta la manera de que algún hacker pueda desencriptar la información y obtener los datos.

- **Antivirus**

Los programas antivirus son una herramienta importante para proteger la información del Proveedor. Estos programas previenen contra los diferentes tipos de virus que existen actualmente, los cuales causan tres tipos de daño principalmente: destruyen la información, saturan los servidores de correo electrónico y mandan información a sus creadores desde el interior de las empresas.

Una característica de los virus, por ello su nombre, es que se reproducen de manera exponencial. En cuanto se activa, permanece en la memoria de la computadora infectando a los programas y archivos que se abran a partir de ese momento.

Hoy en día es un aspecto básico en el área de sistemas contar con un antivirus en cada computadora instalada y también contar con un método de actualización de dicho programa al menos una vez a la semana, ya que diariamente aparecen nuevos virus alrededor del mundo.

2.12. Cableado Estructurado

El cableado estructurado es aquel en el que todos los servicios utilizados para la transmisión de voz y datos, se conducen a través de un sistema de cableado en común (*Figura 2.26.*), bajo estándares de calidad y con las condiciones adecuadas de seguridad y temperatura. En el Apéndice A podrán verse con mayor detalle los tipos y características de los cables que se utilizan con más frecuencia.

El cableado estructurado contempla toda la trayectoria de los medios de comunicación en el sitio, y se subdivide en 6 apartados, que son:

- Entrada al edificio.
- Cuarto de equipos.
- Cableado de la dorsal (*Backbone*).
- Gabinete.
- Cableado Horizontal.
- Área de trabajo.

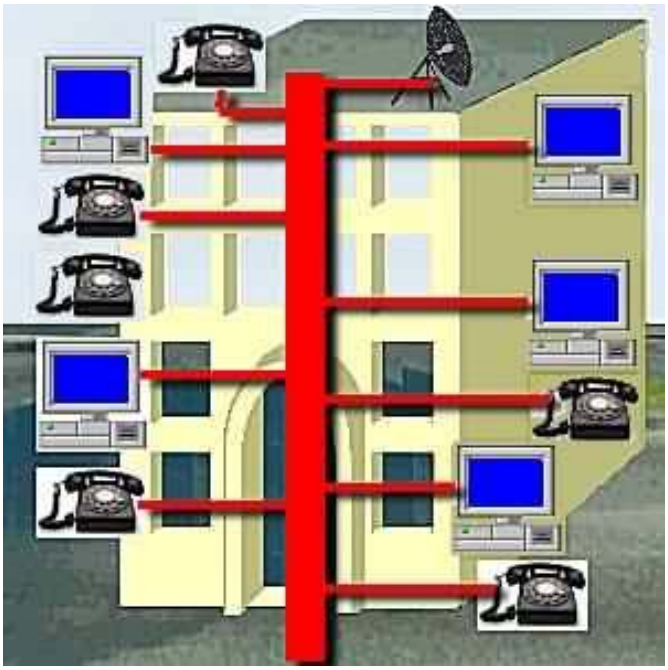

Figura 2.26. Diseño de Cableado Estructurado en una Oficina.

Entrada al edificio

La entrada a los servicios del edificio es el punto en el cual, el cableado externo se une al Backbone dentro del edificio (*Figura 2.27.*). Este punto comienza en la entrada de los servicios de telecomunicaciones al edificio (acometidas), incluyendo el punto de entrada a través de la pared y hasta el cuarto donde se rematan los servicios. Los requerimientos de la interfaz de red están definidos en el estándar TIA/EIA-569.

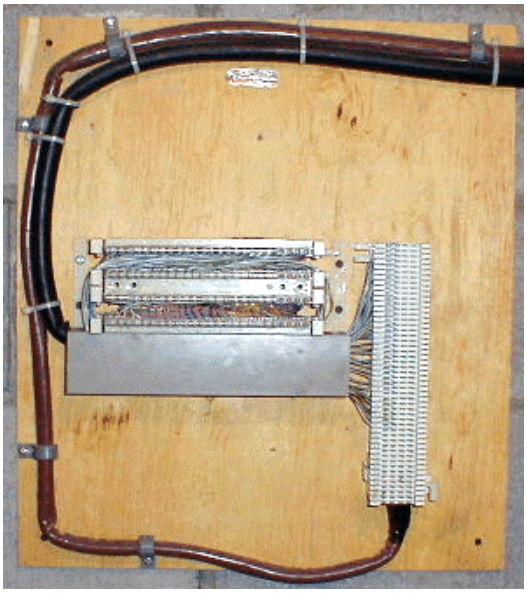

Figura 2.27. Unión del cableado externo al Backbone.

Es importante mantener la documentación de todos los servicios que entrega la compañía que nos brinda el servicio, para que en caso de falla, ésta se pueda identificar fácil y rápidamente. Esta sección debe permanecer protegida, ya que si algún cable quedara suelto, los servicios quedarán interrumpidos.

También es común que en esta área se tenga instalada la tierra física (*Figura 2.28.*), Importante para mantener los voltajes estables en toda la instalación eléctrica de las oficinas.

Figura 2.28. Tierra física.

- **Cuarto de equipos**

El cuarto de equipos es un espacio centralizado dentro del edificio (*Figura 2.29.*), donde se albergan los equipos de red (*routers, switches, mux, dtu*), equipos de voz (*PBXs*), video, etc. Los aspectos de diseño del cuarto de equipos están especificados en el estándar TIA/EIA 569.

- **Cableado del Backbone**

El Cableado del Backbone permite la interconexión entre los gabinetes de telecomunicaciones, cuartos de telecomunicaciones y los servicios de la entrada.

Este cableado normalmente atraviesa los diferentes pisos del edificio, comunicando las oficinas a las que se les da el servicio (*Figura 2.30).*

Figura 2.29. Cuarto de Equipos.

Figura 2.30. Backbone que atraviesa varios pisos.

Está formado por el cable principal, conectores y cables hacia los cuartos de telecomunicaciones, terminaciones mecánicas, regletas y jumpers, usados en las conexiones algunos partes que se nombraron se muestran en la *Figura 2.31*.

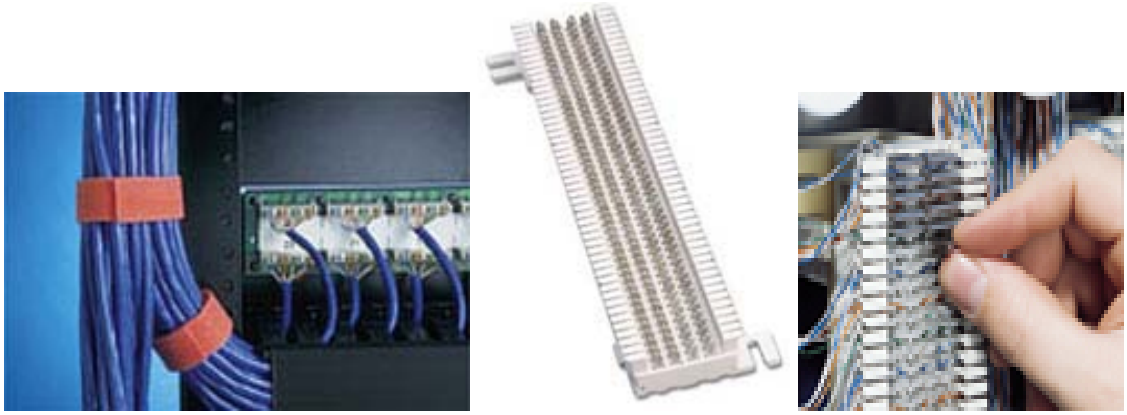

Figura 2.31. Tableros de conexión, regletas telefónicas y jumpers.

- **Gabinete de Telecomunicaciones**

El gabinete de telecomunicaciones (o rack de telecomunicaciones), es el gabinete que alberga el equipo de comunicaciones y el panel donde se remata el cableado. Este incluye las terminaciones mecánicas del cableado a la dorsal y horizontal, como se ve en la *Figura 2.32.* También podemos observar en la *Figura 2.3*3., una Gaveta con Servidores.

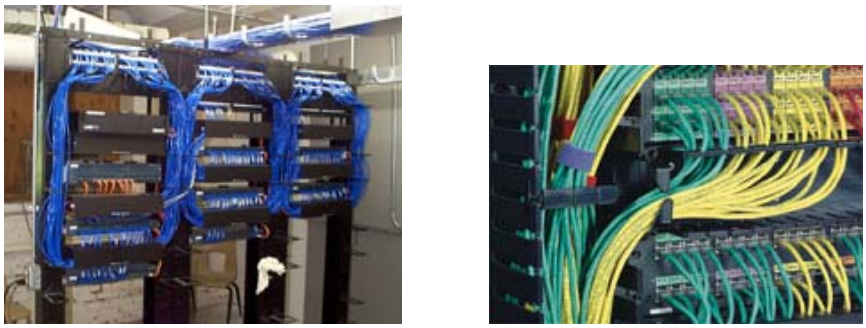

Figura. 2.32. Racks y Patch Panel de telecomunicaciones.

Figura 2.33. Gabinete con Servidores.

- **Cableado horizontal**

El cableado horizontal se extiende desde el rack de telecomunicaciones hasta el área de trabajo del usuario (*Figura. 2.34.*). Todo el trayecto a través de la oficina hasta que se conecta al equipo del usuario.

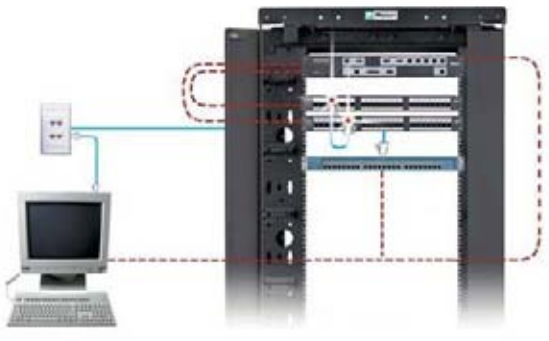

Figura. 2.34. Cableado desde el rack hasta el lugar de trabajo.

En el cableado horizontal encontramos muchos elementos que nos van a proporcionar una conexión estable, sin estorbos y agradable a la vista. Estos elementos son:

a) Cableado horizontal, ordenado e identificado. Hay cables de diferentes colores que nos ayudan a identificar los equipos que se conectan. De esta forma podemos identificar rápida y fácilmente alguna falla y también podemos ordenarlos usando los cinturones para sujetarlos (*Figura. 2.35.*).

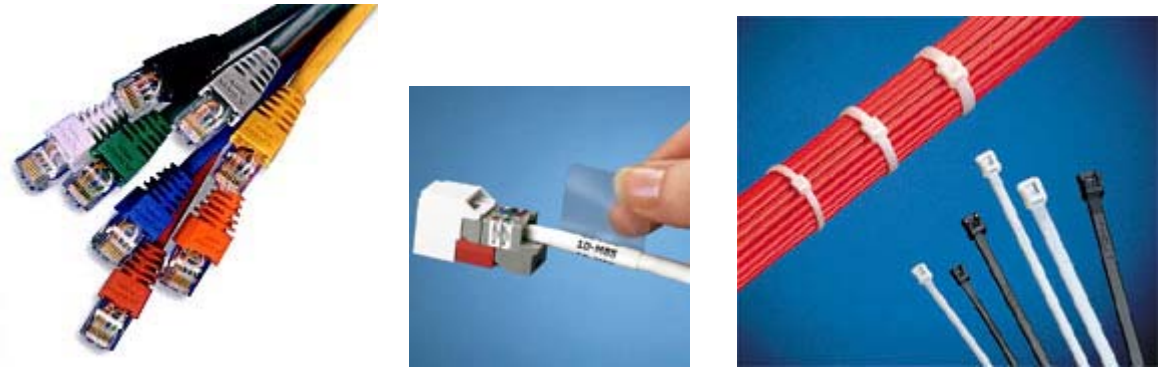

Figura. 2.35. Cables de colores, su identificación y la manera de ordenarlos.

b) Ductos de protección del cableado. No es conveniente que haya cables sueltos, con los que se pueda tropezar el usuario y causar algún accidente o desconexión. Todos los cables, ya sea de voz, datos o corriente, deben ir dentro de ductos de protección (*Figura. 2.36.*), con las especificaciones adecuadas y que dejen suficiente holgura a los cables. No se deben mezclar

cables de voz y datos con los de corriente en los mismos ductos, a menos que explícitamente lo indique el fabricante.

Figura. 2.36. Ductos de protección.

c) Terminaciones, rosetas (*Fig. 2.37.*) y placas de diferentes tamaños y diseños

Figura. 2.37. Varios tipos de rosetas de red para telecomunicaciones.

Tres tipos de medios son reconocidos para el cableado horizontal, cada uno debe de tener una extensión máxima de 90 metros:

a) Cable UTP 100-ohms, 4-pares, (24 AWG sólido)
b) Cable STP 150-ohms, 2-pares
c) Fibra óptica 125-µm, 2 fibras

- **Área de trabajo**

Los componentes del área de trabajo se extienden desde el enchufe o roseta de telecomunicaciones a los dispositivos o estaciones de trabajo (*Fig. 2.38.*).

Figura. 2.38. Lugar de trabajo.

Los componentes del área de trabajo son los siguientes:

- Dispositivos: computadoras, terminales, teléfonos, etc.
- Cables de parcheo: cables modulares, cables adaptadores y conversores, *jumpers* de fibra, etc.
- Adaptadores: deberán ser externos al enchufe de telecomunicaciones.

En los puestos de trabajo se proporcionan condiciones confiables y seguras empleando cordones a la medida para optimizar los cables sueltos. La mejora en la confiabilidad es enorme. Un sistema diseñado correctamente no requiere mantenimiento.

2.13. Redes Telefónicas

A causa de las ventajas que ofrecen las tecnologías digitales frente a sus equivalentes analógicas, las tres últimas décadas han estado marcadas por la progresiva digitalización de las redes de comunicaciones que, sucesivamente, han ido sustituyendo tramos enteros de la red analógica. Como se muestra en la *Figura 2.39,* primero fueron los troncales, luego los conmutadores, y finalmente han sido los bucles de abonado, hasta llegar a ser finalmente redes totalmente digitales.

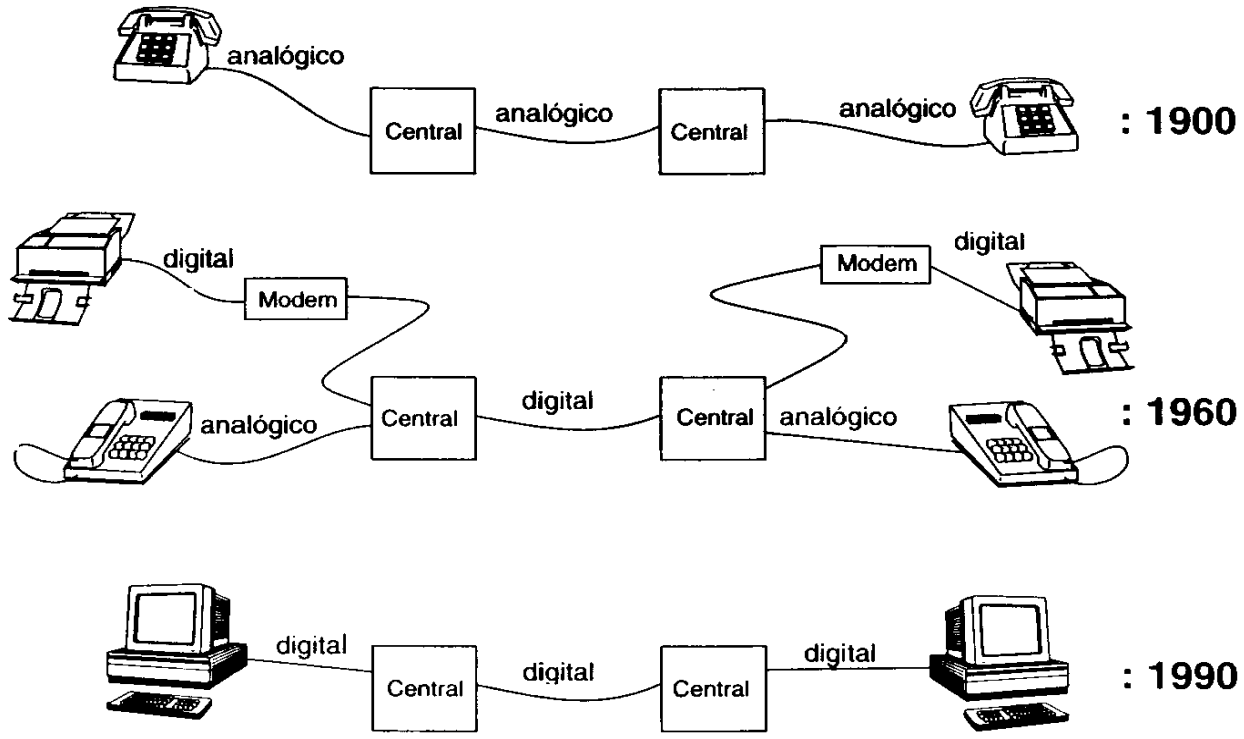

Figura 2.39. Evolución de las Redes Analógicas hacia las Digitales.

Las redes telefónicas funcionan con base en líneas conmutadas. Una línea conmutada (también llamada switched ó Dial-up) permite la comunicación con todas las partes que tengan acceso a la red telefónica pública conmutada, tenemos como ejemplo las siguientes empresas: Telnor, Telmex, Alestra (AT&T), Avantel, etc. En su aplicación en redes de Computadoras, si el operador de un dispositivo terminal quiere acceso a una computadora, éste debe marcar el número de algún teléfono a través de un modem. Al usar transmisiones por este tipo de líneas, las centrales de conmutación de la compañía telefónica establecen la conexión entre el emisor y el receptor para que se lleve a cabo la comunicación entre ambas. Una vez que concluye la comunicación, la central desconecta la trayectoria que fue establecida para la conexión y reestablece todas las trayectorias usadas de modo que queden libres para otras conexiones.

Este tipo de redes tiene gran uso cuando se requiere una cantidad pequeña de tráfico y cuando este tráfico es esporádico. Este tipo de redes es muy utilizada por bancos, industrias, instituciones académicas y usuarios en general.

Las líneas conmutadas de las redes telefónicas presentan algunas ventajas, como son:

- Comunicación muy amplia, debido a que existen mundialmente más de 600 millones de subscriptores.
- El costo de contratación es relativamente bajo.
- No se necesita ningún equipo especial, solo un modem y una computadora.
- El costo depende del tiempo que se use (tiempo medido) y de la larga distancia.

Así mismo, las líneas conmutadas presentan algunas desventajas, como son:

- No ofrecen mucha privacidad a la información.
- Se requiere marcar un número telefónico para lograr el acceso.
- La comunicación se puede interrumpir en cualquier momento.
- El ancho de banda es limitado, en el orden de kilo bits por segundo (kbps).
- La conexión entre ambas depende de que no esté ocupada la línea en la parte marcada y también de que el número de circuitos tanto para la comunicación local como nacional sean los suficientes.

Una vez que hemos mencionado los aspectos relevantes de las Redes de Cómputo, en el siguiente capítulo discutiremos ya en forma con lo que es la Propuesta de este trabajo.

CAPÍTULO 3

ANÁLISIS DE LA PROPUESTA

En este capítulo se determinarán las necesidades y los requerimientos que deben ser reforzados o sustituidos en la Red Financiera, así como las posibles soluciones que la propuesta incluye, con base en un análisis del estado actual de la Institución.

3.1. La Red Financiera y su entorno

La red del banco está dividida básicamente en dos partes. Una parte es la que se conoce como Red Financiera y a la otra se le conoce como Red Interna. En nuestro caso sólo trataremos lo referente a la Red Financiera.

La Red Financiera es el sistema de telecomunicaciones que permite la conexión y el intercambio de información electrónica entre los Intermediarios Financieros (bancos, casas de bolsa e instancias gubernamentales) y el banco.

En el banco se utiliza un sistema de comunicación redundante, con el fin de mantener el servicio continuo tanto a los usuarios internos como a las instituciones que contratan sus servicios, para evitar que queden inhabilitadas por cualquier causa.

La Red Financiera está constituida por:

- Un Site Principal que es donde se administran los servicios y se controlan los enlaces.
- Un Site Secundario de características similares al Principal que le servirá de respaldo en caso de contingencia.
- Sucursales del banco.
- Intermediarios Financieros.

Cuando se constituyó la Red Financiera, si bien no cumplía con todas las características de una red segura, sí cumplía con las exigencias en su momento, y ha venido operando en óptimas condiciones con un alto nivel de disponibilidad. Sin embargo, ha transcurrido demasiado tiempo desde su instalación, han surgido nuevos requerimientos, y con ello la necesidad de actualizarse tecnológicamente, así como de mejorar el servicio dándole mayor funcionalidad. Por esta razón, se hacen indispensables nuevos esquemas de hardware y software que permitan un mayor control, confiabilidad, rapidez, menor costo y mayor capacidad, mejorando así la calidad del servicio, pero sobre todo haciendo más eficiente y segura la información enviada por este medio a las diferentes instituciones que hacen uso de la red.

La Red Financiera opera de lunes a viernes de 7:00 a 22:00 hrs, durante todo el año. Debido a la naturaleza de la información que por ahí se transfiere, es muy difícil darle mantenimiento o modificar la configuración de algún router remoto sin afectar su operación. Además, conforme más aplicaciones y nuevas necesidades van surgiendo, los tiempos de respuesta para habilitar nuevos servicios deben ser más cortos.

Dentro de los servicios prestados por el banco se encuentran diversas aplicaciones sobre la misma red, con distintas necesidades en cuanto a calidad de servicio. El proveer un nivel de servicio y de seguridad adecuado a cada aplicación dependerá de técnicas como redes virtuales, asignación de ancho de banda comprometido, etc.

Actualmente el Banco proporciona dos tipos de servicios: Operativos e Informativos.

Los servicios operativos son los más exigentes en cuanto a rapidez en el acceso y seguridad en la red. Mediante estos servicios los usuarios obtienen y manipulan información importante, efectúan pagos, hacen transacciones, subastas, etc. Para llevar a cabo lo anterior, el Banco requiere de cierta información por parte de cada usuario (clave, contraseña o password, dirección IP y acceso de autorización (*Gateway*)), para su correcto funcionamiento dentro del sistema financiero nacional. Debido a esto, dichos servicios son sumamente sensibles al tiempo de entrega de la información.

Los servicios informativos son también muy importantes pero son menos exigentes en cuanto al tiempo de entrega de la información. A través de estos servicios los usuarios consultan saldos, estados de cuenta, tipos de cambio, estadísticas financieras, etc.

El banco evaluará la posibilidad que por el mismo canal de datos se mantengan los enlaces de voz, que actualmente tiene con sus usuarios de manera independiente a la Red Financiera. La idea es que el tráfico generado por la voz no afecte los tiempos de respuesta del tráfico de datos.

En cuanto a ruteo, se requiere proveer la función de transmisión multicast (envío de información a todos los usuarios), especialmente para las aplicaciones tipo subasta. La solución debe especificar qué limitaciones tendría bajo el sistema de trabajo de la Red Financiera con redes heterogéneas de usuarios.

Previo estudio de factibilidad económica, se podrá instalar switches adicionales en las sucursales para recibir a usuarios de esas localidades, ahorrándoles costos de renta de canales hasta la Ciudad de México.

Con la finalidad de establecer los aspectos que tienen que ser mejorados o sustituidos en la infraestructura de la Red, se define un plan de trabajo que indica el desarrollo a seguir, de acuerdo al siguiente procedimiento:

- Levantamiento de información de los Sites de la Red Financiera.
- Determinación de requerimientos.

3.2. Levantamiento de información de los Sites de la Red Financiera

Como primer punto, para las mejoras de la Red Financiera, se realiza una recopilación de información de los sitios que la componen, para determinar las condiciones actuales de operación, ubicación de los equipos, software y versiones de

sistema operativo utilizados por los routers y switches. Así mismo, se describen también los aspectos más importantes en lo referente a la operación actual de la Red Financiera.

El método que vamos a seguir es explicar cómo está conformada la infraestructura que involucra la Oficina Central (constituida por el Site Principal y el Secundario), las sucursales y los Intermediarios Financieros (usuarios externos), como se observa en la *Figura 3.1*.

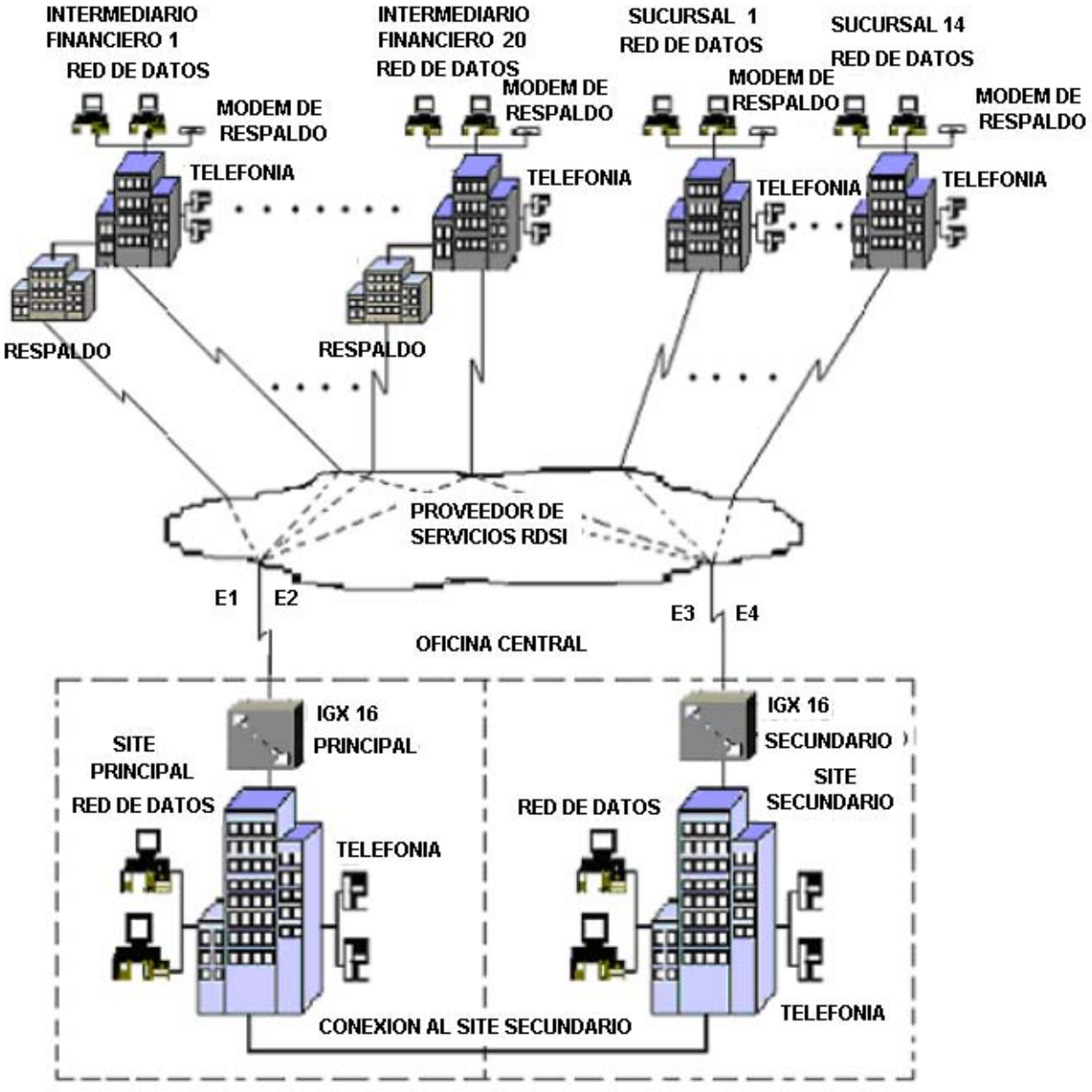

Figura 3.1. Esquema de la Red Financiera del Banco.

De manera general podemos decir que el Banco cuenta con 14 sucursales que se encuentran distribuidas en el interior de la República. Se conectan utilizando un enlace RDSI al Site Secundario de la Oficina Central ubicada en el Distrito Federal. Existen 20 Intermediarios Financieros que hacen uso de la Red Financiera y que utilizan dos enlaces remotos para su conexión. Estos dos enlaces se conectan hacia el Site Principal y Secundario respectivamente. Algunos de los Intermediarios Financieros cuentan con un sitio de respaldo en caso de contingencia, dicho enlace se conecta solamente al Site Secundario.

La conexión entre el router del Intermediario Financiero y su respaldo, se lleva a cabo a través de un enlace de fibra óptica; Todos los equipos, prioridades y listas de acceso, son configuradas en ambos routers, de esta manera, si falla alguno de ellos, todo el soporte de la red lo tendrá el otro.

Oficina Central

La Oficina Central está formada por dos Sites: Principal y Secundario. Ambos cuentan con los mismos equipos y configuraciones, teniendo en cuenta que uno es respaldo del otro. Los dos Sites están interconectados a través de dos enlaces FDDI, uno con tecnología estándar Gigabit Ethernet, que una a los routers WAN Principal y WAN Secundario y otro enlace de 2 Mbps con formato E1 que une a los routers LAN Principal y Secundario respectivamente.

El Site Principal se encuentra ubicado en el Distrito Federal, en él se localiza el equipo con que se implementan las redes WAN Principal y LAN Principal. Existen dos switches de Frame Relay, que dan salida a los routers WAN Principal y WAN Secundario respectivamente.

Los switches de Frame Relay IGX16 están formados básicamente por Tarjetas E1 y *HSSI (High-Speed Serial Interface / Interfaz Serial de Alta Velocidad)*. Ambas tarjetas tienen sus respectivas tarjetas de respaldo para que se conmuten en caso de que exista alguna falla. La interfaz HSSI es empleada para enlazar al router con el switch de Frame Relay, el cual a su vez da entrada a cada uno de los routers remotos.

En los dos switches fueron habilitados PVC´s hacia cada uno de los routers remotos y hacia cada sucursal del Banco.

En el Site Principal se utilizan dos routers de la marca Cisco modelo 7204, denominados WAN Principal y LAN Principal, que tienen idénticas características. Ambos cuentan con dos interfaces FDDI y una interfaz HSSI. Una de las interfaces enlaza a los dos routers, la otra interfaz FDDI se utiliza para enlazar al router WAN Principal a la subred de producción y en el caso del router WAN Secundario a la subred de respaldo.

Al igual que el router para el enlace WAN, los dos routers LAN Principal y LAN, Secundario son Cisco modelo 7204, tienen idénticas características y configuración.

Los routers LAN Principal y LAN Secundario contienen dos interfaces FDDI, cuatro interfaces Ethernet y cuatro interfaces Seriales. Una de las interfaces FDDI se utiliza para enlazar a los dos routers, la otra interfaz FDDI es utilizada para enlazar al router LAN Principal a la subred de producción y a la subred de respaldo en caso del router LAN Secundario.

La comunicación entre los routers LAN Principal y LAN Secundario se realiza a través de sus interfaces seriales. Además de los routers, se tiene en cada site dos switches Cisco modelo Catalyst 6000, que utiliza Frame Relay como tecnología de transporte, este switch sirve para interconectar al router WAN Principal con el router WAN Secundario y a los routers LAN, Principal y Secundario respectivamente.

El switch Catalyst 6000 contiene 2 ranuras que soportan tarjetas con 24 puertos cada una, la definición de las conexiones se establece con el número de slot (ranura) / el número de puerto. Por ejemplo, la conexión entre el switch y el router WAN Principal se realiza utilizando el puerto 1 del slot 2 y se representa como 2/1.

Otro punto importante de mencionar es el uso de un *Servidor de Acceso Remoto (RAS)* modelo AS5300 de Cisco, conectado a la subred de producción. Dicho RAS da acceso al Backbone cuadrado vía Dial-up a los routers remotos. Este respaldo se utiliza en caso de que ambos enlaces a través de sus interfaces seriales 1/0 y 1/1 se vean afectados por alguna falla. La técnica empleada para enlazar a los routers remotos vía el RAS es por medio de rutas estáticas flotantes. Dichas rutas estáticas direccionan al Backbone a través de las interfaces asíncronas de los routers remotos.

En la *Figura 3.2.* se presenta la configuración de la red, en ambos sites, para las sucursales y los Intermediarios Financieros. Por motivos de espacio, solamente se representan algunos intermediarios y sucursales.

Todas las interfaces de los routers que componen al Backbone cuadrado, excepto la HSSI, emplean el protocolo de ruteo *OSPF (Open Shortest Path First / Ruta Primaria Más Corta Disponible*), mientras que la interfaz HSSI de los routers WAN, Principal y Secundario, corren el protocolo EIGRP*(Enhanced Interior Gateway Routing Protocol / Protocolo de Ruteo con Puerta de Enlace Mejorado)*

Tanto las sucursales como los Intermediarios Financieros poseen una interfaz asíncrona, que sirve como respaldo en caso de que las interfaces seriales fallen. Dicha interfaz se conecta hacia el Servidor de Acceso Remoto utilizando la línea telefónica y un modem, que es configurado para que solo pueda realizar llamadas y se conecte vía Dial-up al RAS.

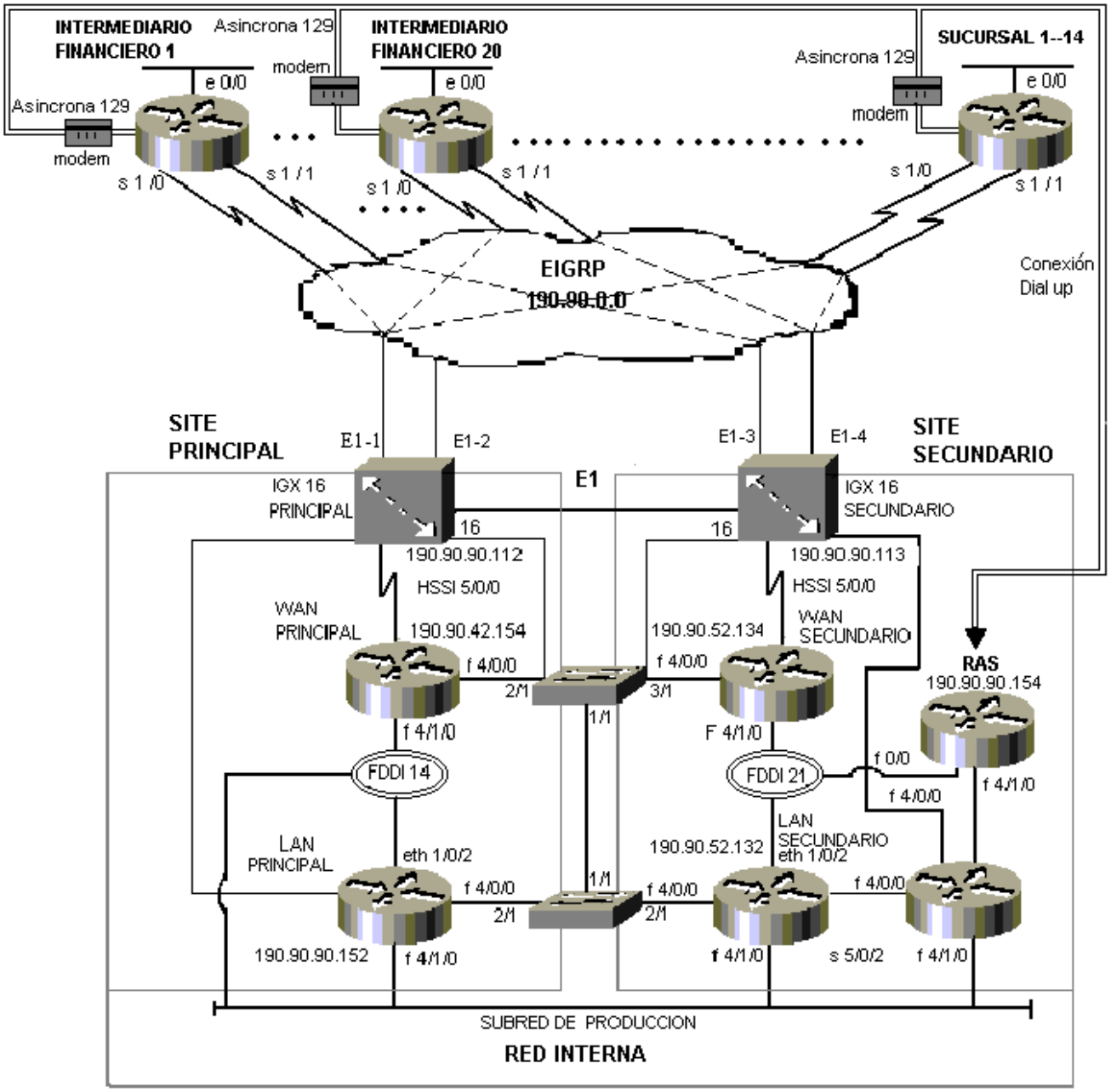

Figura 3.2. Configuración de la red en la Oficina Central.

En la *Figura 3.3.* se muestra la conexión de las sucursales hacia el Site Secundario; Cuando la conexión en las interfaces seriales falla, utiliza Dial-up para conectarse.

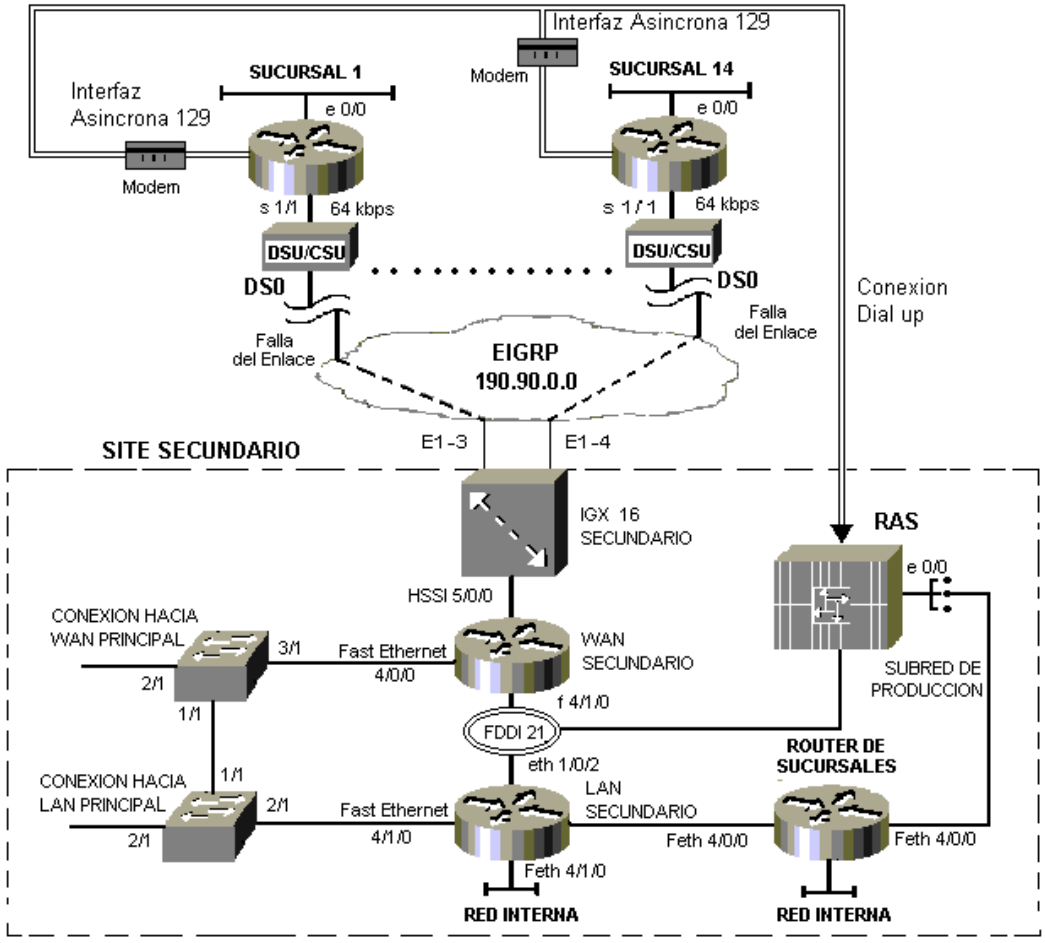

Figura 3.3. Diagrama del Dial-up a través del Site Secundario.

El Site Principal que se encuentra actualmente tiene la siguiente disposición del equipo instalado, como se muestra en la *Figura 3.4:*

1. Rack smart switch cabletron modelo 9C406 y 8600
2. Multiplexor cabletron y acometida de fibra óptica
3. Rack del megamux, y multiplexores
4. Rack de equipo de internet , routers Cisco 2610 y fuente de poder
5. Rack smart switch cabletron para telefonía.
6. *Equipo de microondas.
7. Rack Equipo de Telecomunicaciones; router cisco modelo 7200, Catalyst 6000
8. Rack de RAS 4500, router 7500VXR.
9. *Pix Firewall de Internet y equipo para internet
10. *UPS Liebert S3.
11. *UPS Liebert 6000.

12. Hubs y acometida a la sala de monitoreo.
13. Equipo de monitoreo, stratawiew, spectrum y Cisco Works
14. Estaciones de Respaldo Internet

Nota: Los equipos marcados con * no son utilizados para la Red Financiera, sin embargo se mencionan para tener una completa representación del Site.

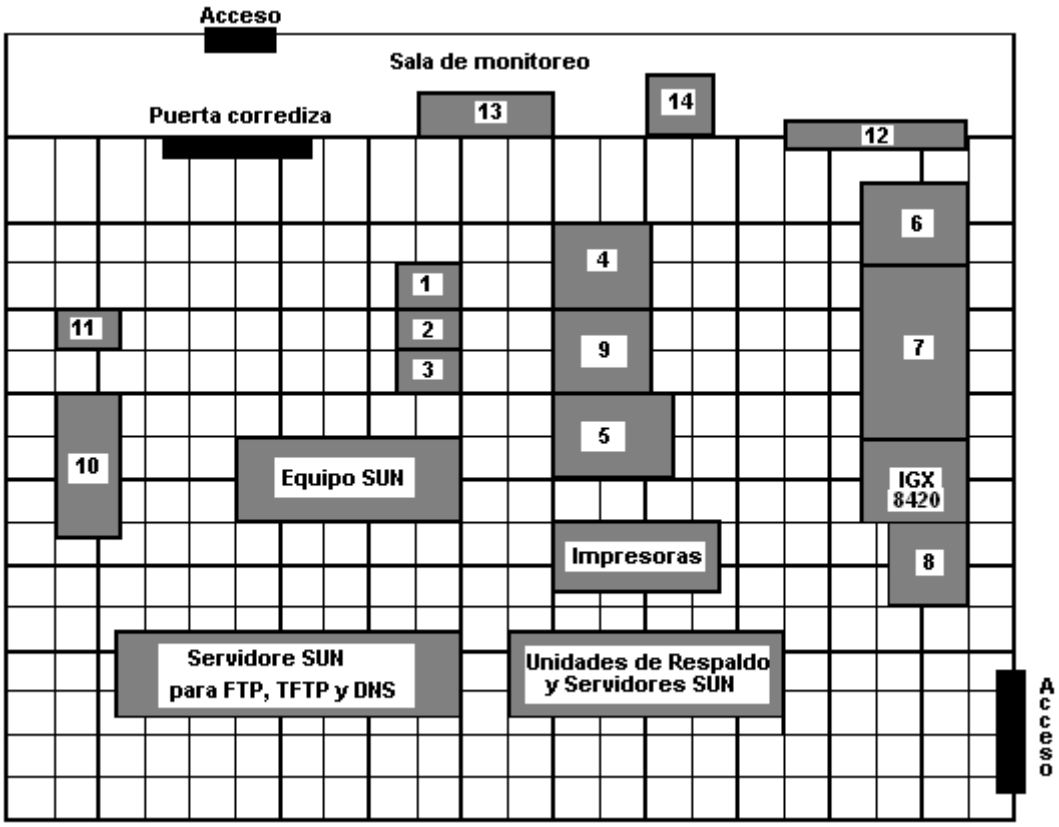

Figura. 3.4. Disposición de Equipos en el Site Principal.

Sucursales del Banco

Los equipos de comunicación que actualmente operan en las sucursales (routers, switches y hubs) son de la marca Cisco. Los modelos varían entre los Cisco 3640, utilizados como routers de operación, y Cisco 2610, utilizados como routers de respaldo. Se cuenta también con un módem, el cual se conecta a la interfaz asíncrona del router. El módem sirve como respaldo del enlace en caso de contingencia y se conecta al Site Secundario utilizando la línea telefónica vía Dial-up hacia el RAS. Dicho módem solamente pueda hacer llamadas, pero no puede recibirlas, es por ello que sólo se activa cuando encuentra tráfico interesante en el enlace, es decir, cuando se ingresa a los servicios que proporciona el Banco.

Cada sucursal cuenta con un enlace DS0 de 64 kbps, que utiliza RDI como línea de transporte. El DS0 está compuesto por un canal con portadora de 64 kbps (llamado

B) y un canal de datos de 16 kbps (llamado canal D). El canal B se utiliza para transportar señales de voz y el canal de datos sirve para señalización. El enlace DS0 se contrata con un proveedor de servicios de RDI, y sirve para conectarse al Banco.

El proveedor de servicios entrega el DS0 en un par de cobre, conectado a un *CSU/DSU (Channel Service Unit / Data Service Unit , Unidad de servicios de Canal / Unidad de Servicios de Datos)*, la conexión final al router se realiza con un cable, DB25 a V.35 que lo une con la interfaz serial del router.

El CSU/DSU es un dispositivo que protege y diagnostica las líneas de telecomunicaciones, funciona como un modem externo que convierte una trama de datos digitales provenientes de la red LAN, en tramas apropiadas para una red WAN y viceversa. El CSU recibe y transmite señales desde la WAN y provee de una barrera para la interferencia eléctrica, maneja señales de eco loopback (lazo cerrado) desde la compañía telefónica proveedora del servicio, para propósitos de prueba.

El DSU maneja líneas de control y convierte tramas de entradas y salidas usando los protocolos RS-232C, RS-449, y V.35. El DSU utiliza el multiplexaje por división de tiempo; para establecer el ancho de banda maneja tiempos de error y regeneración de la señal. El DSU funciona como un modem de interfaz entre el equipo terminal de datos (que en nuestro caso es un router) y la unidad de servicios de canal (que es el proveedor de servicios).

Los routers que forman a las sucursales del banco se conectan solamente por la interfaz serial s1/1 hacia el Site Secundario y son 14 en total.

En el Site Secundario, además de los routers, se tiene un switch Cisco modelo Catalyst 6000, que utiliza Frame Relay como tecnología de transporte y que enlaza al router de sucursales, con la interfaz HSSI del router LAN Secundario.

Las sucursales se enlazan al banco a través del IGX 16 localizado en el Site Secundario. El IGX 16 utiliza un canal E1 punto multipunto completo para conectar a todas las sucursales a la red del banco. El esquema de este tipo de conexión se puede observar en la *Figura 3.5.*

Intermediarios Financieros

Los enlaces remotos hacia la Red Financiera están constituidos por un total de 20 routers marca Cisco, instalados en los sitios de usuario. Los modelos de estos routers son cisco 3640, cuatro de estos son Wellfleet modelos: FN, AFN, AN.

Cada router remoto es propiedad de los Intermediarios Financieros, y se conectan a la red a través de dos enlaces WAN de 64 kbps, utilizando Frame Relay como tecnología de transporte. En su mayoría los enlaces son dedicados RDSI, uno se enlaza al Site Principal y el otro es conocido como Secundario o respaldo.

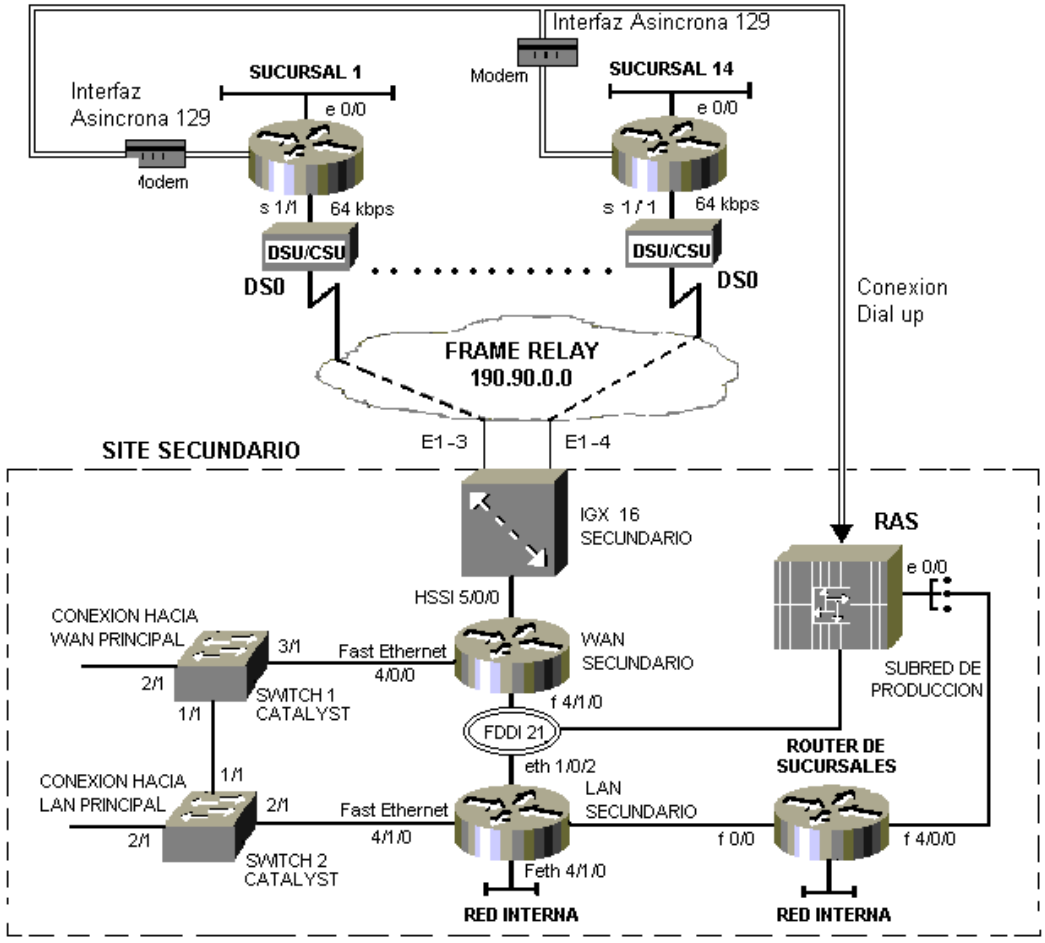

Figura 3.5. Diagrama de conexión para las sucursales.

El protocolo que se utiliza para la transferencia de información es TCP/IP y el protocolo de ruteo usado es el EIGRP, entre los routers remotos y el Backbone. Las interfaces de conexión a la red local del usuario dependen de la tecnología con que éste cuente, es por eso que hay routers Ethernet y Token Ring.

El Intercambio de tablas de ruteo con la red del usuario se basa en rutas estáticas. Las direcciones IP de los routers remotos se asignan de acuerdo a la posición que ocupan en el E1, y son direcciones de clase B, válidas en la estructura de la red.

Los routers de las Instituciones Financieras poseen un módem que sirve como respaldo y que funciona de la misma forma que el módem de las sucursales, para entrar en función en caso de contingencia.

Generalmente en los Sites propiedad de los Intermediarios Financieros se tienen descanalizadores, con varios E1's, switches, hubs y routers para otros servicios.

Sin embargo, éstos se consideran como parte de la infraestructura interna de cada institución. Algunos de los Intermediarios Financieros poseen dos canales DS0, con sus respectivos CSU / DSU, que sirven como enlace hacia las interfaces seriales 1/0 y 1/1 del router y se conectan a la red del banco usando Frame Relay.

En la *Figura 3.6,* se muestran la conexión de los Intermediarios Financieros a la red y su respaldo, que utiliza la interfaz asíncrona para conectarse vía Dial-up.

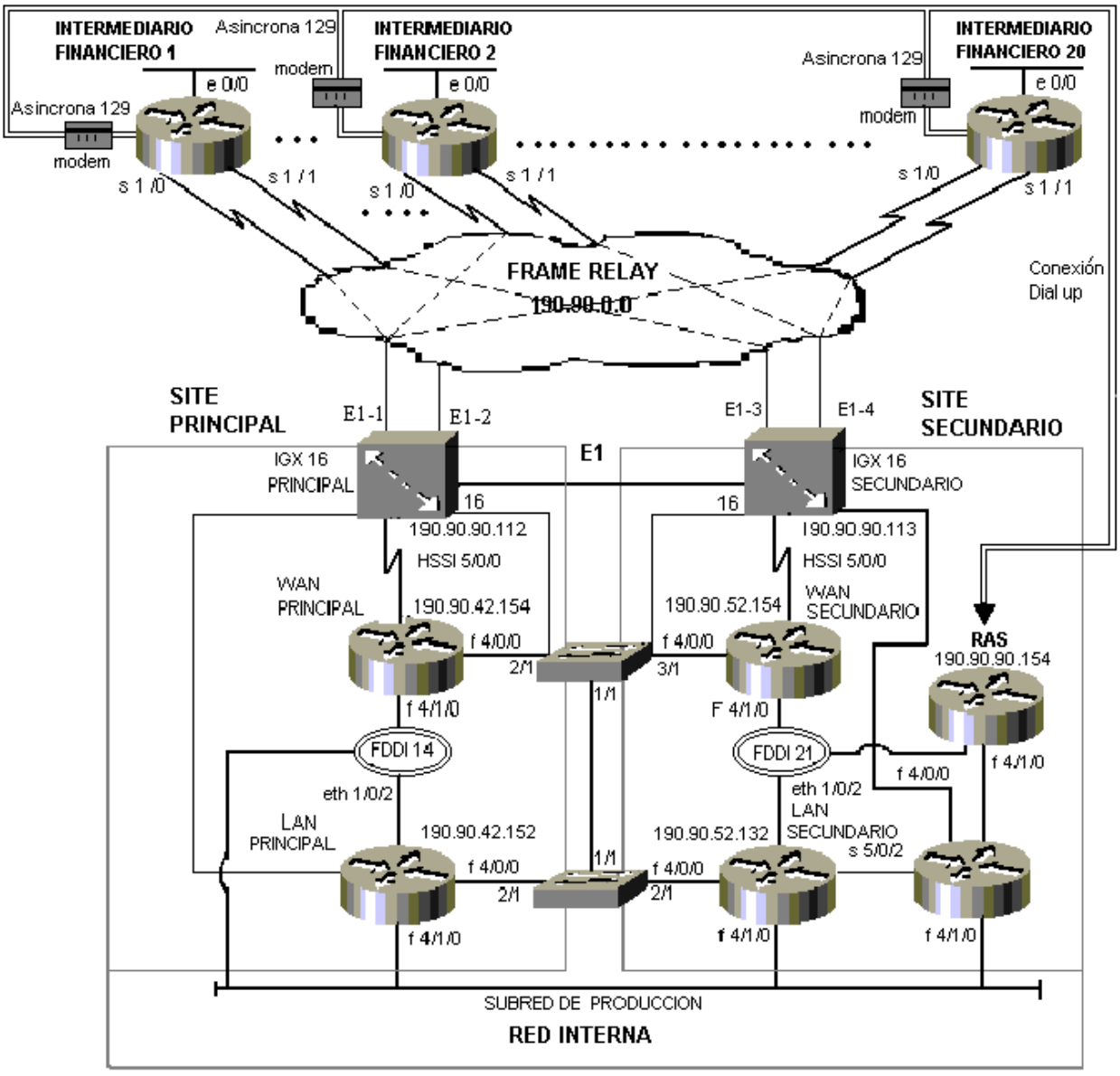

Figura 3.6. Diagrama de conexión de los Intermediarios Financieros.

Características de equipos

De acuerdo a la descripción presentada para cada elemento de la Red Financiera, procederemos a definir algunas de las características de los equipos que

conforman al Site Principal, Secundario, a las sucursales y a los Intermediarios Financieros. En cada uno de los Sites se tienen los siguientes equipos:

Descanalizador Cisco IGX modelo 8420

- Contiene cuatro E1 de 31 canales cada uno.
- Contiene 16 slots para las tarjetas que incluyen voz y datos, distribuidas como se muestra en la *Tabla 3.1.*

Slot	Tarjeta	Descripción
1	NPM	Network Processor Module (Módulo Procesador de Red): Encargada de la administración y control del IGX
2	NPM	Tarjeta redundante del sistema
11	UFM-C	Universal Frame Relay Module (Módulo Universal de Frame Relay): Tarjeta con 4 puertos HSSI.
12	UFM-C	Tarjeta redundante del sistema
13	UFM-U	Universal Frame Relay Module U (Módulo "U" Universal de Frame Relay): Tarjeta de Frame Relay con descanalizadora con 4 puertos E1 G.702.
14	UFM-U	Tarjeta redundante de slot 13
15		Tarjeta Madre
16	NTM	Network Trunk Module (Módulo de redes troncales): Tarjeta troncal para la conexión entre IGX, contiene 4 troncales.

Tabla 3.1. Tarjetas que forman el switch de Frame Relay IGX 8420.

La *Figura 3.7,* muestra las tarjetas de ruteo universales para el IGX, las cuales son colocadas en las diferentes ranuras.

Figura 3.7. Tarjetas Universales de ruteo para el Cisco IGX 8420.

Tanto en el Site Principal como en el Secundario, se tienen routers Cisco modelos 7204, con idénticas características, algunas de ellas son las siguientes:

Routers Cisco 7204

- Utiliza software de sistema operativo de Interconectividad *Cisco (Cisco Internetwork Operating System Software)* denominado IOS-RSP Software (RSP-JSV40-M), cuya versión es 11.0(9.2).
- La memoria ROM tiene un sistema de arranque denominado System Bootstrap, cuya versión es la 10.1(8)CA1.
- La memoria Flash es BOOTFLASH, y su software es (RSP-BOOT-M), cuya versión es 11.2(15)P.
- El sistema operativo es cargado en la memoria Flash y el archivo de imagen es obtenido por el sistema a través del puerto 0 del router, o slot 0. En este caso es "slot0:rsp-isv40-mz_110-9_2.bin", reiniciado a través del slot 0.
- Puede manejar el protocolo X.25 con software versión 3.0.0.

Además de estas características, en la *Tabla 3.2.* se proporcionan otros dispositivos que la caja o chasis del router Cisco 7204 contiene.

Router Cisco modelo 7204	
Cantidad	Dispositivo
1	Procesador RSP4 (R5000)
1	Memoria Ram 64 Mbytes
1	Memoria NVRAM 123 kbytes
1	SIMM de Memoria Flash de 8Mbytes
1	Tarjeta PCMCIA de 16 Mbytes
2	Tarjetas Controladoras VIP2 (Versatile Interface Processors / Procesador de Interfaz Versátil)
2	Tarjetas Fast Ethernet / IEEE 802.3
4	Tarjetas Fast Ethernet / IEEE 802.2
4	Tarjetas Seriales
3	1 Tarjeta HSSI

Tabla 3.2. Características del router Cisco 7204.

En la *Figura 3.8,* se muestra un bosquejo del router Cisco 7204, donde se pueden observar la disposición de los puertos y de los módulos que contienen a las diferentes tarjetas, también se muestra el slot 0 donde se introduce la tarjeta PCMCIA utilizada para cargar el sistema operativo.

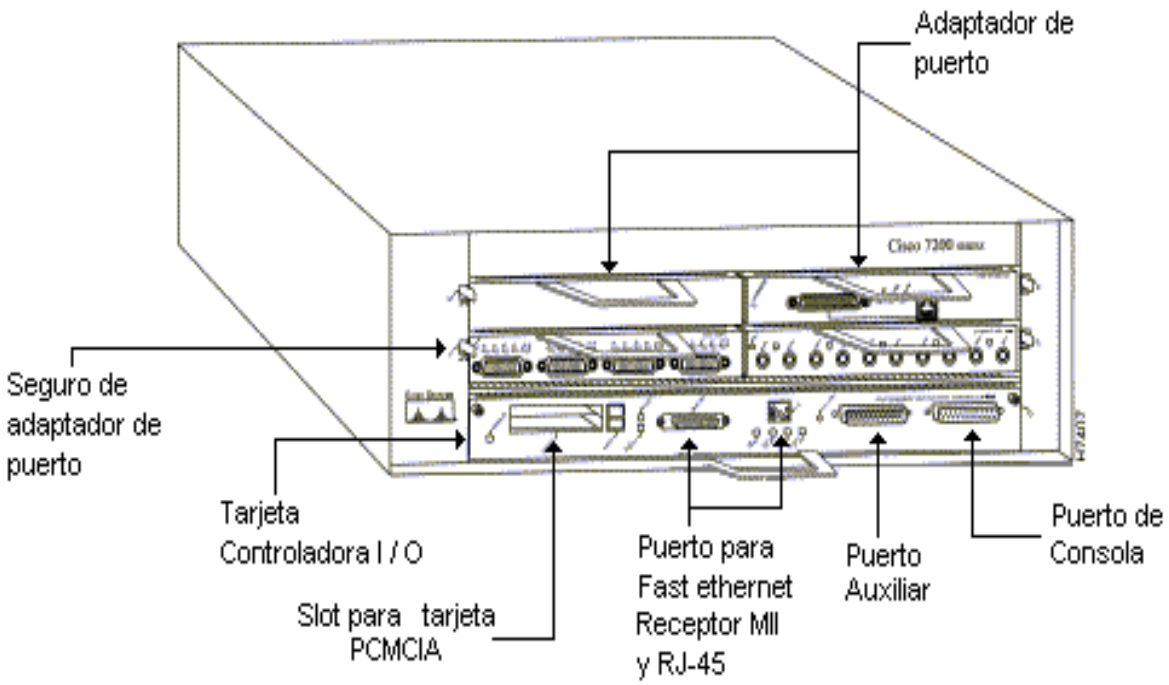

Figura 3.8. Router Cisco 7204 Vista frontal.

En la *Figura 3.9,* se muestra la disposición de los slots y puertos en el router Cisco modelo 7204.

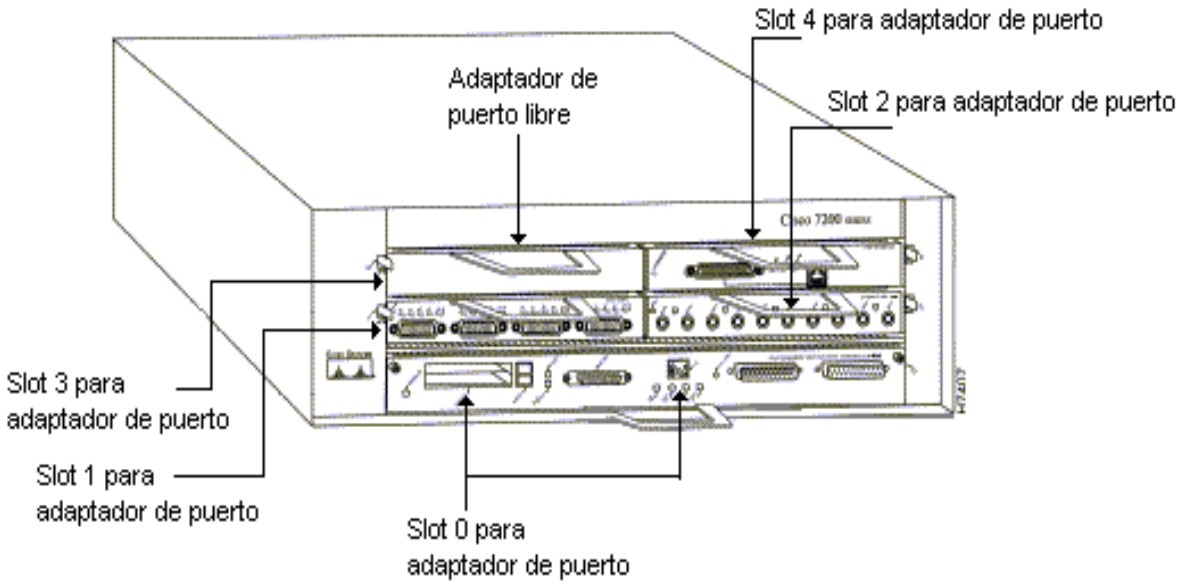

Figura 3.9. Números de slots del adaptador y el puerto.

En la *Figura 3.10,* se muestran las tarjetas Ethernet y Fast Ethernet para los distintos tipos de conectores.

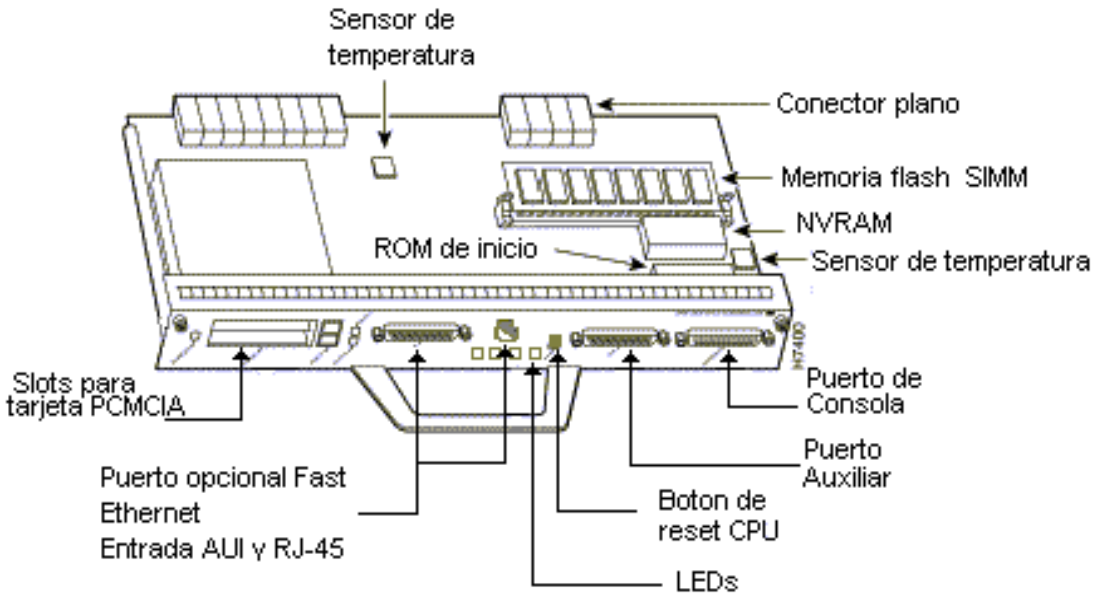

Figura 3.10. Tarjeta controladora de interfaz I/O para puerto Fast Ethernet.

El Router Cisco 7204 modelo VXR

- Tiene 4 slots para tarjetas modelo VXR, cuya versión es la 2.0.
- Maneja el protocolo X.25.
- Posee un software primario para ISDN, cuya versión es 1.1.

En la *Tabla 3.3.* se proporcionan otras características del router Cisco 7204 VXR.

Router Cisco modelo 7204 VXR	
Cantidad	Dispositivo
1	Procesador NPE 200
1	Memoria Ram 122 Mbytes
1	Memoria NVRAM 125 kbytes
1	SIMM de Memoria Flash de 4 Mbytes
1	Tarjeta PCMCIA de 20 Mbytes
1	Tarjetas Fast Ethernet / IEEE 802.3
1	Tarjeta HSSI
48	Interfaces Seriales
4	Tarjetas canalizadoras E1 / PRI, que pueden manejar voz y datos.

Tabla 3.3. Características del router Cisco 7204 modelo VXR.

Otro de los equipos que se encuentra en los Sites primario y Secundario es el switch Catalyst 6000, cuyas características se muestran en la *Tabla 3.4.*

Switch Cisco modelo Catalyst 6000	
2 Slot para insertar tarjetas de puertos	
2 Módulos de Puertos modelo WS-X6248-RJ-45	Con 48 Puertos distribuidos en cada slot
Memoria Dram	De 65 Mbytes
Memoria NVRAM	De 512 Kbytes
Memoria Flash	De 16 Mbytes
Módulo de 48 puertos para RJ-45	A 10/100 Mbps
Fuente de poder	De 1300 Watts de AC

Tabla 3.4. Características del Switch Catalyst 6000 de Cisco.

Tanto en las sucursales como en los sitios de los Intermediarios Financieros, se tienen routers Cisco modelos 3640, cuyas características se presentan en la *Tabla 3.5.*

Router Cisco modelo 3640	
Procesador R4700	integrado
Soporta protocolo X.25	sí
Sistema operativo IOS	Versión 11.1
Memoria RAM	60 Mb
Memoria NVRAM	125 kb
Memoria Flash	16 Mb
Interfaz Ethernet / IEEE 802.3	1, Puerto LAN 10/ 100 Base TX
Módulo de 4 Interfaces seriales	1
Interfaz Asíncrona	1
Puerto de Consola	1
Fuente de poder	1
Ranura para Tarjeta PCMCIA	slot 0

Tabla 3.5. Características del router Cisco modelo 3640.

En la *Figura 3.11, s*e tiene la vista frontal y posterior del router Cisco 3640.

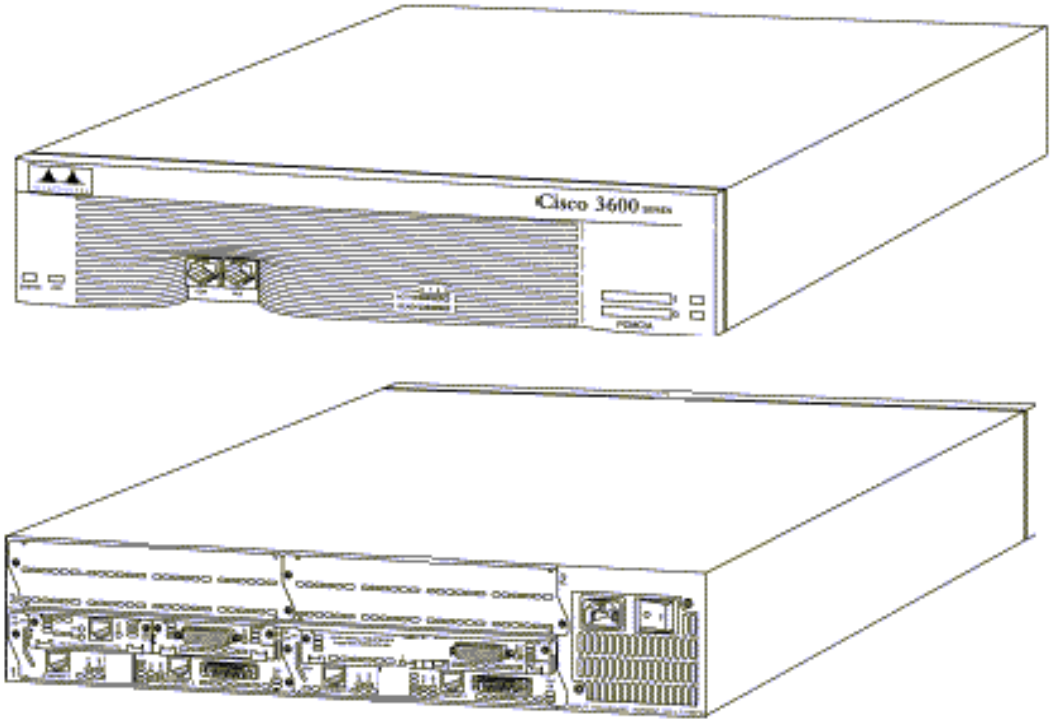

Figura 3.11. Router Cisco modelo 3640

Routers alternos

Algunos de los Intermediarios Financieros tienen routers de la marca Wellflet modelo *BLN-AN (Back Link Node - Access Node / Retorno del Nodo de Enlace - Nodo de Acceso)* y Wellflet modelo *BCN-AFN (Backbone Concentrator Node -Access Node Feeder / Concentrador nodos de canal - Fuente de Nodos de Acceso)*. Estos son concentradores de canal con multiprotocolo.

En las *Tablas 3.6. y 3.7.* se presentan algunas de sus características:

Router BCN -AFN	
Velocidad de procesamiento	700 Mbps
Memoria DRAM	416 MB
Módulo de ruteo de ATM	1
Interfaces FDDI	13 slots
Fuentes de poder	4
Puede enviar	Desde 800,000 hasta 1 millón de *pps (paquetes por segundo)*.
Requiere 1 PS (Proveedor de Servicio	Por cada 4 slots usados.
Un PS adicional	Provee la redundancia requerida.

Tabla 3.6. Características del router Wellflet modelo BCN- AFN.

Router BLN - AN	
Velocidad de procesamiento	700 Mbps
Memoria RAM	128 MB
Módulo de ruteo de ATM	1
Interfaces FDDI	4 slots
Fuentes de poder	2
Puede enviar por un nodo de canal AN (Access Node / Nodo de Acceso)	Hasta 330,000 *pps (paquetes por segundo)*.
Requiere 1 PS (Proveedor de Servicio)	Por cada 4 slots usados.
Un PS adicional	Provee la redundancia requerida.

Tabla 3.7. Características del router Wellflet modelo BLN - AN.

En las *Figuras 3.12. y 3.13* se puede ver un bosquejo de estos modelos.

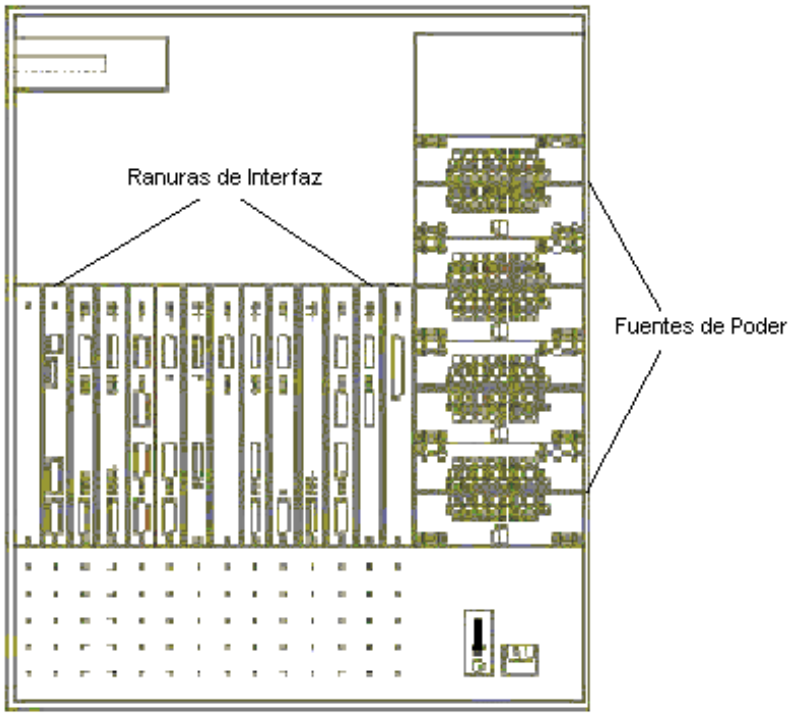

Figura 3.12. Router Wellfleet modelo BCN

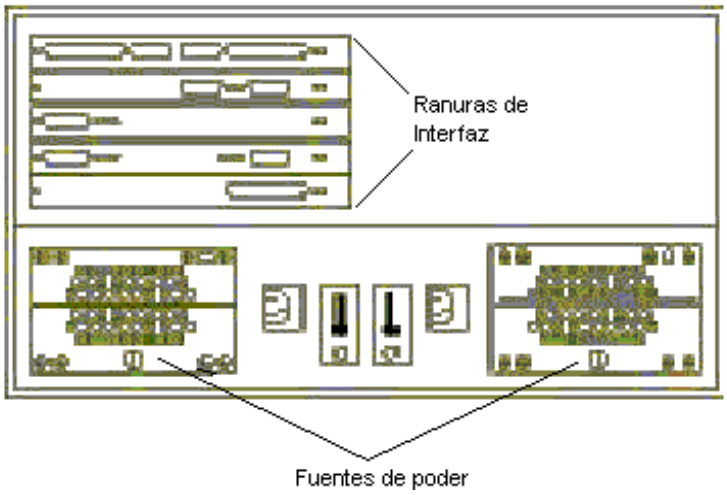

Figura 3.13. Router Wellfleet modelo BLN

3.3. Determinación de requerimientos

Tomando como punto de partida la situación actual de la Red Financiera, y las necesidades que han surgido con el paso del tiempo, así como los avances tecnológicos que imperan actualmente, concentraremos nuestra atención en la serie de requerimientos por parte del banco para el mejoramiento de su operación y la calidad de sus servicios.

La determinación de estos requerimientos se realizó en cuatro facetas, que se listan a continuación:

- Administración
- Seguridad
- Disponibilidad
- Integración de servicios

3.3.1. Administración

Debido a la naturaleza de operación de la Red Financiera, los equipos utilizados deben ser tan dinámicos como el crecimiento de las necesidades de la red, entendiendo este dinamismo como la facilidad para administrarlos y su sencillez de operación. El proyecto debe considerar las siguientes funciones:

Configuración dinámica. Cualquier modificación debe ser hecha de manera que no afecte la operación de toda la institución conectada. Con la plataforma actual, cualquier cambio (apertura de filtros de tráfico, creación de rutas estáticas, etc.) debe hacerse con un tiempo mínimo de 24 horas de anticipación, ya que es necesario reiniciar al router para que éste tome la nueva configuración,

y dicho reinicio debe ser aplicado fuera de horarios de operación (usualmente a las 23:00 hrs.).

Herramientas de administración. Al interactuar con redes heterogéneas, es necesario contar con herramientas de administración confiables, fáciles de utilizar por el personal técnico, con el fin de obtener una solución rápida al ocurrir cualquier falla.

Monitoreo. El monitoreo no sólo debe desplegar información de cómo está funcionando la Red en el momento actual, también debe mostrar suficientes datos para analizar el desempeño de la red, y con esto definir las tendencias de crecimiento que se deban aplicar a canales de comunicación o recursos de los equipos. Actualmente usa una plataforma de monitoreo basada en el sistema Spectrum de Cabletron, para administración, configuración y monitoreo.

Los equipos del sistema de monitoreo deben incluir alguna herramienta que determine si existe comunicación con un dispositivo de dirección IP determinada como el *"traceroute*" (trazo de ruta), o el comando ping.

3.3.2. Seguridad

La naturaleza de la información que se transfiere es, por obvias razones, sumamente delicada y por lo tanto la Red debe proporcionar un enlace confiable, no sólo de disponibilidad sino en el enfoque de integridad y confidencialidad de la información. Por otra parte, debido a que el banco se conecta con empresas externas, implica que en este escenario, los sistemas de seguridad sean más robustos y confiables, ya que están conectados a un usuario que si bien no tiene una función directa con el banco, cuenta con la infraestructura para lograr una conexión de importancia a las redes de información. Por la naturaleza del presente proyecto, la seguridad es el tema central, y es en el que pondremos especial interés a su solución. Los aspectos importantes que plantearemos son los siguientes:

Filtros y tablas de ruteo. Se requiere mantener el mismo esquema de seguridad y depurarlo, los filtros deben incluir más puertos de *TCP* y *UDP*. Sería deseable sólo exportar las direcciones de los *hosts* del banco y no las subredes completas como se hace actualmente.

Firewalls. Es muy importante proteger la información y toda la red de computadoras de cualquier posible ataque de los hackers. Para esto es necesario implementar un sistema de seguridad que les impida pasar dentro de cualquier enlace de la Red Financiera. Para ello se hace necesario hoy en día, instalar uno o más Firewalls que les permitan a los usuarios autorizados acceder cualquier recurso permitido de la red, pero con la seguridad de que ningún usuario no autorizado pueda hacerlo.

Encripción. Aunque se cuentan con enlaces punto a punto, el ofrecer encripción en los enlaces WAN sería una particularidad que prevendría una probable

irrupción en la información, ya que la Red descansa en enlaces contratados a una empresa diferente al banco y a sus usuarios, y muy probablemente se diversificará debido a la apertura comercial en el ramo de comunicaciones que se está dando en el país. Este esquema de seguridad debe ser soportado para cualquier canal de comunicación, incluyendo los enlaces de respaldo. En materia de criptografía, implantar una solución que abarque el ambiente de infraestructura de red, indicando la tecnología más apropiada para el esquema de la Red Financiera.

Esquema jerárquico de passwords. Actualizarse con un mayor número de niveles jerárquicos, ya que actualmente sólo se cuentan con dos niveles de passwords, uno de ellos con demasiados privilegios *(manager / administrador)* y el otro muy limitado *(guest / usuario)*, de tal manera que los técnicos encargados de dar solución a algún problema no cuentan con las herramientas suficientes para diagnósticos rápidos y confiables.

Control de acceso. Se requiere que personal técnico tenga acceso a los *routers* remotos para diagnosticar algún problema. Este personal debe utilizar la mayoría de las herramientas de administración que ofrezcan los equipos, sin tener privilegios para modificar configuraciones o reiniciar al *router.* Se deben garantizar las políticas de seguridad que controlen las rutas de acceso a redes y computadoras dentro del banco.

Autentificación. Se requiere un esquema robusto para controlar el acceso de los administradores de la red, asegurando que quien se conecte a los equipos es en realidad quien dice ser. También que se autentifique cualquier intento de conexión a los mismos *routers*, ya sea por Telnet, *TFTP (Trivial File Transfer Protocol / Protocolo de Transferencia de Archivos Trivial)* o con agentes *SNMP (Simple Network Management Protocol / Protocolo de Administración de Red Simple)*. Sería deseable que se establezca un esquema de autentificación para los enlaces conmutados de respaldo.

Auditoría. Todas las conexiones de cualquier administrador de routers deberán anotarse automáticamente en una bitácora, verificando quien se conectó, a qué hora y qué realizó dentro del *router*. También deberán incluirse eventos importantes como pérdida de conexión, algunas alarmas menores que puedan afectar a largo plazo, etc.

Seguridad de configuración. La totalidad de los *routers* remotos son administrados por el Banco, cualquier modificación a la configuración es responsabilidad de esta Institución. La mayoría de los routers instalados almacenan su sistema operativo y su configuración en discos flexibles de $3^1/_2$ pulgadas y con formato DOS. Este disco puede ser sustraído por cualquier persona y ser modificado. Aunque los actos vandálicos directos a routers son normalmente remotos, cabe esta posibilidad y lo deseable es que los equipos cuenten con la seguridad física necesaria.

3.3.3. Disponibilidad

Se necesita que la información requerida, por parte de los usuarios, sea proporcionada sin problemas en el momento en que estos así lo requieran. Por lo tanto, se deben prever soluciones validas para resolver situaciones entre las que se destacan:

Direccionamiento dinámico de los enlaces. Son varias las instituciones que cuentan con dos o más domicilios diferentes con conexión al banco. Una de las preocupaciones de estas instituciones es la de contar con un respaldo activo en caso de pérdida de enlace, utilizando cualquiera de sus domicilios, sin que el usuario note interrupción de servicio. Obviamente se requerirá manejar algún protocolo de ruteo en la interfaz a la red local de cada usuario, interactuando con routers de diferentes marcas.

Respaldo. Los esquemas manejados hasta ahora han dado un buen resultado al contar con un esquema de respaldo de los equipos, lo que permite ofrecer un alto porcentaje de disponibilidad a los usuarios, pero se requiere un puerto WAN extra en los *routers* remotos, para un canal de respaldo a través de líneas conmutadas o de un proveedor diferente al ya contratado. En el caso de una línea telefónica, sería deseable que el módem estuviera integrado al equipo; si el módem es externo, este equipo debe considerarse como parte integral del hardware del proyecto.

Interfaz. Los equipos centrales de comunicación deberán contar con la interfaz apropiada para la conexión LAN del banco y a través de ella mantener el esquema de respaldo a las conexiones de los hosts de producción. Si el esquema se establece con algún proveedor de enlaces digitales permanentes, la interfaz extra deberá soportar la misma configuración que las de operación normal. Cualquiera que sea la solución, deberá mantener los esquemas de seguridad ya mencionados, además de agregar los que se requieran por la naturaleza de los enlaces de respaldo.

Redundancia. Los equipos centrales de comunicación (routers y switches) deberán tener todas las características de redundancia, que se puedan establecer para mantener un nivel de disponibilidad adecuado a la Red Financiera.

3.3.4. Integración de Servicios

La integración de servicios involucra necesidades conjuntas, como compartir recursos, acceso instantáneo a bases de datos, insensibilidad a la distancia física y a la limitación del número de nodos, administración centralizada, etc., con el único propósito de tener la ventaja estratégica en el mercado competitivo global. Por lo tanto, se proporciona, a través de esta integración de servicios, la información dentro de un mismo ambiente.

La integración de servicios debe satisfacer las necesidades de información del usuario y permitirle manejar una amplia gama de servicios de una manera mucho más interactiva. Así, el compromiso de la red Financiera de proporcionar un mejor servicio y la necesidad de mantenerse mejor, se hace cada vez más latente.

La red Financiera no vende tecnología, vende servicios y se utiliza la tecnología como medio para proveerlos. Es así como el servicio a los usuarios necesita perfilarse como un factor fundamental a considerar en la provisión del mismo.

Muchas opiniones pueden nacer a partir de esta consideración y desde luego que muchos factores entran en juego. La decisión final debe ser tomada estudiando los sistemas de transporte existentes con base en las necesidades y requerimientos de los usuarios.

Lo cierto es que cada servicio implica un costo adicional y que integrar nuevas tecnologías e implementarlas puede generar en un principio pérdidas económicas considerables. Por ello se necesita un correcto estudio para determinar las tecnologías a usar. Es muy importante tomar en cuenta que la infraestructura de cualquier sistema no sólo debe de construirse, sino también renovarse y mantenerse, y que el servicio al cliente es hoy en día un punto a favor para garantizar el incremento y la permanencia de los usuarios.

Por ahora dos puntos de suma importancia hay que considerar. En primer lugar la tecnología que se decida adoptar debe ser simple, fácil de usar y a prueba de fallas. En segundo término, es esencial que se cuiden los servicios que serán proporcionados al consumidor, su valor y el control de su contenido. De esta forma la red Financiera otorgará servicios competitivos y sus clientes estarán satisfechos.

Para lograr estos objetivos, será necesario buscar las alternativas que van surgiendo conforme avanza la tecnología. Uno de estos avances son las VPNs o redes privadas virtuales, que nos permiten enlazar lugares distantes a través de Internet, con lo que los costos de comunicación se ven muy reducidos, mientras que la facilidad para lograrla se realiza de manera muy sencilla.

3.4. Posibles soluciones

Las soluciones propuestas parten de los requerimientos de la red Financiera y para un mejor estudio y análisis las dividimos en soluciones de cuatro tipos:

- Administración
- Seguridad
- Disponibilidad
- Integración de servicios

3.4.1. Soluciones de Administración

Se efectuará una discusión minuciosa para lograr los objetivos de facilidad de administración y rapidez, para lo cual se considerarán funciones en los equipos que cumplan con:

Direccionamiento dinámico de los enlaces. Se deberá contar con el equipo que nos permita redireccionar los enlaces, de manera transparente, a otro que esté funcionando, lo anterior en caso de que alguno falle.

Configuración dinámica. Los equipos que utilicemos deberán cumplir con este punto, ya que se utilizarán herramientas dinámicas, esto es que operarán sin la necesidad de esperar a ser reiniciados para cambiar su configuración.

Monitoreo. Los equipos de monitoreo tendrán la capacidad para realizar las funciones de control, actualización y respaldo de las bases de datos, configuraciones y revisión del funcionamiento de los equipos conectados a la red. Esto nos permitirá analizar el comportamiento de la red.

Planeación a Futuro. Los equipos de red serán modulares y dimensionados de tal manera que el sistema pueda crecer en aspectos como:

1. Número de usuarios.
2. Capacidad de canales para cada usuario.
3. Tráfico sobre los canales actuales.
4. Capacidad de memoria de los routers, especialmente de los remotos, para soportar versiones futuras del sistema operativo de esos equipos. Buscar que los equipos tengan capacidad de crecimiento en memoria, a fin de satisfacer el requerimiento de tiempo de vida.
5. Tarjetas de expansión según las necesidades.

3.4.2. Soluciones de Seguridad

La seguridad es el tema primordial de nuestro proyecto y es el que trataremos más a fondo. Entre lo que se planea es establecer un sistema de red de seguridad al acceso remoto a la red financiera, de tal modo que se cumpla con las especificaciones requeridas por parte de los usuarios. Algunos de los factores que se tratan son:

Filtros y Tablas de Ruteo. Los equipos que se instalarán deberán contemplar la posibilidad de incluir filtros y tablas de ruteo, más puertos TCP y UDP.

Encripción. Se requiere incorporar equipo diseñado para encripción y desencripción de información, que nos brinde la seguridad de que en los tramos no protegidos, por donde viaja la información, nadie pueda conocer o alterar los datos. El incluir equipos con estas características nos ayudará además de la seguridad, a que la información fluya con rapidez a través de ellos.

Sistema Jerárquico de Passwords. Se considerarán dos niveles básicos de usuarios, dependiendo de su tecnología de conexión a la red.

- **Nivel 1**.- Usuarios con doble acometida digital dedicada. A este nivel pertenecen Bancos, Casas de Bolsa, entre otros. Adicionalmente estos usuarios tendrán un enlace de respaldo. Por ejemplo, usuarios privilegiados tendrán canales del tipo E1, otro tipo de usuario tendrán canales E0, etc. Esta característica deberá ser considerada dentro del crecimiento de los equipos routers y los cambios que implicaría para el esquema completo de la Red.

- **Nivel 2**.- Usuarios con acceso por línea telefónica conmutada o similar. A este nivel pertenecerán:

    a) Usuarios ubicados en lugares donde no se cuente con infraestructura de canales digitales.
    b) Usuarios con recursos económicos limitados.
    c) Usuarios Intermediarios Financieros menores que transmitan volúmenes de datos pequeños, como: aseguradoras, arrendadoras, empresas de factoraje y almacenes generales de depósito.

Control de acceso. Para cumplir con las políticas de seguridad y controlar las rutas de acceso a la red del banco, se considerará una configuración de filtros de servicios TCP, como por ejemplo Telnet, TFTP introduciendo Firewall, tanto en la parte de red correspondiente al banco como en la entrada de los usuarios remotos.

Autentificación. El enlace de respaldo se conectará y autentificará a través de un RAS localizado en el Site Secundario. El enlace desde las Instituciones Financieras sólo será habilitado manualmente cuando se requiera, previa solicitud y autorización de las oficinas operadoras del banco, con el fin de evitar que alguien no autorizado, dentro de la empresa, tenga acceso a las redes de producción. Aprovechando los equipos de respaldo se desarrollará un sistema de autentificación para los enlaces conmutados, el cual manejará el *PAP (Password Autentification Protocol / Protocolo de Autentificación de Contraseña)* y *CHAP (Control Handshake Autentification Protocol / Protocolo de Autentificación y Control de Reconocimiento)*, que permitirá restringir el acceso sólo a quién esté permitido.

Auditoría. Se debe incorporar algún equipo o programa que nos permita verificar en cualquier momento, qué personas accedieron y/o modificaron la configuración de cualquier equipo crítico, como los routers. También debe identificar eventos como la pérdida de conexión.

Firewall. Es muy importante incluir un esquema de protección contra personas no autorizadas a través de los enlaces. Para ello se debe incluir uno o más Firewalls, que sean compatibles con la tecnología que se está incorporando.

Seguridad de la Información. Se debe incluir un sistema de seguridad física para los equipos, además de un sistema que impida que personal no autorizado tenga acceso a la configuración de los equipos, ya sea a través de contraseñas de seguridad, o que la configuración de los equipos no pueda ser accesada de manera directa.

3.4.3. Soluciones de Disponibilidad

Se dispondrá de routers y switches que operen en Frame Relay y que posean todas las características de redundancia que se puedan establecer para mantener un nivel de disponibilidad adecuado a la red Financiera.

Respaldo dinámico. Se contará con un sistema de respaldo, que contenga no sólo dos enlaces seriales en el router, sino que también tenga un modem conectado a su puerto auxiliar para contingencias, en caso de que ambos enlaces queden fuera de servicio. La conexión del router a través del modem se le conoce también como conexión Dial-up y se enlazará a la Oficina Central utilizando una línea telefónica. El enlace desde la diferentes instituciones al banco será un E0 punto a punto, por lo tanto siempre estará activo, con lo que se pretende disipar pérdidas de enlace.

Interfaz. Todos los equipos de comunicación deberán tener la posibilidad de crecer en tarjetas o accesorios que nos ayuden a proveer la comunicación sin descuidar la seguridad. Deberán ser escalables, tanto en hardware como en software, y deberán accionarse de manera automática y transparente para los usuarios.

Redundancia. La Red Financiera deberá contar con un esquema de redundancia, para que en caso de contingencia no se interrumpa la comunicación, sino que se tomen caminos alternos de manera automática, sin salirse del esquema de seguridad que se está planteando. Para esto se utiliza el Backbone cuadrado, así que este esquema deberá conservarse al final del proyecto.

3.4.4. Soluciones de Integración de servicios

Dos son los factores que un proveedor de servicios debe tener en cuenta. El primero está relacionado con la infraestructura necesaria para hacerlos llegar al hogar u oficina del usuario y el segundo consiste en determinar qué servicios son viables de ofrecer a través del sistema e infraestructura con que se cuenta. Es necesario caminar paso a paso, ofreciendo primero algunos de los servicios que pueden habilitarse.

La integración de servicios es quizás el proceso que toma más tiempo, puesto que éste debe ser gradual. Se deben evaluar extensamente los sistemas para asegurarse de la integración de servicios antes de sacar estos al mercado. Al usuario se le debe explicar de qué se trata esta integración para poder convencerlo y posteriormente instalarle el servicio. La mejor forma de integrar estos servicios es hacerlos simples y fáciles de usar. Además, la naturaleza de la información que se maneja en la red financiera permite que existan diferentes niveles de servicio y que el usuario pueda elegir los que más le convengan.

El mejor protocolo para manejar Servicios Integrados es el IP, por el ancho de banda ilimitado y bajo costo que maneja. Este protocolo es el que será utilizado en este proyecto. De lo que se trata es que el usuario no requiere tener idea alguna de cómo se genera el servicio, o las diferencias entre redes de conmutación de circuitos (como la red telefónica convencional) y redes de conmutación de paquetes (como Internet). Su única preocupación consiste en tener la información en el momento que lo necesiten, especialmente durante emergencias y fallas en la energía eléctrica. Las redes sobre IP ofrecen muchas más aplicaciones de lo que puede ofrecer la conmutación de circuitos.

Existen varios factores que deben ser tomados en cuenta para elegir la mejor tecnología y así lograr el objetivo de Integración, entre ellos destacan:

- Reducción de presupuestos (tiempo, dinero).
- Capacidad de planeación, administración y soporte.
- Retos técnicos y retos de administración de redes.
- Equipos de diferentes fabricantes.
- Arquitecturas, plataformas, sistemas operativos, protocolos, medios de comunicación diferentes.
- Limitaciones en distancia y en tamaño de los paquetes.
- Limitaciones en ancho de banda y potencia.

Para lograr la integración, las redes requieren diferentes tasas de transmisión, prioridad de los datos y niveles de servicio. Estas a su vez tienen diferentes presupuestos disponibles para conexiones en redes WAN. Afortunadamente, existe una gran variedad de servicios brindados por el Proveedor de Servicios de Telecomunicaciones (ejemplo: Telmex, Avantel, Axtel, Telcel, SatMex), y que son posibles soluciones a la Integración de Servicios.

Uno de los puntos principales de este proyecto es ofrecer un alto porcentaje de disponibilidad a los usuarios, tomando en cuenta que la red debe ser segura, confiable y responder a los requerimientos establecidos. Para lograr tal objetivo se ha visto la necesidad de actualizar los dispositivos con que cuenta la institución y definir que elementos de la infraestructura establecida nos sirven en el nuevo sistema. Dicha disposición será presentada en el siguiente capítulo.

CAPÍTULO 4

DESARROLLO DE LA SOLUCIÓN

En este capítulo se desarrolla la solución que se aplicará a la Red Financiera, para corregir las anomalías presentes y dejarla funcionando en óptimas condiciones, tanto de seguridad como de desempeño.

4.1. Proceso de Seguridad en la Red

Uno de los puntos más importantes que tiene que ser mejorado en la Red Financiera, es lo referente a tener redes seguras, por lo que en este desarrollo, y de acuerdo a la información obtenida en el capítulo anterior, se establecen algunos puntos para lograr este objetivo.

El flujo de la información en su estado actual se muestra en la *Figura 4.1,* tanto para las Sucursales como para los Intermediarios Financieros. En el caso de las Sucursales se observa que después de entrar al IGX Secundario, se cuestiona si se trata de una Sucursal la que requiere el acceso, en caso de ser positivo inmediatamente pasa al router de Sucursales, del router de Sucursales al router LAN Secundario y de ahí a la Red Interna. En el caso de que sea un acceso remoto vía modem para una Sucursal, se accesa por el RAS, se autentifica y pasa al router de Sucursales, de ahí al router LAN Secundario y a la Red Interna.

El camino que sigue cuando no se trata de una sucursal es un poco diferente, ya que los Intermediarios Financieros cuentan con enlaces hacia el IGX Principal y Secundario, y en algunos casos con un router de respaldo que se conecta al Site Principal. Por lo tanto, al intentar acceder al Site Secundario y preguntar si se trata de una Sucursal, la respuesta es negativa y se procede hacia el router WAN Secundario; tanto el router WAN Secundario como el router LAN Secundario, se comunican con los router WAN y LAN Principal, respectivamente; a través de switches descritos en la *Figura 4.1*, donde los switches 1 enlazan a los routers WAN y los switches 2 enlazan a los routers LAN. Estos switches están interconectados de tal forma que uno sea respaldo del otro. Enseguida pasa a la red LAN del Site Secundario y finalmente llega hasta la Red Interna.

Cuando se trata de un acceso vía Site Principal el flujo pasa por el IGX Principal, por el WAN Principal y por la LAN Principal hasta llegar a la Red Interna. Para el acceso vía modem de un Intermediario, el proceso que sigue es el siguiente: una vez que pasó por el RAS y se autentificó, se cuestiona si es Sucursal o no, y como no lo es, pasa a ser cuestionado nuevamente si la IP es válida. Si la IP no está validada, la conexión termina, en caso contrario procede a la Red Interna. Por último, si llegara a fallar cualquiera de los enlaces anteriores, entra en operación el respaldo del Intermediario, que se conecta a través del Site Principal pasando por el IGX, siguiendo por la WAN y LAN Principales antes de acceder a la Red Interna.

Una vez que se ha visto en el diagrama a bloques del flujo de información, en la *Figura 4.2,* se muestran los equipos que realizan tales tareas, así como su conexión actual con los routers y las tarjetas que contienen. Del mismo modo se muestran las direcciones IP que utilizan tanto los routers como el IGX.

Como puede observarse, no existe un medio para tener seguridad en los datos enviados y recibidos, por lo que el sistema está propenso a ser atacado por intrusos, que puedan dañar la información proporcionada por el banco, ya que sólo se tiene el

router WAN y en él no se autentifican a los usuarios, éste sólo limita la entrada a través de las listas de acceso y puede ser vulnerada fácilmente por un hacker experto.

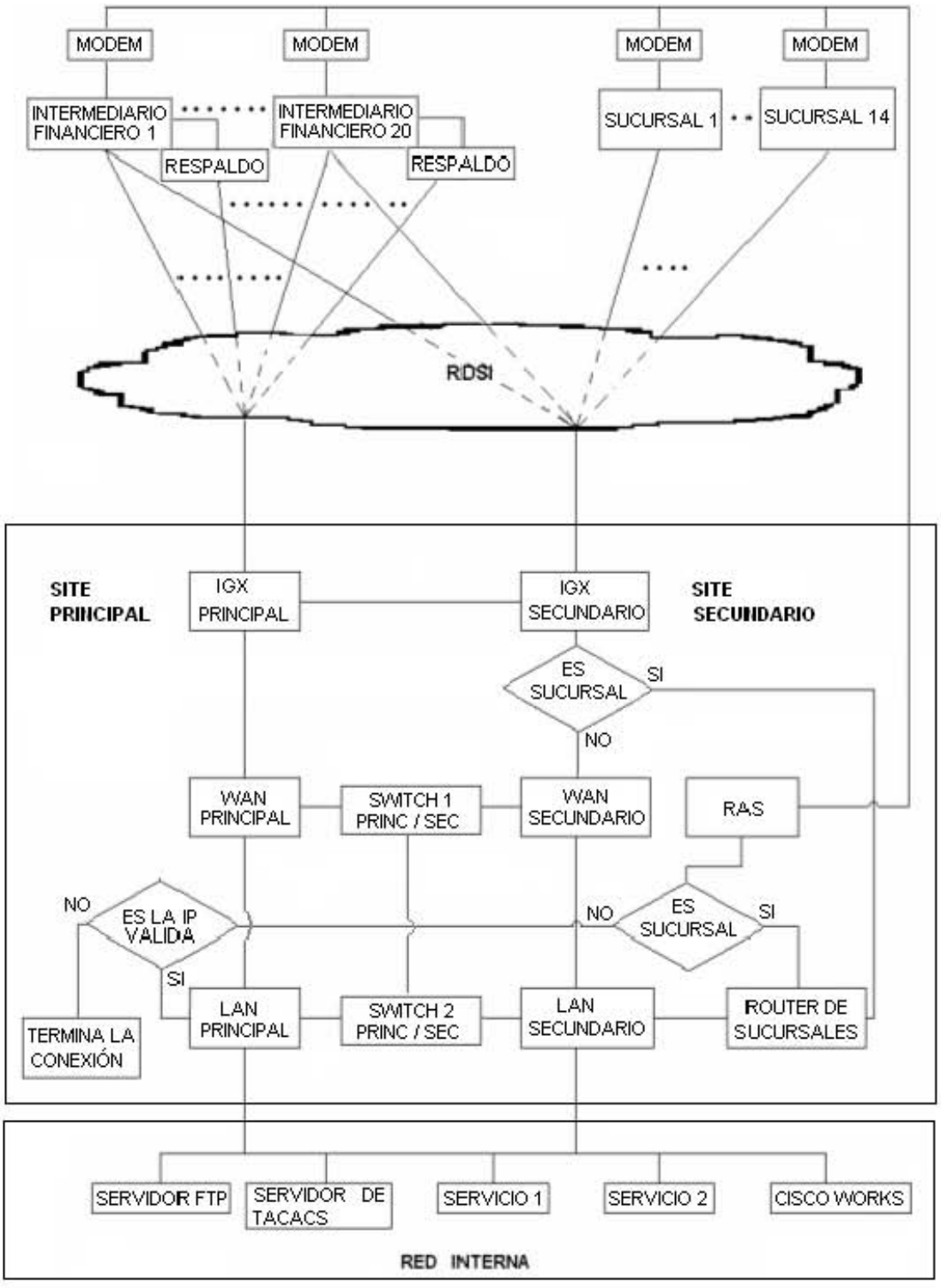

Figura 4.1. Diagrama a bloques de la estructura actual de la red

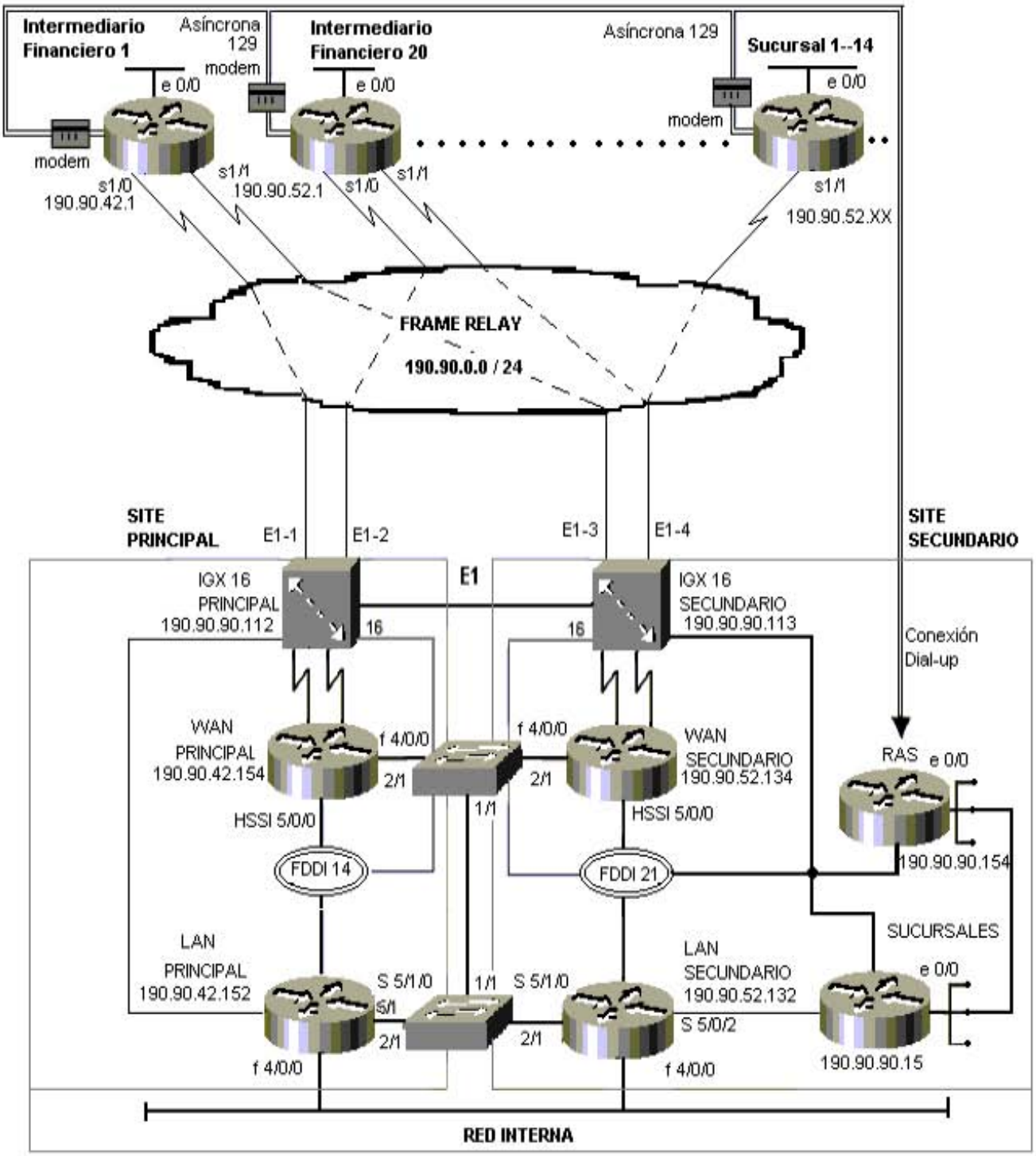

Figura 4.2. Conexión actual de la Red Financiera.

Con base en la información presentada, nuestra propuesta de solución se basa en utilizar un método de encripción de datos que ayude a proteger dicha información, transformándola de tal manera que los datos enviados no puedan ser interpretados aún cuando sean interceptados por algún intruso que quiera acceder a la red.

Como se observo en la estructura anterior de la red, no se contaba con un router para realizar dicha encripción. En la presente propuesta se establece la necesidad de contar con este equipo para que realice el proceso de encripción.

Es cierto que se podría utilizar la infraestructura que se tiene actualmente con los routers WAN y agregarle una tarjeta de encripción, pero esto también aumentaría el tiempo de procesamiento y por consiguiente existiría lentitud en el enlace. Por esta razón, se propone agregar un router, que se encargue exclusivamente del proceso de encripción.

La encripción y desencripción de paquetes ocurrirán únicamente en los routers que se configuren para ello.

Los routers que se encuentran en los saltos intermedios no participan en el proceso de encripción y desencripción. Frecuentemente los routers de encripción se sitúan en los bordes de las redes inseguras, de tal manera que proporcionen una comunicación segura entre dos redes protegidas que están físicamente separadas.

Para tener una mejor idea de dónde estaría situado dicho router de encripción, en la *Figura 4.3,* se muestra un diagrama a bloques donde se determina su posición.

Habrá un router en cada uno de los Sites de la Red Financiera, los cuales soportarán la encripción de los datos que lleguen desde los routers remotos, a través del switch de Frame Relay, representado por el IGX 16, tanto en el Site Principal como en el Secundario.

La conexión final con el router de encripción en ambos Sites de la Red Financiera quedaría como se muestra en la *Figura 4.4*, donde se establece su conexión con los routers WAN Principal y Secundario respectivamente. También se define la conexión hacia el switch de Frame Relay IGX 16, que es por donde arriban los datos desde las sucursales y desde los Intermediarios Financieros.

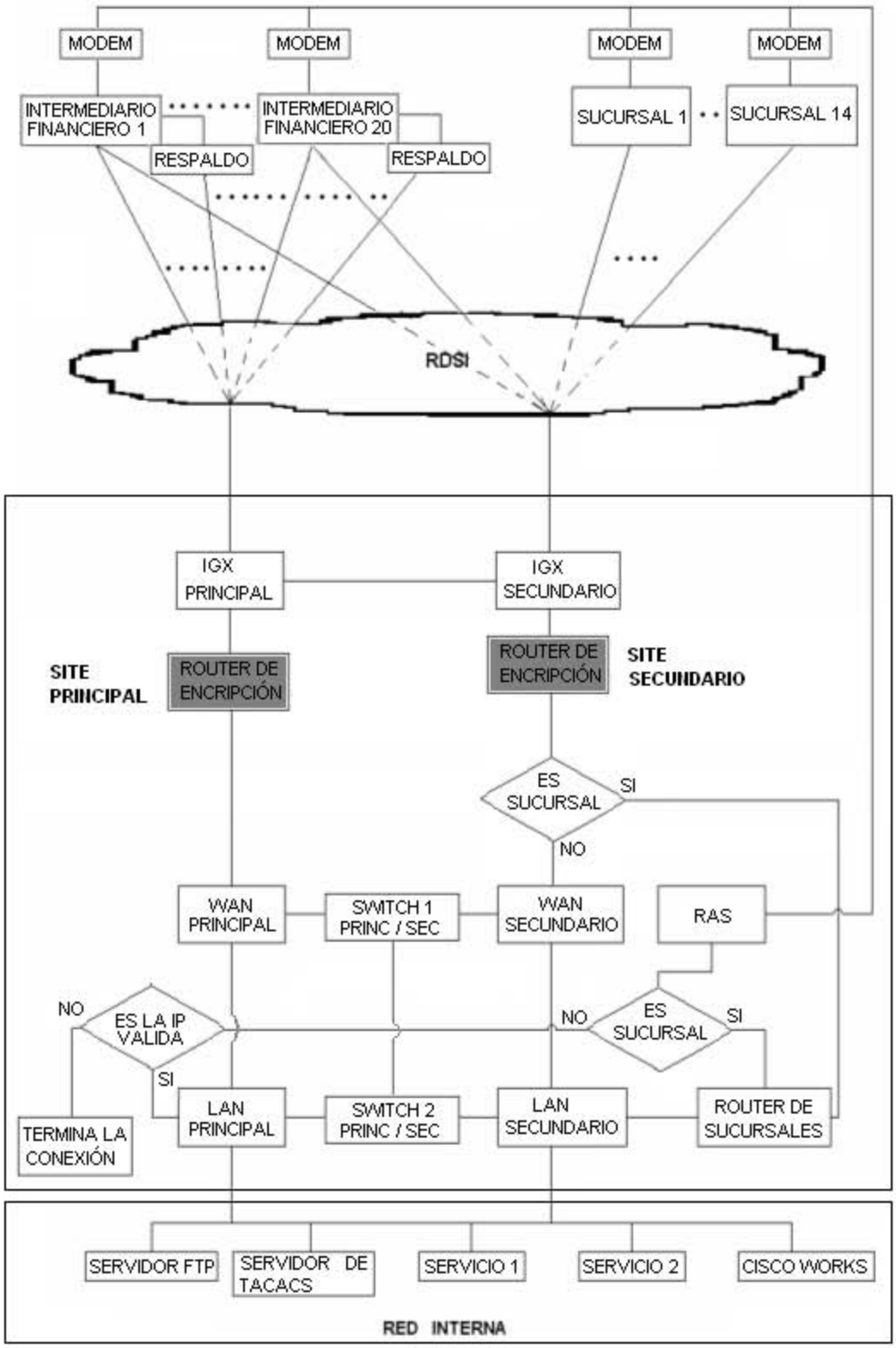

Figura 4.3. Diagrama a bloques de la red con el router de encripción.

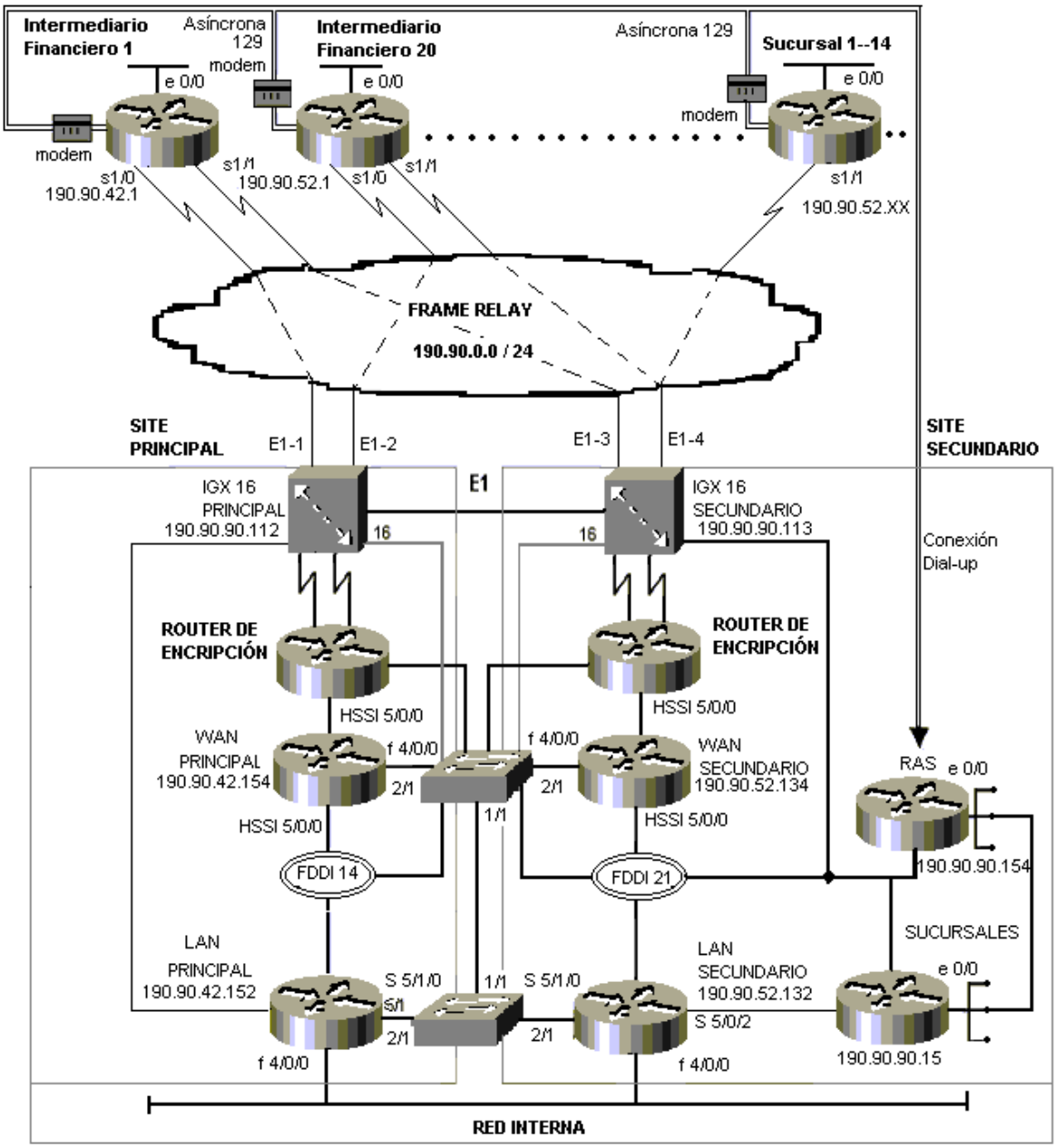

Figura 4.4. Conexión Propuesta para Generar la Encripción de la Red.

Una vez definidos los puntos donde será aplicada la encripción en la red, el siguiente paso será seleccionar el router adecuado para tal propósito. Para el criterio de selección del router de encripción, se realizó un estudio de mercado con tres diferentes proveedores de equipos, cuya comparación de características técnicas más significativas se presentan en la *Tabla 4.1.*

Router			
Marca	**Cisco**	Nortel-Bay Networks	Lucent Technologies
Modelo	**7204**	ASN2	Super Pipe 175
Modular	SÍ	SÍ	NO
No. de puertos WAN	16	14	15
Expansión a 24 puertos WAN	SÍ	SÍ	NO
No. puertos LAN RJ45	4	2	1
Ranura para encripción	SÍ	SÍ	NO
Doble fuente para redundancia de alimentación	SÍ	SÍ	SÍ
Interfaz V.35, RS-232/V24, RS530	SÍ	SÍ	SÍ
Cuenta con 10 puertos seriales de 64 kbps-2Mbps	SÍ	SÍ	SÍ
Cuenta con módulo de 4 puertos seriales de 64 kbps	SÍ	SÍ	NO
Protocolo IP	SÍ	SÍ	SÍ
Encapsulado HDLC	SÍ	SÍ	SÍ
Encapsulado PPP	SÍ	SÍ	SÍ
Encapsulado Frame Relay	SÍ	SÍ	SÍ
Encapsulado BRI de RDSI	SÍ	SÍ	SÍ
Respaldo por RDSI	SÍ	SÍ	NO
No. de Tarjetas RDSI	4	1	NO
Administración SNMP	SÍ	SÍ	SÍ
Software configuración W95 y WNT	SÍ	SÍ	SÍ
Actualización de sofware	SÍ	SÍ	NO
Plataforma de control y monitoreo compatible	SÍ	SÍ	No, plataforma Lucent´s Navis Access
Garantía y Soporte Técnico las 24 horas , tiempo de respuesta 2 horas	SÍ	SÍ	SÍ
Aplica sustitución de piezas por garantía	SÍ	SÍ	SÍ
Certificado conectividad	NO	NO	SÍ
Valor	$40,501.61	$10.684,00	$25,568.00

Tabla 4.1. Características de routers de diferentes proveedores.

De acuerdo a la información descrita en la tabla anterior, la diferencia entre los routers radica en que el router de marca Cisco tiene mayor número de puertos WAN, LAN y tarjetas RDSI, comparadas con los routers de las compañías Nortel-Bay Networks y Lucent; además, la plataforma de soporte para la configuración y monitoreo en el router Lucent Super Pipe 175 no es compatible con los otros routers y especialmente con el equipo Cisco. De acuerdo con los puntos mencionados y con base en que la mayor parte de la infraestructura del Banco está conformada por equipo Cisco, el criterio final de decisión en la selección de los routers se basó en que el Banco tiene un contrato de servicio establecido de compromisos y soluciones a mediano y largo plazo con Cisco Systems, con su infraestructura y soporte técnico. Por tal motivo, se decidió comprar el equipo Cisco, modelo 7204, ya que en el comparativo, aunque existen otros routers con mejores características y menor precio, el equipo Cisco es modular, puede aumentar su capacidad de memoria y en el contrato se estipula la actualización del software y el cambio de piezas o equipo dañado sin costo adicional.

Una vez realizada la selección del router para aplicar el proceso de encripción en la red financiera del Banco, se establece algunos aspectos generales de cómo Cisco realiza la encripción de datos.

El proceso de encripción en un router Cisco se puede realizar a través de la tarjeta de encripción ESA. La tarjeta ESA provee el mecanismo de encripción basado en hardware requerido para llevarla a cabo. El número de producto para la tarjeta de encripción de Cisco es SA-Encrypt y dicha tarjeta utiliza una llave de encripción de datos estándar (DES) de 40 ó 56 bits.

Los routers Cisco que contienen a la tarjeta de encripción ESA utilizan tecnología de llaves públicas, basadas en el concepto de *PE (Protected Entity / Entidad Protegida)*, que protege la autentificación, verificando su validez.

Las llaves públicas son una serie de números aleatorios que se generan dinámicamente a través de software y que hacen uso de la firma digital estándar (DSS) y de la encripción de datos estándar, lo anterior es para permitir el intercambio seguro de datos e información entre equipos similares dentro de la red.

Antes de que pueda realizarse el proceso de encripción, debe de iniciarse una sesión de encripción. Cuando una sesión de encripción está siendo establecida, cada router utiliza su firma digital estándar pública y la firma digital del router de encripción (Firma Digital Privada) para autentificarse mutuamente.

La llave que forma a la firma digital estándar privado, también es generada a través de software pero esta llave no se comparte con ningún otro dispositivo. Sin embargo, la llave que forma a la firma digital estándar pública se distribuye a todos los demás routers.

Para intercambiar llaves entre dos routers es necesario ponerse de acuerdo con el administrador del otro router, para corroborar verbalmente que las llaves públicas fueron intercambiadas correctamente.

Establecida la encripción, el tráfico encriptado puede pasar libremente entre los routers. Cuando la sesión de encripción expira, una nueva sesión se debe establecer antes de que el tráfico encriptado pueda ser enviado.

De acuerdo a los conceptos definidos en el párrafo anterior, se establece la forma de realizar la encripción de los datos utilizando el equipo seleccionado de Cisco.

Básicamente existen dos técnicas para implementar la encripción en un router Cisco. La primera técnica está basada en el uso de listas de acceso y la otra en el uso de túneles *GRE (Generic Routing Encapsulation / Encapsulado de Enrutamiento Genérico).*

- **Encripción con listas de acceso**

Las listas de acceso, en el proceso de encripción, se utilizan para definir qué paquetes IP serán encriptados y cuáles no lo serán. Las listas de acceso para encripción son siempre listas de acceso IP extendidas.

Normalmente las listas de acceso se utilizan para filtrar tráfico. En Encripción, las listas de acceso no se utilizan para filtrar tráfico, sino que se utilizan para especificar cuáles paquetes de IP van a ser encriptados y cuáles no.

Para configurar una lista de acceso se deberá tomar en cuenta lo siguiente:

- Al utilizar la palabra ***permit*** dentro de la lista de acceso, ocasionaremos que todo el tráfico que pase entre la fuente y el destino especificados sea encriptado y desencriptado por el par de routers involucrados en el proceso de encripción. Al utilizar la palabra ***deny*** dentro de la lista de acceso, evitaremos que el tráfico que pase entre la fuente y el destino sea encriptado y desencriptado por el par de routers utilizados para encripción.

- Las listas de acceso para encripción, que se definen en el router local deben tener su contraparte en el router remoto, de tal manera que el tráfico que localmente sé encripta, en el router remoto sé desencripta.

La lista de acceso será aplicada a las interfaces seriales de los routers como una lista de acceso de encripción de salida, donde se especifique todo el tráfico a encriptar. Cisco posee una herramienta de configuración para encriptar datos llamada *crypto maps (Mapas de encripción)*. Los crypto maps contienen todas las listas de acceso que se definieron para encripción en los routers de encripción y debe tener su contraparte en el router remoto. Los mapas de encripción, se utilizan en conjunto con el algoritmo de encripción DES para definir en una lista de acceso cual dato será encriptado.

Una desventaja de esta técnica de encripción es que necesita que la configuración de los equipos que conforman la red soporte la técnica de encripción de listas de acceso.

Para el caso del Banco, se configuran dos listas de acceso correspondientes a cada enlace, es decir, una hacia el router Principal y otra hacia el router Secundario.

En un principio se pensó utilizar la técnica de listas de acceso, pero el esquema que se tenía implementado en la red no estaba soportado por las técnicas de listas de acceso. Es decir, en el esquema las redes que se encuentran después de los routers remotos, propiedad de los Intermediarios Financieros, constituyen la dirección fuente y tendrán un solo destino que son los servidores del Banco. El camino para llegar al destino puede realizarse a través de dos rutas diferentes una hacia el Site Principal y la otra hacia el Site Secundario. Esta es la razón por la que se tienen que configurar dos listas de acceso, correspondiente una hacia el router de Encripción Principal y la otra hacia el router de Encripción Secundario. La implementación de encripción con listas de acceso creó conflictos en los pesos, es decir en el valor que se le proporciona a una lista de acceso para que cuando sea leída en la configuración se aplique primero o tenga una mayor prioridad de ejecución sobre la lista siguiente.

Los valores establecidos para *PE y UPE (Unprotected Entity / Entidad Desprotegida)*, son los que definen las prioridades de ejecución de las listas de acceso. El parámetro PE representa una dirección fuente IP especificada en el mapa de encripción, y que está contenida en las listas de acceso de encripción; el parámetro UPE, representa la dirección IP destino definida en las listas de acceso y validada por el mapa de encripción. El router siempre toma el parámetro PE como la dirección IP de la lista de acceso de menor valor y el parámetro UPE como la dirección IP de la lista de acceso de valor más alto; sin embargo, los valores para las dos listas de acceso creadas PE y UPE siempre coinciden. Esta situación crea un conflicto para la interpretación y ejecución de la encripción con listas de acceso. Debido a esta situación se creó un *Workaround (Entorno de trabajo)*, para tratar de solventar el problema, el Workaround consistió en darle pesos diferentes a ambas listas de acceso, tanto en el router remoto como en los routers de Encripción Principal y Secundario, para que de esta manera se simulase que el sistema estaba compuesto por fuentes y destinos diferentes.

Para esta situación, se agregó una línea ficticia en la configuración de cada una de las listas de acceso para cada enlace correspondiente. Es decir, en el router remoto se configuró la dirección 40.x.0.0, para el enlace correspondiente al Site Principal, y para el enlace hacia el Site Secundario se agregó en la configuración de las listas de acceso la dirección ficticia 50.x.0.0. En el caso de los router de Encripción Principal se agregó la dirección 20.x.0.0 y la dirección 25.x.0.0, para la configuración de las listas de acceso en el router de Encripción Secundario. En todos los casos, la “x” correspondía al número de la dirección WAN de cada router remoto.

La propuesta del Workaround no funcionó realmente bien ya que se tenían muchos problemas con bloqueos de los routers remotos. De tal forma que a nivel de IP, podíamos mandarle ping a los routers remotos y la respuesta era correcta, pero a nivel TCP no podíamos establecer sesiones de telnet o FTP. Esta situación se presentó de manera aleatoria en cualquier router remoto y de forma más o menos constante.

De acuerdo a las recomendaciones de Cisco se sustituyó el sistema operativo IOS por una versión más reciente tanto en los routers remotos como en los del Backbone, sin embargo, el problema persistió, por lo que se decidió no utilizar el Workaround.

Para tratar de solucionar este problema fue aplicar la técnica de encripción con listas de acceso por un solo enlace hacia el Site Secundario, para que así se pudiera soportar la técnica propuesta. De esta forma se configuraron todos los routers con encripción, el sistema se mantuvo estable por dos semanas, presentando un problema con el bloqueo total de los mismos en su enlace hacia el Site Secundario. La recuperación de la comunicación con los routers remotos con el router de Encripción Secundario, tomó aproximadamente dos horas y media. Por este motivo, y por los problemas mencionados anteriormente, se decidió no emplear la técnica de listas de acceso para habilitar la encripción de los datos en la red.

- **Encripción con túneles GRE**

La segunda técnica que se propone para encripción es utilizar túneles GRE. Los túneles son enlaces lógicos que siguen el mismo camino que la conexión de Frame Relay. Los túneles GRE por trabajar en la capa 3 del modelo OSI, están por encima del nivel físico y de enlace, siendo en teoría independiente del medio de transmisión. GRE es un protocolo para configurar túneles que desarrolló Cisco.

Los túneles GRE permiten a los datos que viajan a través de la red como si hubiese un enlace virtual entre cada nodo origen y cada nodo destino. Cuando en ambos extremos de los routers de encripción, tanto locales como remotos, están configurados los túneles GRE, es posible que pase la información a través de ellos. De esta manera, todo el tráfico que pase a través del túnel GRE será encriptado.

Es importante señalar que esta técnica no puede ser selectiva respecto al tipo de tráfico que pase por el túnel GRE, es decir, sólo podemos hacer que todo el tráfico que transite por el túnel GRE sea encriptado o no.

Considerando la inclusión de los routers de encripción, las direcciones IP de los routers remotos se mantienen tal y como se tienen hasta ahora y simplemente se agregarán las interfaces de los túneles con direcciones clase B, 190.90.42.1 hasta la dirección IP 190.90.42.14 para sucursales y de la IP 190.90.42.21 a la 190.90.42.40 para los Intermediarios Financieros; las cuales corresponden desde el túnel 1 hasta el túnel 40. De la misma manera para los túneles creados en el router de Encripción Secundario, las direcciones serán 190.90.52.1 hasta la dirección IP 190.90.52.14, y de la IP 190.90.42.21 a la 190.90.42.40 para los Intermediarios Financieros, las cuales corresponden a los túneles 1 hasta el túnel 40.

Como en la estructura de la red se tienen dos enlaces, uno hacia el Site Principal y otro al Site Secundario, se deben crear dos túneles para cada enlace remoto. Dichos túneles tienen como origen la interfaz serial HSSI 5/0/0 del router de encripción y como

destino las direcciones IP de las interfaces seriales 1/0 (s1/0) para el enlace con el Site Principal y serial 1/1 (s1/1) para su enlace con el Site Secundario.

Los pasos que se llevarán a cabo para implementar los túneles GRE en los routers Cisco de encripción, como en los routers remotos propiedad de los Intermediarios Financieros es:

1. Como primer punto se tiene que generar las llaves que forman las firmas digitales públicas y privadas para todos los routers Cisco de la red. Esto se realiza utilizando el comando ***crypto gen-signature-keys key-name [slot]***. Para los routers de encripción se seleccionaron los nombres clave "key-name", Encrip_Princ y Encrip_Sec, respectivamente. Además, como ambos routers cuentan con la tarjeta de encripción ESA, es necesario proporcionar el número de la ranura en la que ésta se encuentra colocada físicamente (en este caso se encuentra en el Slot 2 en ambos routers). Para el caso de los routers remotos Cisco 3640, el nombre clave "key-Name" seleccionado será el propio nombre del router y como no tiene tarjeta ESA, no es necesario poner el número de ranura. A continuación se muestran algunos ejemplos de como se configuran las firmas digitales DSS en los routers Principal, Secundario y en un Intermediario Financiero;

   Encripción Principal(config)#crypto-gen-signature-keys Encrip_Princ 2
   Encripción Secundario(config)#crypto-gen-signature-keys Encrip_Sec 2
   Intermediario1 (config)#crypto-gen-signature-keys Intermediario1

2. Una vez que se han generado las firmas digitales públicas y privadas, en los routers de encripción y en los routers de los Intermediarios Financieros, dichas llaves se tienen que intercambiar entre ambos. El proceso de configuración continúa al declarar a los routers de Encripción Principal y Secundario como pasivos, utilizando el comando crypto key-exchange passive, y a los routers remotos como activos, utilizando el comando crypto key-exchange ip-address key-name, en donde IP-address corresponde a la dirección IP de la interfaz HSSI 5/0/0 (*ver Figura 4.5.)* de los routers de encripción Principal y Secundario respectivamente. El router remoto, propiedad de los Intermediarios Financieros, tiene que intercambiar las llaves con ambos routers de encripción. El nombre clave o key-name corresponde a la firma digital que se generó anteriormente y está definida por el nombre mismo del router remoto. A continuación se muestra un ejemplo de este tipo de configuración.

   Encripción Principal(config)#crypto keys-exchange passive
   Intermediario1 (config)#cryptokeys-exchange 190.90.0.2 Intermediario1
   Encripción Secundario(config)#crypto keys-exchange passive
   Intermediario1 (config)#cryptokeys-exchange 190.90.0.3 Intermediario1

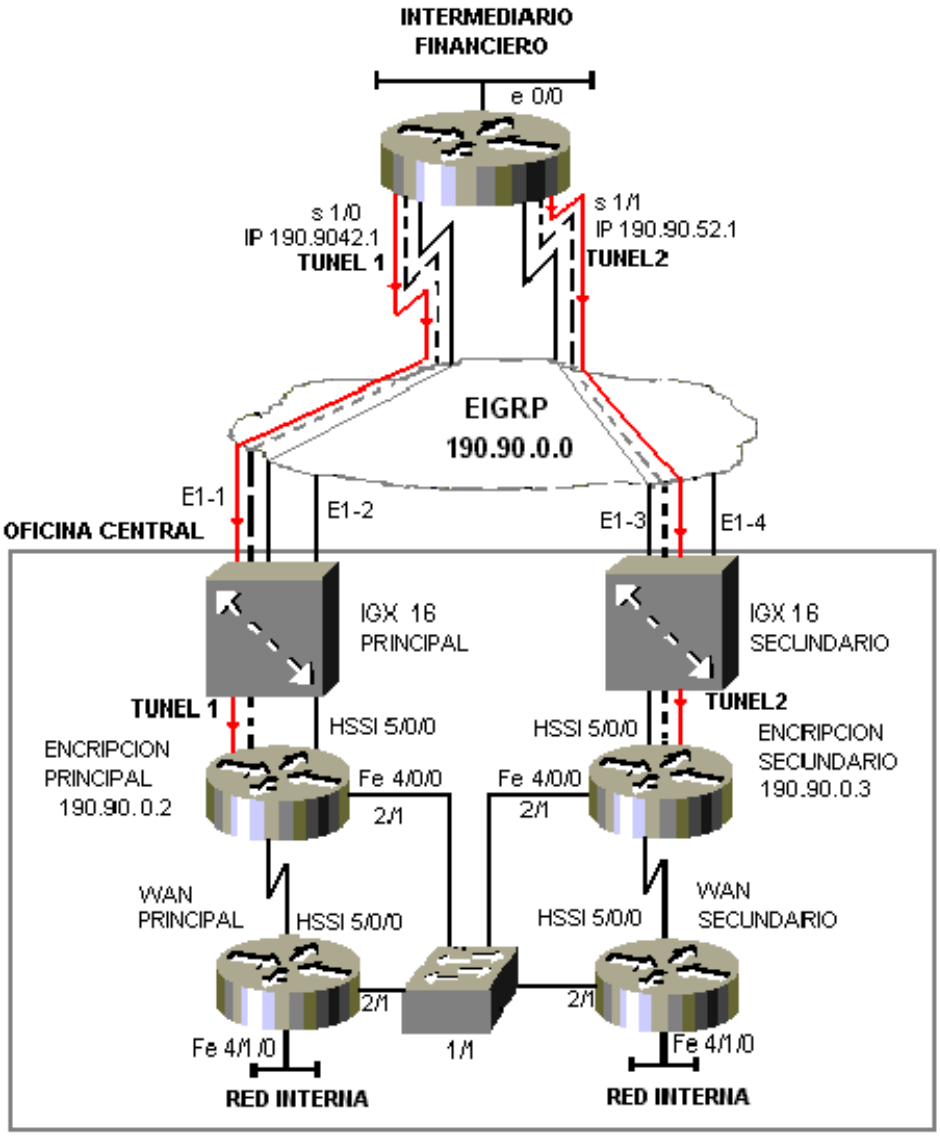

Figura 4.5. Conexión remota a través de túneles.

De acuerdo a la *Figura 4.5,* la configuración de los túneles GRE en los routers remotos, el número de interfaz túnel será 1 para el enlace hacia el router de Encripción Principal, y túnel 2 para el router de Encripción Secundario. Además, por recomendaciones de la compañía Cisco, se deben deshabilitar los procesos de fast switching (conmutación rápida), utilizando la instrucción (no ip route-cache), y de IP de conmutación rápida para multicast, utilizando la instrucción (no ip mroute-cache); esta opción permitirá evitar las colisiones en los

puertos LAN de los routers. Con esta recomendación, se decidió deshabilitar los procesos descritos en ambos túneles de los routers remotos.

Para el caso de los routers de encripción, el número de interfaz túnel se seleccionó basándose en el número de la dirección IP de la WAN del router remoto para el cual corresponde el túnel. Por ejemplo, para el caso del Intermediario 1, que tiene una dirección 1 para su enlace WAN, los routers de Encripción Principal y Secundario, tendrán el número de interfaz túnel igual a 1. La forma en que se configura el túnel 1 para el Intermediario Financiero en los routers de encripción Principal y Secundario y en el router del Intermediario Financiero 1 se presenta a continuación.

La configuración de la interfaz túnel 1 en el router de Encripción Principal será:

```
Encripción Principal(config)#interfaz Tunnel 1
Encripción Principal(config-if)#ip unnumbered Hssi 5/0/0
Encripción Principal(config-if)#tunnel source Hssi 5/0/0
Encripción Principal(config-if)#tunnel destination 190.90.42.1
```

La configuración de la interfaz túnel 1 en el router de Encripción Secundario será:

```
Encripción Secundario(config)#interfaz Tunnel 1
Encripción Secudario(config-if)#ip unnumbered Hssi 5/0/0
Encripción Secundario(config-if)#tunnel source Hssi 5/0/0
Encripción Secundario(config-if)#tunnel destination 190.90.52.1
```

La configuración de la interfaz túnel 1 hacia el Site Principal y el túnel 2 hacia el Site Secundario en el router remoto se muestra a continuación:

```
Intermediario1 (config)#interface Tunnel1
Intermediario1 (config)# ip unnumbered  Serial 1/0
Intermediario1 (config)# no ip route- cache
Intermediario1 (config)# no ip mroute-cache
Intermediario1 (config)#tunnel destination 190.90.0.2
Intermediario1 (config)#interface Tunnel2
Intermediario1 (config)# ip unnumbered  Serial 1/0
Intermediario1 (config)# no ip route- cache
Intermediario1 (config)# no ip mroute-cache
Intermediario1 (config)#tunnel destination 190.90.0.3
```

Tanto en las interfaces túneles de los routers remotos como en los routers de encripción, se deben configurar los mapas de encripción (crypto map's), los cuales contienen el nombre del router remoto al que se aplican y la lista de acceso que habilita el tráfico a encriptar. Los comandos para configurar los mapas de encripción (crypto map) son:

Crypto map-name seq-num
Set algorithm 40-bit-des
Set peer key-name
Match addresss [access-list-number| name]

Para los routers remotos el mapa de encripción (map name) sé selecciónó utilizando el nombre del mismo router más el número “1”, para su enlace hacia el Site Principal, y “2“, para el enlace con el Site Secundario. El número de secuencia seq-num siempre se fijó a 10. El nombre clave (key-name) para el enlace con el Site Principal será Encrip_Princ. 1, y Encrip_Sec 2 para el enlace hacia el Secundario.

Se seleccionó la lista de acceso 101 para el enlace hacia el Site Principal y 102 para la lista de acceso hacia el Site Secundario. El número de secuencia seq-num se configuró de acuerdo a la dirección IP WAN que tiene el router remoto para el cual se aplicará dicho crypto map. En nuestro ejemplo, el Intermediario Financiero 1 tiene la dirección 1 de WAN, y por lo tanto los routers de Encripción Principal y Secundario tendrán el crypto map 1 que se aplicará a dicho router. El nombre clave (key-name) se tomó con base en el nombre del router remoto para el cual se aplica dicho mapa. Por último, el “acces-list-number” es el número de la lista de acceso que se había configurado para el router remoto. A continuación se muestra un ejemplo de configuración de los túneles y mapas de encripción para el Intermediario 1, tanto en el router principal como en el remoto;

Intermediario1(config)# crypto map Intermediario1 10
Intermediario1(config-crypto-map))#set algorithm 40-bit-des
Intermediario1(config-crypto-map))#set peer Encrip_Princ
Intermediario1(config-crypto-map)#match address 101
Intermediario1(config)# crypto map)#crypto map Intermediario2 10
Intermediario1(config-crypto-map))#set algorithm 40-bit-des
Intermediario1(config-crypto-map))#set peer Encrip_Princ
Intermediario1(config-crypto-map))#match address 102

Encripción Principal(config)# Encrip_Princ 1
Encripción Principal(config-if)# ip unnumbered Hssi 5/0/0
Encripción Principal(config-if)# tunnel source Hssi 5/0/0
Encripción Principal(config-if)# tunnel destination 190.90.42.1

Encripción Secundario(config)#interfaz Tunnel 1
Encripción Secudario(config-if)#ip unnumbered Hssi 5/0/0
Encripción Secundario(config-if)#tunnel source Hssi 5/0/0
Encripción Secundario(config-if)#tunnel destination 190.90.52.1

Una vez que se han configurado los túneles, el siguiente paso será configurar las listas de acceso tanto en los routers remotos como en los routers de Encripción Principal y Secundario respectivamente.

Para configurar las listas de acceso, en los routers remotos y en los routers de encripción, como se mencionó anteriormente, se utilizan las listas de acceso son 101 para el enlace primario y 102 para el secundario, para ello se toma como base la dirección IP del enlace WAN al cual estará aplicada la lista de acceso. En nuestro ejemplo, al Intermediario 1 le corresponde la dirección 1 de WAN, por lo tanto, los routers de encripción tendrán la lista de acceso 101 que se aplicará a dicho router.

En el caso de los routers remotos, se crearán dos listas de acceso, una para cada interfaz serial. Así, para la serial 1/0 tendremos la dirección 190.90.42.xx y para la interfaz serial 1/1 tendremos la dirección 190.90.52.xx, donde xx corresponde a la dirección asignada de la sucursal1 a la 14 y de la 21 a la 40 para el caso de los intermediarios financieros, como se muestra en el siguiente código descriptivo:

```
Encripción Principal(config)#access-list 101 permit gre host 190.90.0.2 host 190.90.42.1
Encripción Principal(config)#access-list 101 permit gre host 190.90.0.2 host 190.90.52.1
Intermediario 1 (config)# access-list 101 permit gre host 190.90.0.2 host 190.90.42.21
Intermediario 1 (config)#access-list 102 permit gre host 190.90.0.2 host 190.90.52.21
```

Podemos observar que las listas de acceso hacen relación a la llave “permit gre”, la cual corresponde al tipo de encapsulado del túnel, y también tiene como fuente las direcciones IP de sus interfaces seriales (s1/0 para el enlace Principal y s1/1 para el enlace Secundario) y como destino las direcciones IP de las interfaces HSSI 5/0/0 de los routers de Encripción Principal 190.90.0.2 y 190.90.0.3 para el router de Encripción Secundario.

En el lado de los routers de Encripción Principal y Secundario también se deberán crear sus correspondientes túneles hacia cada uno de los routers remotos. Es decir, para el router de Encripción Principal, el túnel inicia en su interfaz serial HSSI 5/0/0, que es la interfaz hacia todos los routers remotos y termina en la interfaz serial 1/0 del router remoto. Para el router Encripción Secundario, el túnel inicia en su interfaz HSSI 5/0/0 y termina en la interfaz serial 1/1 del router remoto.

Las listas de acceso deben ser aplicadas tanto en las sucursales como en los Intermediarios Financieros. Por ejemplo, para aplicar la lista de acceso 101, en la interfaz del túnel 1 de la Sucursal1, se utiliza la instrucción *ip access-group 101 in*, con esta instrucción todas los equipos contenidos en la lista 101 pueden acceder a la interfaz túnel 1, del router. Esta acción se realiza al configurar la interfaz del túnel 1 de la siguiente manera;

```
Sucursal1(config-int-tunel)#
interface Tunnel1
bandwidth 56
ip unnumbered Serial1/1.2
ip access-group 101 in
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
```

tunnel source Serial1/1.2
tunnel destination 190.90.42.2
Sucursal1#

Para el caso de los routers de encripción Principal y Secundario, se deberán configurar tantas listas de acceso como routers remotos con encripción existan.

El formato de la lista de acceso es el mismo que se utilizó para los routers remotos, con la diferencia que la fuente y el destino se intercambian, quedando la interfaz HSSI 5/0/0 como la dirección fuente y la interfaz serial del router remoto como la dirección destino. Posteriormente, se crean los crypto map´s y será muy importante aplicarlos tanto a las interfaces seriales como a las interfaces túneles.

Al realizar un análisis de la seguridad de la red, un punto vulnerable se refiere a la falta de una barrera que limite el acceso a la red desde los puntos remotos, y que a su vez permita el acceso desde la oficina central para poder administrar los routers propiedad de los Intermediarios Financieros. En los diagramas a bloques de las *Figuras 4.1, y la Figura 4.3*, se describe el proceso actual del flujo de información**.**

Regresando a la *Figura 4.1*, como puede observarse, el flujo de la Información, una vez que se accesaron a los routers WAN y LAN Principal y Secundario, el proceso sigue hacia la red interna. En este punto no existe ninguna forma que pueda proporcionarnos seguridad en los datos. Cuando se conecta una sucursal, o un respaldo a través del modem vía RAS, sucede la misma situación, el paso de información sigue hacia la Red Interna y solamente es filtrado usando listas de acceso y rutas estáticas en los router de sucursales, o en los routers WAN y LAN Principal y Secundario respectivamente.

Aun con la solución propuesta en el punto anterior de encriptar los datos, mostrada en la *Figura 4.3,* la situación de no tener seguridad en el acceso a la Red Interna persiste, sobre todo cuando se conecta a través de Dial-up.

Si bien es cierto que tanto en el RAS como en los routers remotos se configuran passwords para validar el acceso y autentificación, una vez validado el acceso, pueden seguir hasta los servidores de la Red Interna, lo cual es muy peligroso en el caso de que algún intruso pueda estar escuchando la red y cambie el password de autentificación.

La situación descrita es uno de los puntos más importantes que tiene que ser mejorado, y para realizar este propósito, se utilizará una barrera de fuego PIX Firewall.

El PIX no solamente permitirá el acceso a los servicios prestados por el banco a las direcciones válidas en cada router remoto, también puede limitar el acceso de los usuarios internos a la red externa o pública como puede ser Internet.

Con la finalidad de evitar los accesos no autorizados, se propone instalar un PIX Firewall para acceso a la Red Interna, conectado como se muestra en la *Figura 4.6.* La conexión propuesta para insertar al PIX Firewall entre los routers LAN Principal y Secundario nos ayudara a tener el control de acceso a la Red Interna, ya sea desde un enlace remoto de los Intermediarios Financieros, Sucursales del Banco, o también cuando se acceda por medio del modem de respaldo vía el servidor de acceso remoto.

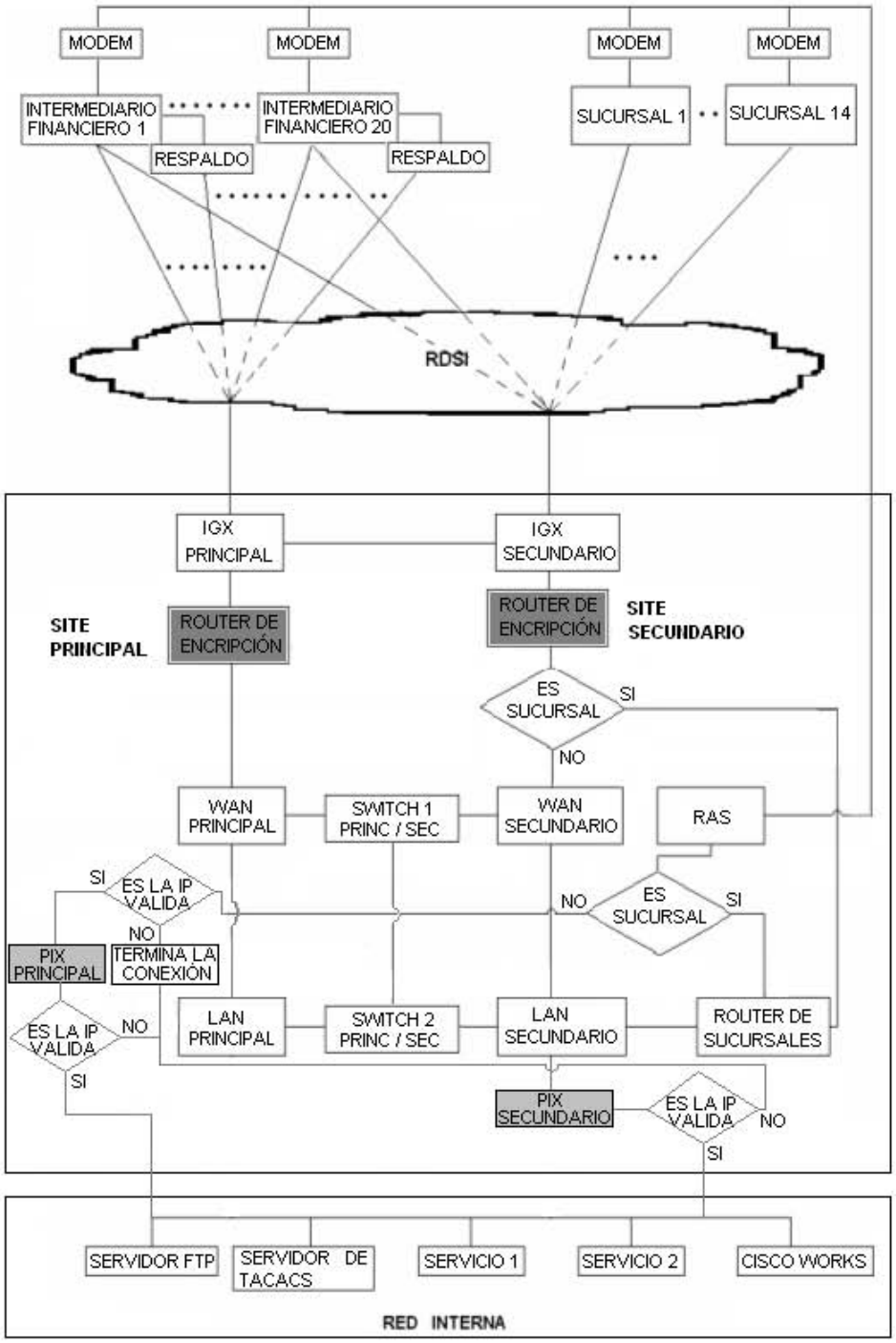

Figura 4.6. Solución propuesta utilizando un PIX Firewall.

El PIX Firewall es un dispositivo que nos ayudará a prevenir conexiones no autorizadas entre dos o más redes, el uso de este dispositivo permitirá que una vez que sea validado el proceso de encripción para acceder a la red en el PIX Firewall, las direcciones válidas procedentes de los Intermediarios Financieros sean transformadas en direcciones válidas dentro de la Red Interna, a este proceso se le llama *NAT (Netwok Address Translation / Traslación de Direcciones de Red)*.

Así, el flujo de la información y datos pasarán por un proceso de encripción y autentificación para poder acceder a los router WAN, posteriormente seguirá su camino hacia los router LAN, el cual decidirá de acuerdo a sus listas de acceso y rutas estáticas declaradas si sigue su camino hacia la Red Interna, de ser válida pasa al PIX Firewall donde la dirección es transformada en una dirección válida dentro de la Red Interna y filtrada hacia el servicio que adquirió con el banco.

Una vez que hemos descrito algunas características de los Firewalls, presentamos un comparativo de diferentes proveedores y seleccionaremos el más conveniente, dicho comparativo se muestra en la Tabla 4.2.

Firewall			
Marca	3COM	Cisco	Lucent Technologies
Modelo	SuperStack 3	PIX 525	VPN Brick 80
Procesador	233 MHz Strong ARM RISC	Intel Pentium III a 600 MHz	350 MHz, AMD K6-2
Memoria RAM	16 MB	32 MB, expansión a 256 MB	64MB
Memoria Flash	4 MB	16 MB	4 MB
Puertos	3 puertos RJ-45	De 1 a 3 puertos RJ-45	4 puertos RJ-45
Métodos de Encripción Soportados	ARC4, DES, 3DES	DES, 3DES	3DES
Clientes VPN Soportados	640,000 simultáneos	280,000 simultáneos	300,000 simultáneos
Interfaces	3 Interfaces RJ-45 Ethernet 10/100,	8 Fast Ethernet 10/100BaseT, RJ-45 duales integrados, 3 Gigabit Ethernet.	4 Ethernet 10/100 1 video SVGA. 1 Serial DB9 1 Externo Floppy 1 teclado PS/2
Protocolos que soporta	PPP, Frame relay, ethernet, Ethernet, ATM, NAT, DHCP.	PPP, NAT, PAT, Ethernet, DHCP.	Fast ethernet, X.25, Ethernet, Serial
Ranuras PCI	3	4	3
Precio	$469.75 a $528.95 dólares	$6,800.00 a $9,720.26 dólares	$1000.00 a $3000.00 dólares

Tabla 4.2. Comparación de Firewalls de diferentes proveedores.

De acuerdo con los datos de la T*abla 4.2*, podemos observar que el PIX Firewall de la marca Cisco posee una mayor velocidad de procesamiento, 600 MHz utilizando

un procesador Intel Pentium III; además, puede tener hasta 256 MB de memoria RAM, superando a los otras marcas que se utilizaron en el comparativo. Si bien es cierto que maneja menor número de sesiones simultáneas de VPN, y aun sin manejar la cantidad de puertos que tiene el PIX Lucent Brick 80, y que su precio es mayor; por las características mencionadas anteriormente, de mayor velocidad y capacidad de memoria, se decidió comprar el equipo PIX Firewall 525 de la compañía Cisco con la finalidad de homologar el equipo que se tiene en el Site.

Una vez establecida la selección del equipo, ya que nuestro interés está en la red externa, solamente definiremos algunos aspectos que se implementarán en el PIX para proteger a la Red Interna. En nuestro caso las direcciones válidas dentro de la red deben ser de clase B, y serán distribuidas de acuerdo a estándares establecidos para que no se traslapen con las direcciones asignadas a otros usuarios.

Dentro del PIX se definieron las direcciones de entrada de datos las cuales serán filtradas, también se determinaron las direcciones válidas desde la Red Interna para poder acceder al correo electrónico, realizar Telnet o modificar la configuración de algún router remoto. La configuración para esta situación se presenta a continuación:

```
PIX (config)#
ip address outside  190.90.90.117   255.255.255.0
ip address inside    190.90.10.135   255.255.255.0
ip address failover 190.90.20.1  255.255.255.0
ip address intf4     190.0.2.1  255.255.255.255
ip address intf5    190.0.2.3   255.255.255.255
PIX#
```

También se pueden definir las personas que tienen prioridades de cambiar la configuración de los equipos. A continuación se muestran los comandos dentro del router para que estas personas puedan configurar los equipos.

```
PIX (config)#
ip local pool admin1 190.90.20.25
ip local pool admin2 190.90.22.18
ip local pool admin3 190.90.23.79
PIX#
```

En la configuración del PIX se habilitaron la traslación de direcciones (NAT) y la validación de algunas direcciones IP que pueden acceder a la red interna; además se definieron aquellas direcciones IP que tendrán permitido el acceso a los sistemas internos, asignándoles direcciones privadas. La utilidad de esta estructura permitirá retener direcciones inválidas, ya que además de trasladar la dirección, la autentifica y valida para permitir o negar su acceso dentro de la red Interna. El comando NAT se

utiliza para establecer el nivel de seguridad en la interfaz que deseamos iniciar una conexión hacia otra interfaz de menor nivel de seguridad. La declaración de estas direcciones se realiza utilizando el siguiente formato:

PIX (config)#
nat (inside) 0 190.90.90.0 255.255.255.0 0 0
static (inside,outside) 190.90.20.5 190.90.20.5 netmask 255.255.255.255 0 0
static (inside,outside) 190.90.20.15 190.90.20.15 netmask 255.255.255.255 0 0
static (inside,outside) 190.90.20.40 190.90.20.40 netmask 255.255.255.255 0 0
access-group 2 in interface outside
PIX#

En el ejemplo mostrado la instrucción NAT (inside) permite al host 190.90.90.0 iniciar una conexión desde una interfaz de nivel bajo de seguridad. El comando static (inside, outside) permite el acceso al host 190.90.20.5 desde una dirección de interfaz global de salida 190.90.20.5. La instrucción access- group 2 in, aplica la lista de acceso 2, la cual contiene todos los host que pueden acceder a la red interna.

Por último, para definir qué equipos de la Red Interna pueden acceder a los servicios públicos como Internet, correo electrónico, y hacer FTP, se definen en la lista de acceso 4, la cual contendrá a los usuarios que acceden al servidor interno. Así, las direcciones IP válidas tendrán el acceso al servidor 190.90.21.25, utilizando los puertos 2076 al 2078.

Así también, el servidor cuya IP es 190.90.20.14, accesa al servidor 190.90.100.43 utilizando el puerto 2001, y también el usuario con IP 190.90.20.65 puede acceder a Internet. La lista de acceso 4 se aplica a la interfaz de salida utilizando la instrucción access-group 4 in interface outside; estas configuraciones se muestran a continuación:

PIX(config)#
access-list 4 permit tcp any host 190.90.21.25range 7076 7079
access-list 4 permit tcp any host 170.70.10.100 range ftp-data ftp
access-list 4 permit tcp any host 190.90.20.65 eq www
access-list 4 permit tcp host 190.90.100.43 190.90.20.14eq 2001
access-group 2 in interface outside
PIX #

La conexión final del PIX Firewall, junto con las direcciones que utilizan, se muestran en la *Figura 4.7*.

Otro punto importante que tiene que mejorarse para mantener la disponibilidad de los servicios es la refiere a la creación de un nuevo enlace RDSI o DS0 de 64 kbps para las sucursales.

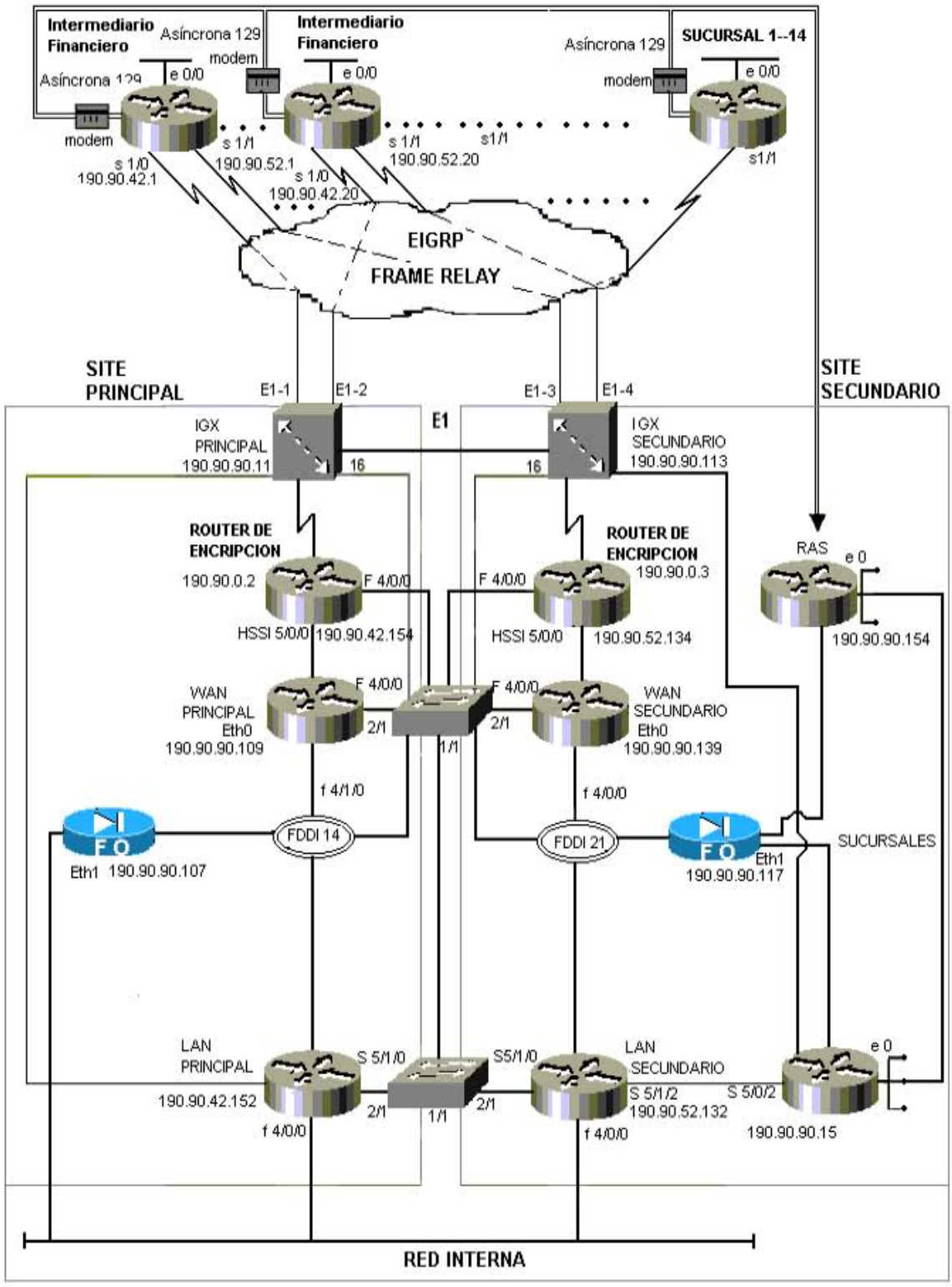

Figura 4.7. Conexiones del PIX Firewall.

4.2. Enlace DS0 o RDI para las Sucursales

Las sucursales sólo tienen un enlace por medio de la serial 1/1(s1/1) del router remoto hacia el Site Secundario. Sobre este enlace se transmiten voz y datos. El modem sirve como respaldo en caso de falla del enlace serial, pero cuando está en operación, sólo puede soportar la transmisión de datos. Un problema se presenta cuando ambos enlaces quedan fuera de producción; es decir, que el enlace serial falle y el modem quede fuera de servicio. En tal situación se perderá toda la comunicación con la sucursal.

La conexión actual de la Sucursal se muestra en la *Figura 4.8,* donde se puede observar que sólo se tiene la conexión al Site Secundario, a través del router de Sucursales, y su conexión a través del modem de respaldo localizado en este sitio.

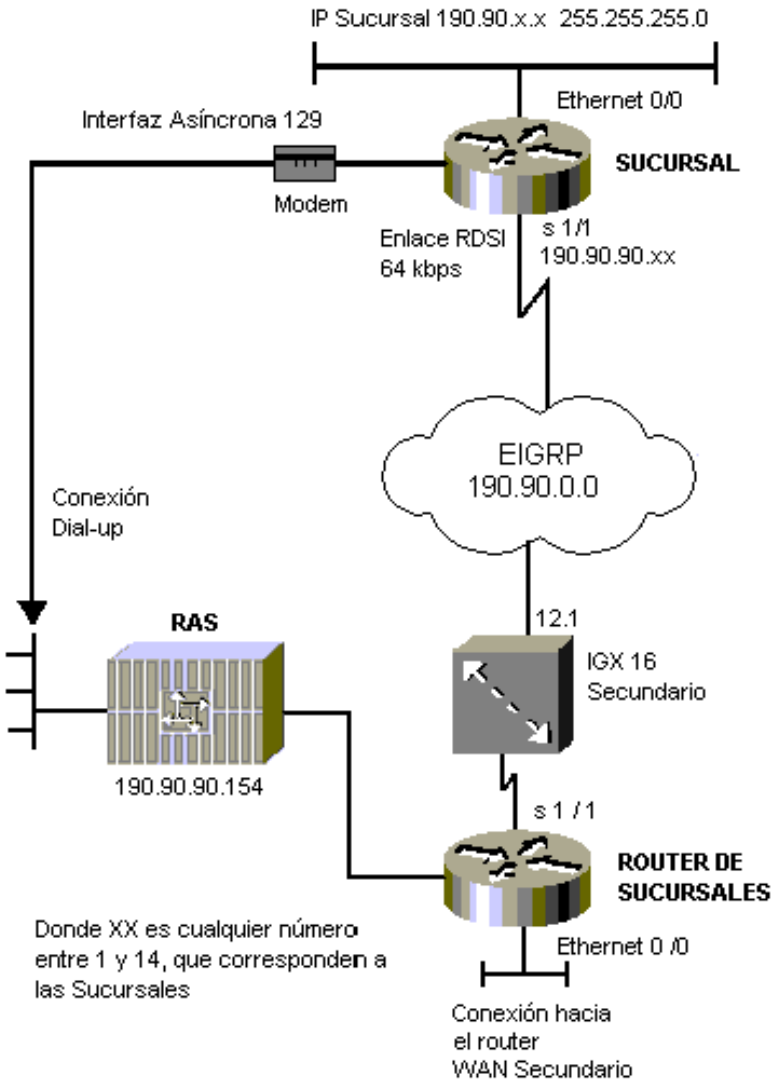

Figura 4.8. Conexión actual de una sucursal del Banco.

Una primera opción para resolver la problemática planteada sería contratar un nuevo enlace RDSI de 64 kbps conectado ala interfaz serial 1/0 s(1/0), formando una nueva conexión hacia el Site Principal para las respaldar a las sucursales, la integración de este nuevo enlace nos proporcionará el ancho de banda necesaria para soportar el servicio. Con la finalidad de proteger todavía más, tanto a las Sucursales como a los Intermediarios Financieros, se puede configurar la nueva conexión hacia un nuevo RAS que se localizará en el Site Principal y que funcione como respaldo en caso de contingencia cuando falle el RAS actual. Obviamente se requerirá manejar algún protocolo de ruteo en la interfaz a la red local de cada usuario, interactuando con routers de diferentes marcas. Este enlace permitirá proteger al sistema en caso de pérdida del enlace por la serial 1/1 (s1/1), la conexión del nuevo enlace RDSI y la implementación de una nueva conexión hacia un RAS en el Site Principal, se muestra en la *Figura 4.9.*

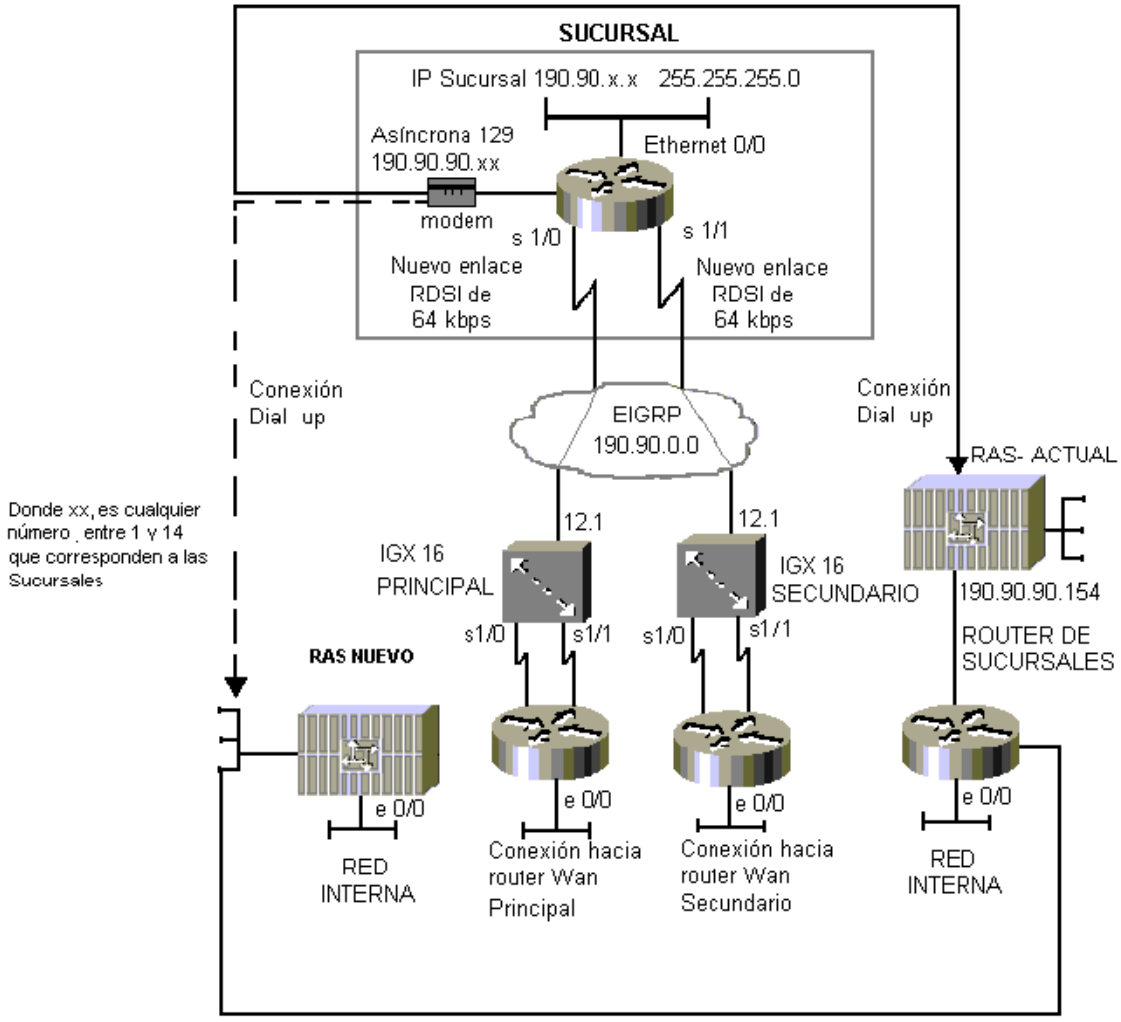

Figura 4.9. Conexión de la Propuesta usando un enlace RDSI y un RAS Nuevo.

Otra propuesta para prevenir el problema mencionado, es contratar un enlace DS0 de 64 kbps. Para que se utilice en la interfaz serial 1/0 del router de cada una de las Sucursales, este enlace permitirá proteger al sistema cuando la s1/1 falle, como se ve en la *Figura 4.10*.

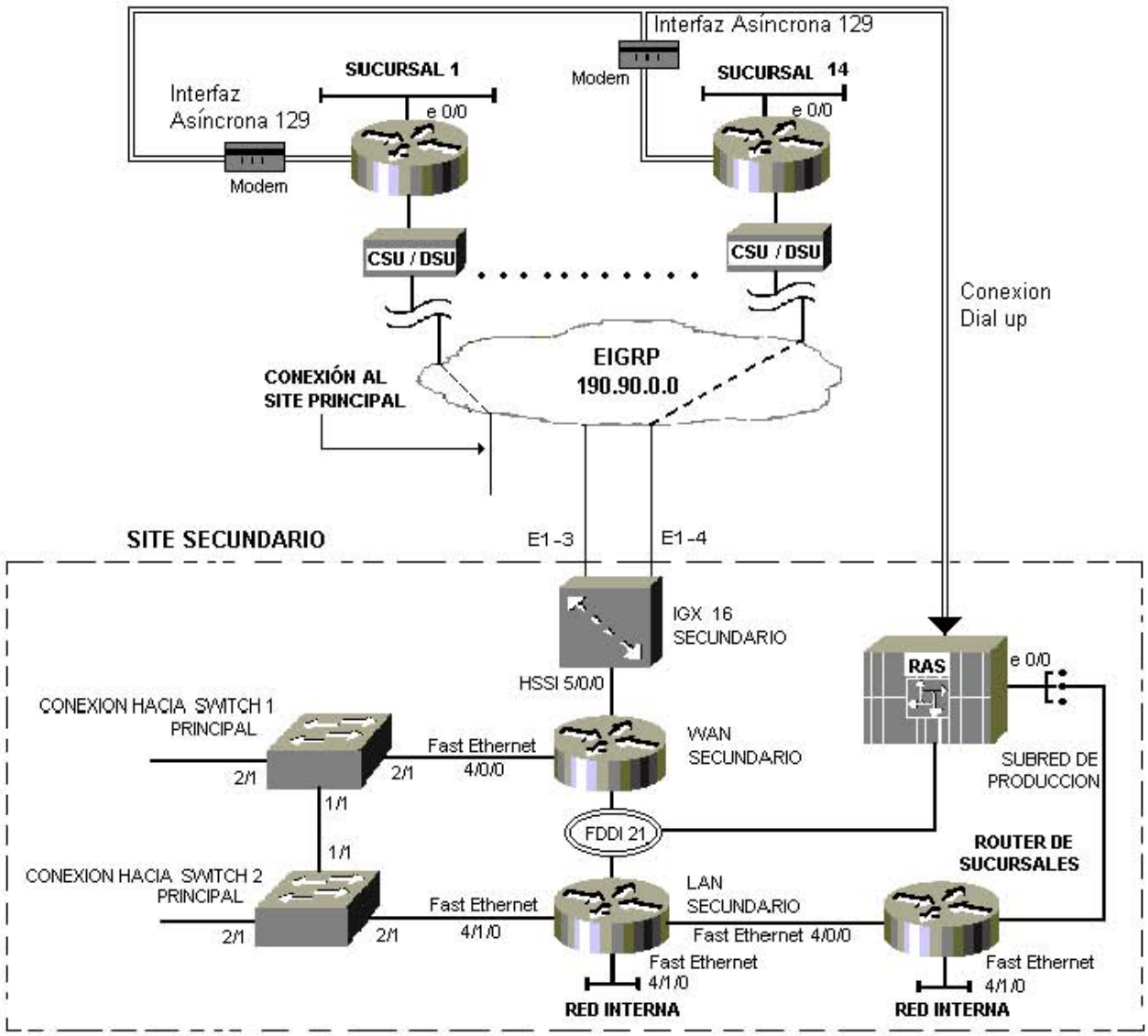

Figura 4.10. Conexión propuesta con un enlace DSO hacia el Site Principal.

Sin embargo, ambas propuestas tienen que ser evaluadas cuidadosamente, ya que el hecho de contratar otro enlace mejoraría nuestro servicio y disponibilidad, pero

se requerirá contratar 14 enlaces RDSI o DS0 de 64 kbps, uno para cada sucursal. Además de adquirir otro servidor de acceso remoto RAS para el Site Principal y activar la infraestructura de conexión entre el nuevo servidor de acceso remoto y el RAS que se encuentra actualmente en producción.

Es por ello que se realiza el siguiente estudio de factibilidad en cuanto a la adquisición de un nuevo enlace de DS0 con diferentes proveedores de servicio, así como el costo estimado del mismo. También se debe establecer un comparativo para comprar un nuevo RAS que permita soportar el respaldo de los enlaces en el Site Principal.

De acuerdo al estudio de tres diferentes proveedores de servicios RDSI, para una línea arrendada, se cuentan con las siguientes características:

- Costo de instalación con cargo a Cuenta Maestra ó recibo telefónico.
- Acceso Básico RDSI proporcionado por centrales digitales vía cobre.
- Servicio Conmutado que consta de un número digital RDSI.
- Permite la agrupación o suma de accesos básicos para manejar aplicaciones que requieran mayor ancho de banda, es decir desde 128, 256, 384 kbps ó más.
- Capacidad para manejar 2 llamadas ó servicios simultáneos sobre una misma línea RDSI, utilizando sus 2 canales "B" de manera independiente y manejar diversas aplicaciones como: llamadas de LD, Transmisión de Datos y/o de Imágenes a Velocidades de 64 kbps, en cada uno de estos canales, etc.
- Respaldo a Redes Privadas de Voz y Datos.
- Sujeto a Disponibilidad de Facilidades Técnicas.

El costo de una línea RDSI contratada se muestra en la *Tabla 4.3.*

Cantidad	Instalación	Renta Mensual sin IVA	Costo total Sin IVA	Costo total con IVA incluido
1	$ 4,499.00	$ 499.00	$ 4,998.00	$ 5,747.70

Tabla. 4.3. Costo de un enlace RDSI.

El costo por 14 líneas arrendadas se muestra en la *Tabla 4.4.*

Cantidad	Instalación	Renta Mensual sin IVA	Costo total Sin IVA	Costo total con IVA incluido
14	$ 62,986.00	$ 6,986.00	$ 69,972.00	$ 80,467.80

Tabla 4.4. Costo de arrendamiento de 14 líneas RDSI.

En nuestra aplicación la mayoría de las sucursales se encuentran en el interior de la república y entonces para los DS0s se hace el cálculo con base al servicio Ladaenlace de 64 kbps, este servicio se contrata localmente, con la finalidad de evitar el costo de enlaces de larga distancia, desde la sucursal hasta la oficina central del

Banco. Con la contratación de este tipo de enlace, utilizaremos la infraestructura del E1-3 y del E1-4 con que cuenta el Site Secundario y que posee canales libres, ya que se está pagando la renta de los 30 canales del E1 aunque no se utilicen todos.

En lo que respecta a los enlaces digitales “DS0”, se cuentan con las siguientes características:

- Enlaces de fibra óptica entre centrales de Telmex.
- Ancho de banda de 64 kbps.
- Monitoreo continuo por parte de Telmex.
- Par de cobre desde la última central de Telmex hasta el local del cliente.
- Bajo tiempo de respuesta en caso de fallas.
- Bajo costo en la contratación y renta mensual.
- Enlace dedicado.
- Capacidad de Enlaces Punto -Punto o Punto – Multipunto.
- Enlace de fibra óptica en el nodo central en Punto – Multipunto.

El enlace dedicado DS0 (Ladaenlace de 64 kbps local) tiene el costo presentado en la *Tabla 4.5.*

Cantidad	Instalación	Renta Mensual	Costo total Sin IVA	Costo total con IVA incluido
1	$14,000.00	$ 907.00	$14,907.00	$17,143.05

Tabla 4.5. Costo de arrendamiento de un enlace DS0 de 64 kbps.

El costo de 14 enlaces dedicado DS0 de 64 kbps se muestra en la Tabla 4.6.

Cantidad	Instalación	Renta Mensual	Costo total Sin IVA	Costo total con IVA incluido
14	$196,000.00	$ 12,698.00	$208,698.00	$240,002.70

Tabla 4.6. Costo de arrendamiento de 14 enlaces DS0.

Como puede observarse en las *Tablas 4.3, y 4.5*, el costo de una línea RDSI es menor que el de un enlace DS0, además la línea RDSI puede utilizar dos canales independientes y manejar aplicaciones de voz y datos con velocidades de 64 kbps en cada canal.

La diferencia más notable se encuentra si tomamos en cuenta los 14 enlaces que necesitamos para cada una de las sucursales del banco, donde el costo de los DS0 es de tres veces el costo de los enlaces RDSI; además, considerando que en algunas sucursales sólo se tienen una o dos computadoras, y que el personal sólo puede utilizar dos servicios a la vez, aunado a que la estructura de la red de las sucursales del Banco actualmente está soportada por enlaces DS0, la decisión final de la contratación de un nuevo enlace queda en manos del Banco.

Para subsanar la disponibilidad de los servicios prestados por el Banco y aumentar la utilidad de las herramientas prestadas por la globalización de los sistemas de información, se trata de subsanar la disponibilidad utilizando proveedores que ya cuentan con una línea establecida como Internet ó utilizando otros métodos, como los mencionados a continuación:

El contratar una línea telefónica pública que nos permita acceder a los servicios que el Banco proporciona, no solamente nos permitirá fortalecer la disponibilidad del servicio prestado, sino que también puede utilizarse para conexiones donde el tiempo de respuesta no sea muy crítico. Es así como en el siguiente estudio se vio la posibilidad de colocar un nuevo RAS en el Site Primario, con la finalidad de conectar a todos los intermediarios y sucursales a este nuevo RAS. La selección de un servidor RAS se presenta en el comparativo con tres diferentes proveedores de equipos en la *Tabla 4.7.*

Servidores de Acceso Remoto			
	Cisco AS5300	3Com	Compaq
	AS5300	Super stack II 3000	RAS 5408
Procesador	RISC 250 MHz	RISC 2 Power PC	Pentium II 233 MHz
Memoria SDRAM	128 MB default 512 MB expansión	20 MB DRAM	32 MB
Memoria flash	32default, 64 MB expansión	8 MB flash, expandible a 16 MB	No tiene
Interfaces	2 Fast ethernet 10/100, 8 seriales de 8 Mbps, 8 puertos T1, 2 E1 para voz y datos. 2 troncales.	6 T1, E1,ó PRI, Ethernet 10 Base –T, 1 FlexWAN de 56 kbps a 2 Mbps, 6 PRI-T1, E1,ó PRI,	2 Ethernet 10/100, 4 T1/E1-PRI, 1 RS-232 puerto serial, 8 RDSI-BRI
Número de modems	60 modems	30 modems	16 modems

Tabla 4.7. Comparación de servidores RAS. (Continúa).

Protocolos soportados	IP, IPX, NetBEUI, HRSP, ethernet, PPP multilink,Frame relay, HDLC, NAT.	Fast Ethernet, HDLC, Ethernet, RDSI PRI, BRI, PPP, TCP/IP, UDP/IP	PPP(multilink),IP, NAT, DHCP, LAN, TCP/IP, IPX/SPX; PAP, CHAP.
Modems soportados	ITU-T V.34, V.32bis, V.90 or V.92, V.90, ITU-T V.42, Asíncrono modo PPP	V.90, V.34, V.32, Bell 103, Bell 212A, AT&T,	33.6 KBPS/ V.34,
Seguridad	RADIUS, TACACS+, PAP,CHAP, encripción	RADIUS, TACACS+, PAP,CHAP,	NT Domain Securite PAP, , CHAP, MS-CHAP Encripción(40- and 128-bit)
Conexiones simultáneas	96 a 120	180	16
Voltaje	100-240 VACV	1.5 –100 VAC	100-240 VAC
Potencia	114 a 140 Watts	50 Watts	280 Watts
Temperatura	0° a 40°C	0° a 40°C	10° a 35 °C
Precio	$86,571.10	$ 90,000.00	$79,950.00

Tabla 4.7. Comparación de servidores RAS.

Con base a los datos obtenidos en la *Tabla 4.7,* podemos observar que el RAS de la compañía Cisco posee mayor velocidad de procesamiento, 250 MHz, comparada con los otros dispositivos mostrados en la tabla anterior; la capacidad de memoria del equipo Cisco es de 128 MB por default, siendo 6 veces mayor que la memoria del RAS de 3Com y 4 veces mayor que la del RAS de Compaq; de igual forma, la memoria flash del RAS de Cisco 32 MB es 4 veces mayor que la memoria flash del RAS de 3Com. También, el RAS de Cisco posee 8 puertos seriales con una velocidad de 8 Mbps con respecto a los otros equipos que poseen uno. Además, el número de modems internos soportados por el RAS de Cisco (60 modems) es mayor comparado con los 30 modems del RAS Super Stack II 3000 de 3Com y de los 16 modems soportados por el RAS 5408 de Compaq.

De acuerdo las características mencionadas, aunado a que el precio del RAS de Cisco es menor que el precio del RAS Super stack II 3000 de 3Com, se decidió adquirir el RAS de Cisco modelo AS 5300 para el Site Principal.

Conexión usando VPN's

La comunicación entre el Site Principal y el Site Secundario debe ser fluida y segura para facilitar el trabajo dentro de la organización. Habitualmente en la oficina de administración central residen los servidores de bases de datos, de correo y aplicaciones necesarias para el trabajo diario del personal. En este caso se plantean tres diferentes opciones para interconectar las oficinas:

- **Una primera posibilidad** es ser propietario de las líneas punto a punto que unan las sucursales e Intermediarios Financieros con el Site Central. Esta solución tan simple es extraordinariamente costosa y necesita de licencias para instalar las líneas, haciendo un comparativo, una línea E1 punto a punto arrendada tiene un costo de instalación de $ 209,233.30 pesos y una renta mensual $12,238.30 pesos, por lo que el ser propietario de una línea implicaría que los costos de implementación se triplicarían y por consiguiente se considera como una solución no rentable.

- **Una segunda opción** es alquilar para uso exclusivo las líneas punto a punto que unen las sucursales e Intermediarios Financieros con el Site Principal. Esta segunda opción es contratar una línea E1 punto multipunto cuyo costo de instalación es de $ 104,583.30 pesos con una renta mensual de $ 18,375.15 pesos. Esta solución aún siendo más económica que la anterior sigue siendo excesivamente costosa.

- **Una tercera solución** consiste en contratar con un proveedor de servicios una VPN. Este proveedor ofrece su propia red para interconectar las oficinas. La red del proveedor es pública, ya que la pueden usar otras organizaciones, pero el proveedor se compromete a que los datos procedentes de una compañía no van a llegar a otras entidades. Igualmente garantiza la confidencialidad de la información. Esta última solución es económicamente la más rentable; por ejemplo, si contratamos una conexión permanente a Internet en el corporativo, y a cada uno de los usuarios remotos le contratamos una cuenta de acceso a Internet con un costo de $ 180.00 mensuales, así cada vez que se requiera hacer alguna consulta se "entra" a nuestra página y mediante una contraseña se tiene acceso al sistema de información. De esta forma sólo se pagan las llamadas locales y las cuentas. Al emplear la conexión por VPNs, la solución puede rondar en los $220,000 mensuales, lo que representa un ahorro significativo frente a las demás opciones, además, los problemas de seguridad son mínimos, teniendo en cuenta las ventajas que aporta, por ello es esta solución la que se pretende implementar en los servicios que proporciona el Banco.

Debido a los servicios que proporciona el banco surge la necesidad de contar con un medio de comunicación para los usuarios que se encuentren fuera de las oficinas y en distintos puntos geográficos. Este tipo de usuario emplea otra forma de acceso a la red del Banco, a través de un modem vía Dial-up utilizando la línea telefónica pública. En este proceso el acceso a la red se realiza y es autorizado por medio del RAS, que permite a usuarios localizados fuera de la LAN, llamados usuarios remotos, conectarse a la red corporativa a través de dispositivos como son los modems, RDSI, o a través de Internet con VPNs. Este último punto es tratado en los siguientes párrafos.

La forma de proveer el servicio de las VPN por parte de los proveedores está condicionada por la infraestructura de sus redes de datos. Las soluciones más comunes son las siguientes:

- Mediante circuitos ATM.
- A través de túneles tradicionales (GRE, IP-IP, etc.).
- Utilizando IPSec *(Internet Protocol Securite / Protocolo de Seguridad de Internet)*
- Implementando MPLS *(Multi Protocol Label Switching / Protocolo Múltiple de Conmutación Etiquetada).*

Circuitos ATM

Esta tecnología utiliza únicamente dos velocidades de transmisión, STM-1 (155Mbps) y STM-4 (620Mbps).

Para suministrar VPNs con ATM lo que se hace es reservar PVCs del ancho de banda deseado entre las sedes que se desean unir. Esta solución está empezando a entrar en desuso por varias razones:

- Tiene el problema del doble enlace N2, lo que quiere decir que en caso de tener N centros, si quiero conectarlos con todos los nodos restantes, hay que proveer N(N-1) enlaces y esto puede llegar a suponer una cantidad excesiva de enlaces. Así para interconectar 50 nodos, se necesitan 50(49)= 2450 enlaces.
- El tráfico actual mayoritario es IP. La gestión de las redes ATM es diferente del de IP, con lo que se tienen que duplicar dichos sistemas (uno para IP y otro para ATM). Esto supone duplicar esfuerzos tanto en operación y mantenimiento como en recursos humanos.

Túneles IP

En las redes que no utilizan ATM como protocolo de transporte, se pueden utilizar túneles IP (ó GRE). En este caso ambos túneles contienen datos que viajan a través de la red como si hubiese un enlace virtual entre cada nodo origen y cada nodo destino. Cuando ambos extremos de un túnel GRE están localizados entre el par de routers de encripción, es posible que pase la información a través del túnel GRE. Para

nuestro caso hacemos uso de la técnica de túneles GRE, ya que también puede utilizarse en el proceso de Encripción.

Túneles IPSec

IPSec tiene como característica más importante la posibilidad de encriptar los datos transmitidos. Esta cualidad es hoy en día el gran valor que tiene este protocolo y es lo que está permitiendo su rápida difusión en el mundo empresarial.

Sus desventajas son varias: es un protocolo complejo, su configuración es complicada y requiere la intervención del cliente para su configuración.

A pesar de estos inconvenientes IPSec está teniendo una gran difusión en las redes actuales debido a la seguridad que proporciona tener los datos encriptados.

Implementación MPLS

MPLS (Multiprotocol Label Switching/ Multiprotocolo de Conmutación Etiquetado) es un protocolo que se encapsula entre la capa de red y la capa de enlace de datos. Básicamente lo que se consigue es decrementar el tiempo de resolución del *salto siguiente (next-hop)* para los paquetes IP. Este protocolo habilita a los proveedores de servicios a enviar diferentes VPNs sobre una simple infraestructura compartida, redireccionando el tráfico que no transita por el camino más corto,

El protocolo de señalización usado para MPLS es *RSVP (Reserved Source Virtual Protocol / Protocolo Virtual de Recursos Reservados)*. Este protocolo es un estándar en Internet para la reserva de recursos. Con RSVP se pueden reservar anchos de banda mínimos, se permite la gestión del tráfico según su origen y según su tipo. Actualmente representa la forma más completa y sencilla de implementación de técnicas de ingeniería de tráfico.

Las VPNs implementadas con MPLS sólo se aplican al Backbone del proveedor. Esto significa que el cliente sólo tiene que solicitarla y el proveedor se encargará de configurarla y de activarla sin afectar al cliente.

Las VPNs implementadas sobre una red MPLS contarán con una actividad baja. RSVP también permite técnicas de protección de los caminos MPLS, con lo que a pesar de la caída de algún enlace del Backbone del proveedor, no se apreciará la pérdida de conectividad en ningún instante, siempre y cuando exista un camino físico alternativo.

Este protocolo basa las VPN en la creación de una tabla de rutas distintas para cada VPN. Esta situación permite la reutilización del espacio de direcciones. Para los clientes esto añade una ventaja más, ya que puede crear una VPN sin necesidad de cambiar el direccionamiento de sus equipos.

4.3. Seguridad de Redes usando Firewalls

Algunos de los puntos más importantes en una red de comunicación son la seguridad de los datos que se envían por la red pública y de las prioridades de acceso de los usuarios internos. El acceso a los servicios estará determinado a través de un enlace privado de Internet, que tiene que ser autentificado por medio de los servidores de seguridad y el *Firewall (barrera de Fuego),* que nos permitirán validar la autentificación del usuario y en su acceso a los servicios que proporciona el Banco.

El proceso de acceso a la red del Banco, utilizando VPNs, se inicia cuando una persona trata de conectarse a los servicios que este presta, utilizando la red pública. Una vez iniciada la secuencia de autentificación, con la clave del usuario y su llave o contraseña para acceder al servidor de VPN, dicha información tiene que ser validada en la base de datos que está contenida en el servidor de control de acceso. Este servidor toma dicha información, la desencripta y la compara con la información que tiene almacenada en su base de datos, si esta información es la misma, valida el acceso y permite la comunicación.

La forma de proteger a la red privada a través de los Firewalls, considera que estos últimos poseen capacidad de encripción de VPN, ya sea integradas o como característica opcional. Este recurso ofrece a las empresas una alternativa sencilla y rentable en comparación con las líneas dedicadas tradicionales o el acceso remoto a través del modem. Al momento de implementar una VPN todos los dispositivos deben soportar el mismo nivel de encripción.

Como puede observarse en la *Figura 4.11,* el Firewall, de acuerdo a una estructura de direccionamiento, cambia las direcciones externas (direcciones públicas) para que puedan ser utilizadas en direcciones válidas dentro de la red del Banco (direcciones privadas). Para realizar esta función el PIX utiliza rutas estáticas y listas de acceso, que permitan realizar este procedimiento. Una vez que se validan las direcciones, el usuario puede obtener acceso a los servidores que contienen los servicios proporcionados por el Banco. Los Firewalls son equipos que nos ayudarán en la seguridad de la red. La pérdida de datos insustituibles es una amenaza real para cualquier empresa que conecta su red con el mundo exterior.

Un Firewall que posee una DMZ, *Figura 4.11*, provee protección efectiva para empresas que ofrecen a sus clientes la posibilidad de conectarse a su red, a partir de cualquier medio externo, ya sea a través de Internet o cualquier otra ruta. La decisión de optar por un Firewall con DMZ debe basarse en la cantidad de usuarios externos que acceden a la red y la frecuencia con la que lo hacen. Un Firewall con DMZ crea un área de información protegida en la red. Los usuarios externos pueden ingresar al área protegida, pero no pueden acceder al resto de la red. Esto permite a los usuarios externos acceder a la información a la que tienen permiso, pero previene que obtengan información no autorizada.

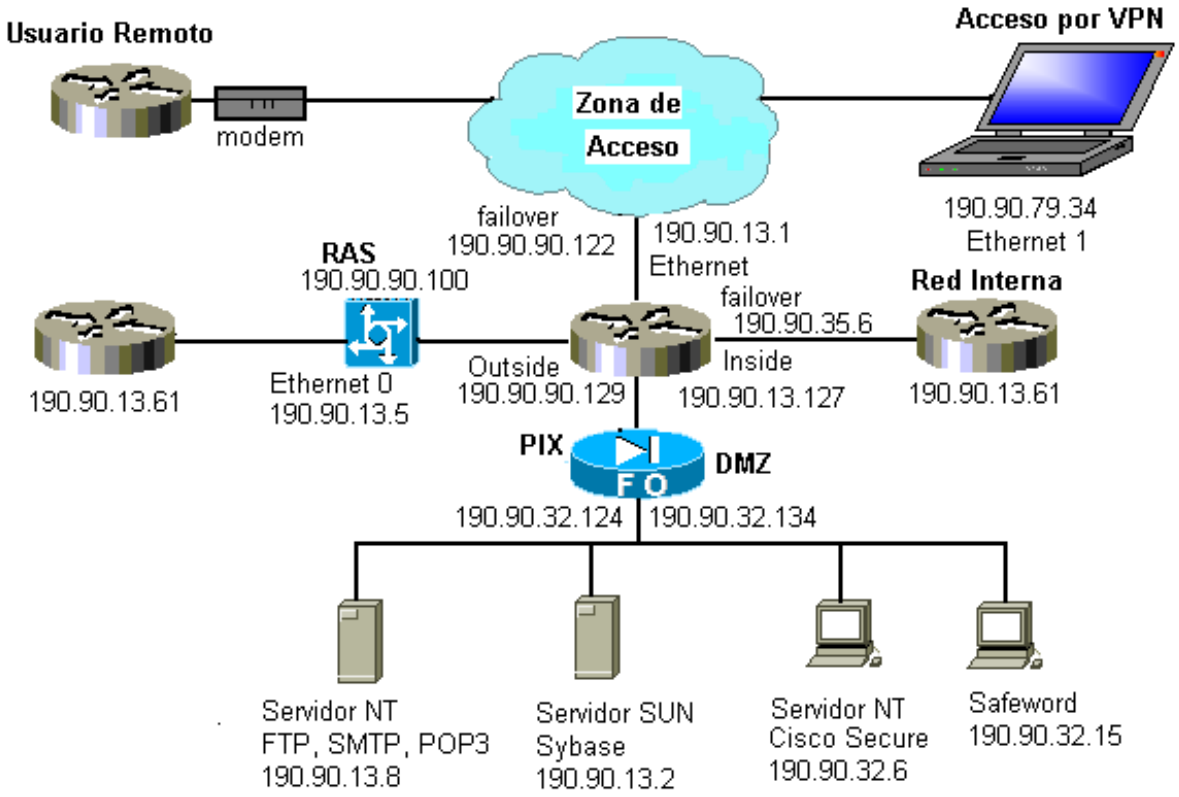

Figura 4.11. Esquema de conexión de usuarios remotos usando el PIX Firewall.

Un Firewall es un sistema que permite ejercer políticas de control de acceso entre dos redes, por ejemplo: una red LAN privada y una red pública (como Internet). El Firewall define los servicios que pueden accederse desde el exterior y viceversa. Los medios a través de los cuales se logra esta función varían notoriamente, pero en principio, un Firewall puede considerarse como un mecanismo para bloquear y permitir el tráfico.

En los siguientes puntos se presentarán la forma de configurar a un PIX Firewall para soportar redes VPNs. Para ello, permanentemente se definen las interfaces que el PIX utiliza como entradas hacia la red y cuales se utilizan como salidas, como se muestra en la siguiente configuración:

```
pixUno#
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 DMZ-Slot:2 security10
nameif ethernet3 DMZ-Slot:3 security20
```

También se proporciona un nivel de seguridad tanto para las entradas como para las salidas, siendo 0 el valor mínimo con seguridad nula y 100 el máximo; para nuestro caso consideramos un nivel de seguridad de 100. La conexión de seguridad en la red utilizando VPNs a través de los PIX Firewall se muestra en la *Figura 4.12.*

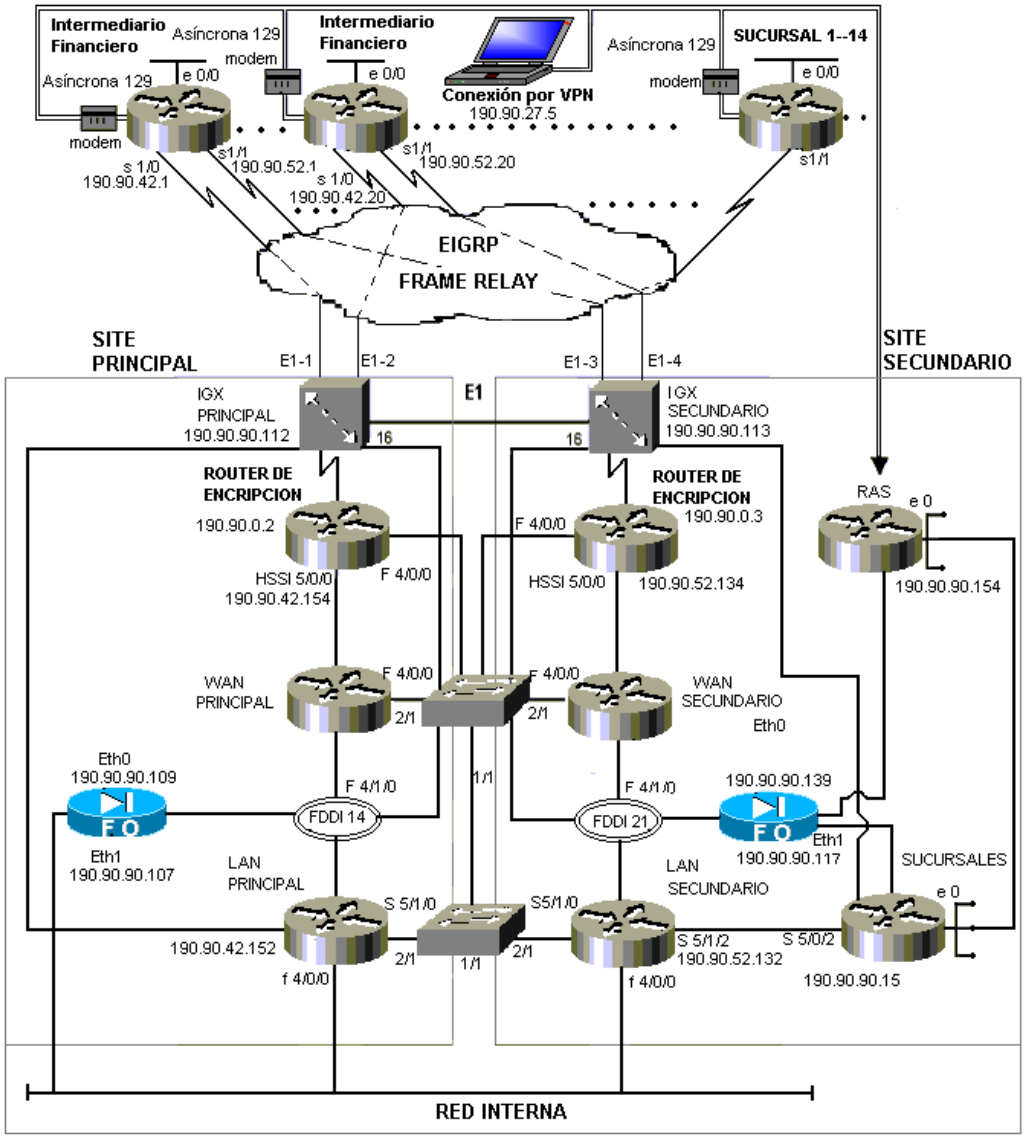

Figura 4.12. Esquema completo de Conexión de usuarios remotos usando el PIX Firewall.

Dentro del PIX Firewall modelo 525 que utilizamos, se configuraron DMZs. Dentro de la configuración se incluye el slot 2, donde está alojada físicamente la tarjeta que contiene las interfaces DMZ, y el nivel de seguridad que establece la posibilidad de acceder a la información. La configuración propuesta para las interfaces donde están soportadas las DMZ se presenta a continuación:

```
PixUno(config)#
nameif ethernet2 DMZ-Slot:2 security10
nameif ethernet3 DMZ-Slot:3 security20
PixUno#
```

Una vez establecidas, tanto las interfaces que se utilizan como entradas y salidas en el PIX como las DMZs, debemos configurar las direcciones IP para las interfaces de salida y de entrada, así como las direcciones para las DMZs que permitirán el acceso a los servidores de producción de la Red Interna del Banco. La configuración de estos puntos se presenta a continuación:

```
PixUno(config)#
ip address outside 190.90.90.129 255.255.255.0
ip address inside 190.90.13.127 255.255.255.0
ip address DMZ-Slot:2 190.90.134. 255.255.255.0
ip address DMZ-Slot:3 192.168.1.3 255.255.255.240
PixUno#
```

Para validar las direcciones de las interfaces de entrada y salida en el PIX se utilizan rutas estáticas, así la forma de configuración queda definida de la siguiente manera:

```
pixUno(config)#
static (inside,outside) 190.90.79.126 190.90.10.22 netmask 255.255.255.255 0 0
static (inside,outside) 190.90.79.123 190.90.10.39 netmask 255.255.255.255 0 0
static (inside,outside) 190.90.79.122 190.90.10.62 netmask 255.255.255.255 0 0
pixUno#
```

Una vez establecidos estos puntos en el esquema de configuración del PIX, se deben configurar las listas de acceso que nos permitan validar las direcciones externas que pueden acceder a la red. Esto nos servirá también para definir que es lo que los usuarios puede realizar o que servicios puede manipular. Por ejemplo, se puede definir para una IP propuesta 190.90.79.0 que corresponde a la VPN, la cual puede acceder a cualquier parte de la red. De la misma manera se permite el paso del usuario con IP 190.90.13.61 al servidor, por medio del puerto 1563. La configuración para otras computadoras se muestra a continuación:

```
pixUno(config)#
access-list vpn permit ip 190.90.79.0 255.255.255.0 any
access-list CSM-acl-DMZ-Slot:3 permit ip any any
access-list CSM-acl-inside permit icmp any any echo-reply
access-list CSM-acl-inside permit tcp host 190.90.13.61 host 192.90.13.5 eq 1467
access-list CSM-acl-inside permit ip host 190.90.21.45 any
access-list CSM-acl-inside permit ip host 190.90.27.132 any
access-list CSM-acl-inside permit ip host 190.90.27.139 any
pixUno#
```

Finalmente, para el caso de las tarjetas Ethernet, que sirven para soportar tanto el tráfico entrante como saliente en el PIX, se configuran utilizando el comando failover y la dirección propuesta:

```
pixUno(config)#
failover
failover timeout 0:00:05
failover poll 5
failover ip address outside 190.90.90.129
failover ip address inside 190.90.90.127
failover ip address DMZ-Slot:2 190.90.134
failover ip address DMZ-Slot:3 190.90.90.133
pixUno#
```

Lo descrito anteriormente nos permite concluir con el diseño de nuestra solución, para el siguiente capítulo presentaremos la forma de implementarlo.

CAPÍTULO 5

IMPLEMENTACIÓN DEL SISTEMA

En este capítulo se describe la implementación del sistema, estableciendo la configuración requerida en cada dispositivo que conforma la Red, y así mismo se presentan las pruebas desarrolladas y las gráficas del comportamiento de los enlaces.

5.1. Reglas Generales al instalar el Equipo de Comunicaciones

En la instalación del equipo de comunicaciones se siguieron los siguientes pasos:

1. Solamente personal calificado pudo instalar, reemplazar y dar servicio al equipo.
2. Se verificó que no esté en uso, ya que podría perderse información.
3. Se desconectó el cable de alimentación de energía antes de remover cualquier cubierta, ya que podría existir peligro de una descarga eléctrica.
4. Nunca se trabajó cuando hubo peligro de descarga eléctrica.
5. Nunca se dio por hecho que un circuito eléctrico estuvo desconectado, siempre se verificó que los circuitos elécticos no tuvieran energía.
6. Se revisó cuidadosamente cualquier posible punto de riesgo en la instalación, como humedad, contactos eléctricos no aterrizados, extensiones de cables, etc.

Se tomó en cuenta que en caso de accidente eléctrico, se debía proceder de la siguiente forma:

- Tener mucho cuidado de no tocar a la persona accidentada, para no sufrir una descarga.
- Apagar el interruptor del chasis y desconectar cualquier fuente de energía eléctrica.
- Si fuera necesario, solicitar asistencia médica, informando la causa el accidente.

Una vez tomadas las precauciones anteriores, se procedió a ver la manera de instalar un equipo de comunicaciones. Describiremos un solo equipo, ya que con todos se procedió de la misma forma.

5.1.1. Instalación del Router Cisco

Se tienen que seguir los siguientes pasos, para no tener problemas durante la instalación del equipo:

- Asegurarse que la energía eléctrica esté disponible en el Site y cerca de donde se va a instalar el router.
- Asegurarse que todos los componentes estén presentes.
- Anotar cómo estará colocado el router en él site y cuáles serán sus conexiones.

Colocar abrazaderas al Router

El router Cisco se instala en el Rack correspondiente, con dos abrazaderas que se pueden colocar tanto en la parte delantera como en la trasera del chasis del router, *Figura 5.1.* Al instalar también canaletas para el acomodo de cables, se verificó su correcta colocación.

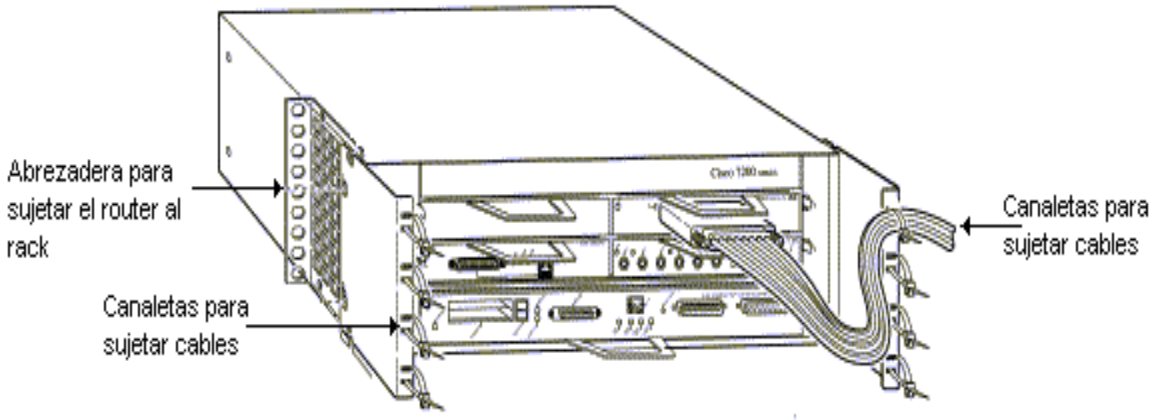

Figura 5.1. Forma de instalar abrazaderas al router Cisco.

Montar el router en el Rack

Al instalar el router en el Rack, *Figura 5.2,* se tuvo cuidado de utilizar los tornillos y las herramientas adecuadas para no lastimar el Rack y que el equipo quede firme.

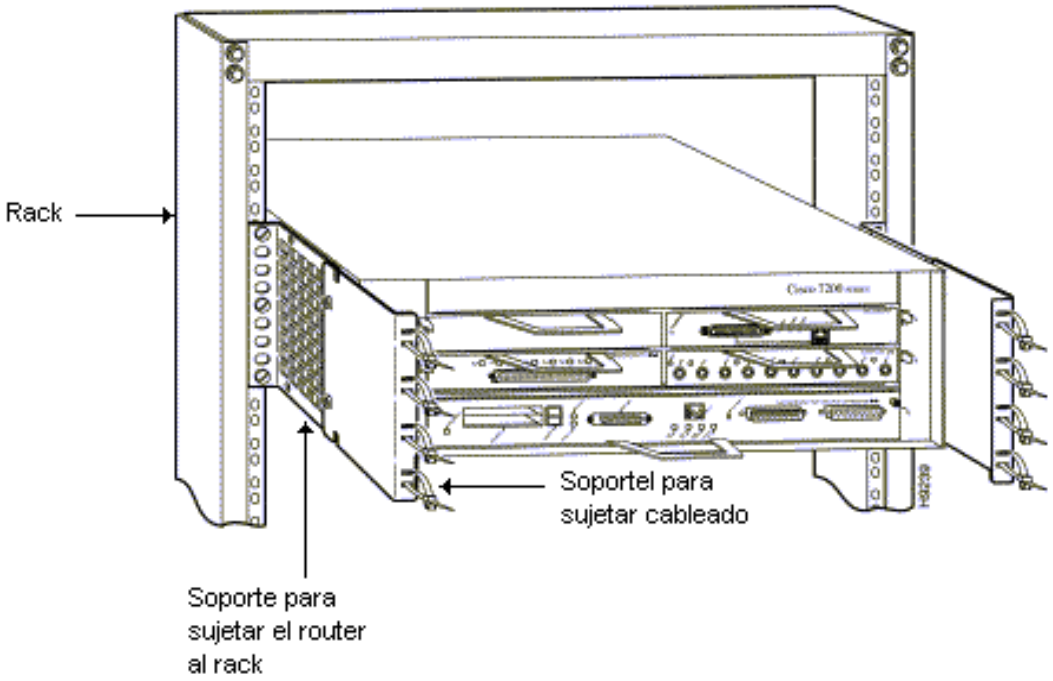

Figura 5.2. Forma de instalar el router Cisco en el Rack.

Conexión de Cables

Al colocar los cables es conveniente colocarlos primero del lado del router, para ello se procede con la siguiente secuencia:

Paso 1. Es importante colocar los cables en las interfaces adecuadas. En las *Figuras 5.3. a 5.10,* podemos ver algunos ejemplos de los diferentes cables que se utilizan para conectar los routers.

Interfaz Ethernet 10BASE-T de 4 u 8 puertos:

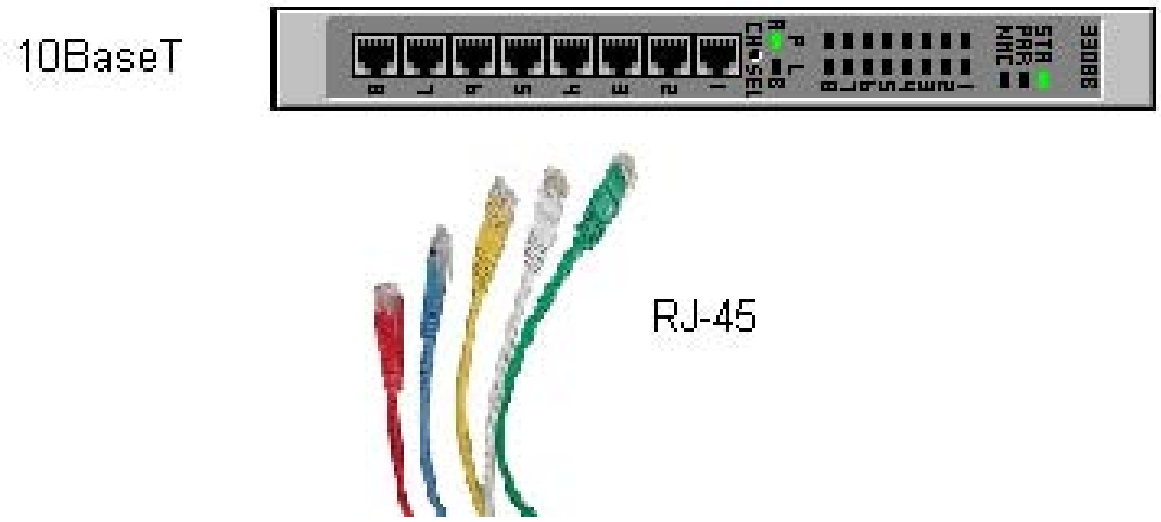

Figura 5.3. Interfaz Ethernet 10BASE-T de 4 u 8 puertos.

Interfaz Ethernet 10BASE-FL:

Figura 5.4. Interfaz Ethernet 10BASE-FL.

Interfaz Serial Síncrona:

Figura 5.5. Interfaz Serial Síncrono.

Interfaz Token Ring:

Figura 5.6. Interfaz Token Ring.

Interfaz Fast Ethernet 100BASE-TX:

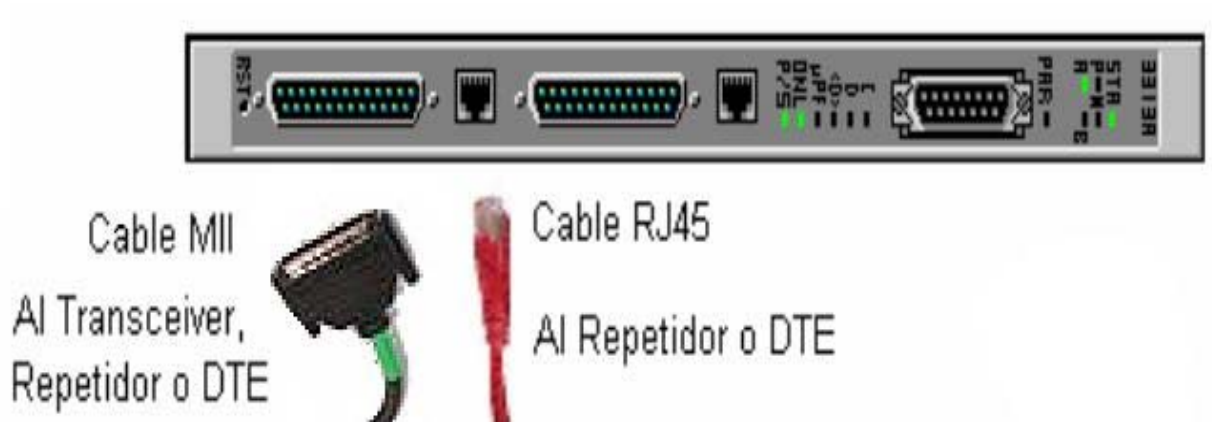

Figura 5.7. Interfaz Fast Ethernet 100BASE-TX.

Interfaz Fast Ethernet 100BASE-FX:

Figura 5.8. Interfaz Fast Ethernet 100BASE-FX.

Interfaz FDDI Multimodo:

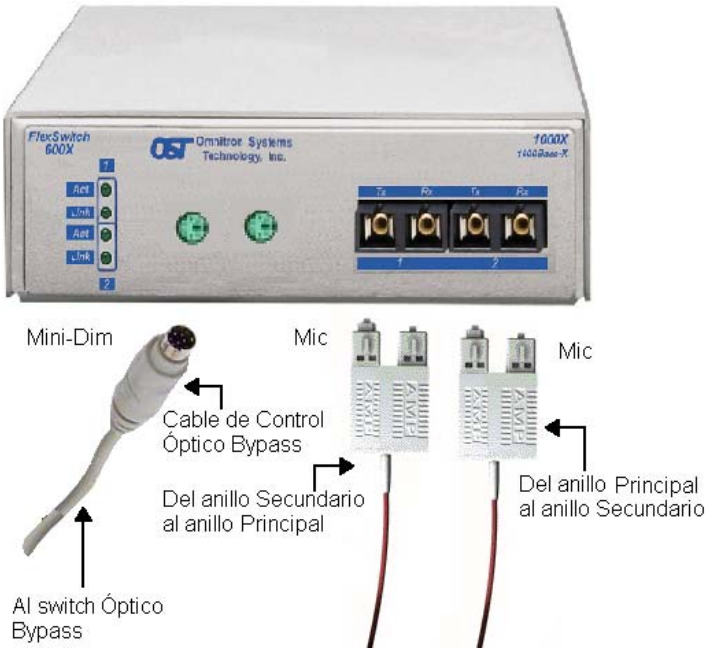

Figura 5.9. Interfaz FDDI Multimodo.

Interfaz FDDI Modo Sencillo:

Figura 5.10. Interfaz FDDI Modo Sencillo.

Paso 2. Conectar los cables Fast Ethernet, de la consola y auxiliares, a la tarjeta controladora I/O; La posición de los cables se puede ver en la *Figura 5.11.*

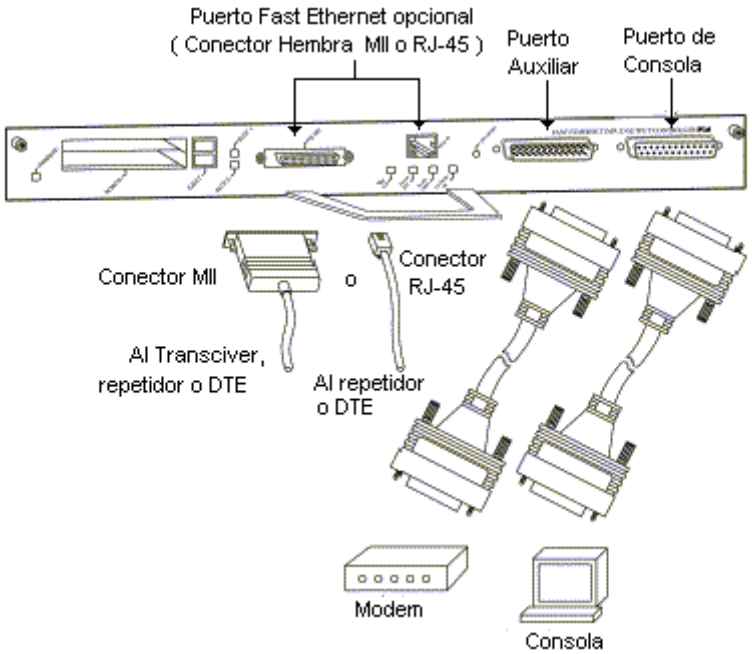

Figura 5.11. Conexión de los cables en el router.

Paso 3. Conectar la energía eléctrica al router. La colocación del cable se muestra en la *Figura 5.12.* Es muy importante colocar el clip de retención del cable, para evitar que por descuido se desconecte la energía eléctrica.

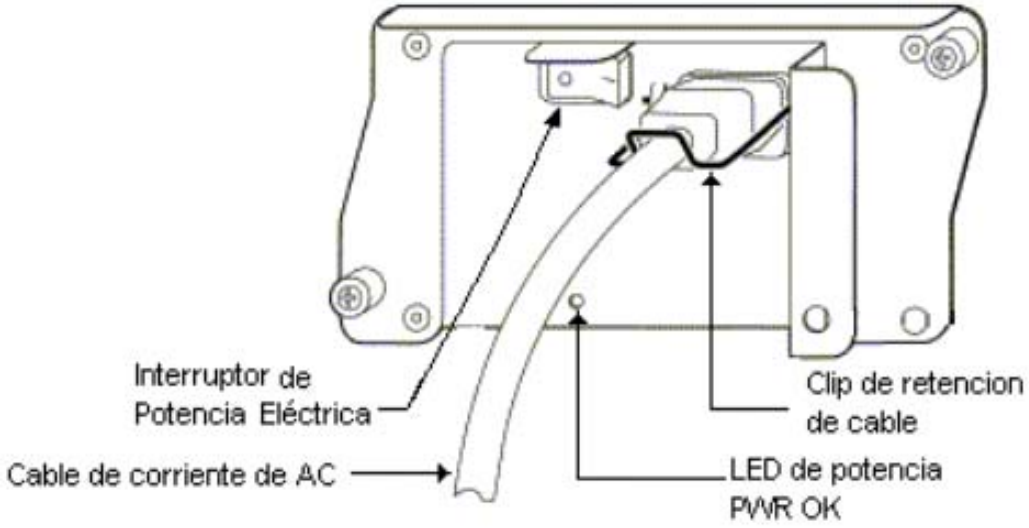

Figura 5.12. Conexión de la Energía Eléctrica.

5.1.2. Arranque del Router

La secuencia para poner en operación al router es la siguiente:

Paso 1. Colocar el interruptor de energía eléctrica en posición de encendido. El Led verde de OK se enciende y los ventiladores comienzan a funcionar.
Paso 2. Observar los indicadores (Leds) de la tarjeta controladora I/O, dicha tarjeta está insertada en la parte posterior del router, y los indicadores, dependiendo del modelo, se encuentran en la parte posterior o en la parte frontal del router. Para este modelo en particular, los indicadores están dispuestos como se ve en la *Figura 5.13.*

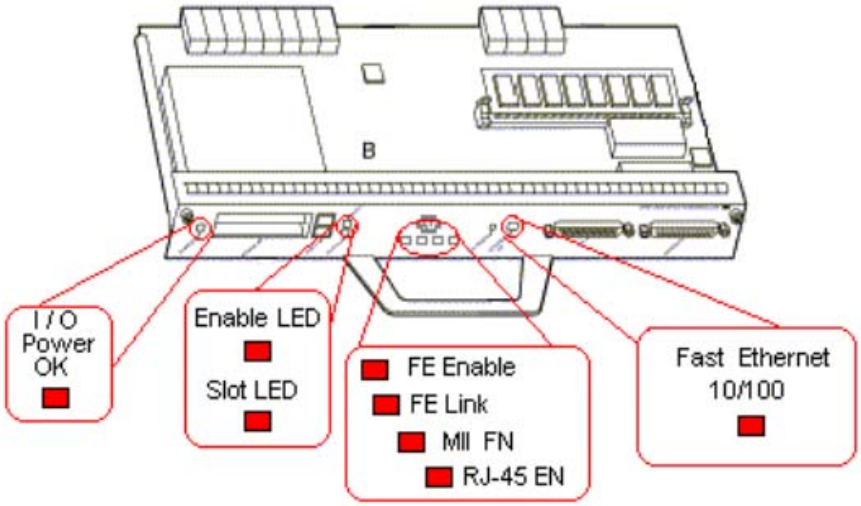

Figura 5.13. Indicación de los Leds de la Tarjeta Controaldora I/O.

A continuación se muestran las indicaciones de los Leds:

- IO Power OK. Indica que la tarjeta controladora I/O está recibiendo energía. Se enciende durante el inicio y así permanece mientras no se apague el equipo.
- Enabled Led. Indica que la tarjeta controladora I/O está operando. Se enciende durante el inicio y así permanece durante la operación.
- Slot Leds. Al parpadear indican actividad de la tarjeta. Debe estar encendida durante el inicio, y después parpadeando.
- Leds del puerto Fast Ethernet. Encendidos después de que se prendió el aparato.
    - FE Enable. Indica que el puerto está operando.
    - FE Link. Indica que el puerto ha establecido conexión con la red. ON indica actividad de red en el puerto.
    - MII EN. Indica que el receptor del puerto MII está en operación (después de que se ha configurado).
    - RJ-45 EN. Indica que el receptor del puerto RJ-45 ha establecido una conexión válida con la red. ON indica actividad de red en el puerto a través del receptor del conector RJ-45.

Algunos de los Leds del adaptador no se encenderán a menos que se hayan configurado dichas interfaces. Es muy importante que se escuchen los ventiladores del router o que los Leds muestren algún tipo de actividad, de otra manera es indicativo que hay problemas en el equipo.

Los demás equipos como el router, el RAS y el PIX Firewall, se instalan en el Rack de manera similar. Asimismo, los cables, los conectores y los indicadores son similares, por ello no se menciona su instalación.

5.2. Configuración de los Equipos

Una vez instalados los equipos en la posición que les corresponde, procedemos a su configuración. Para preparar los routers que serán utilizados en la encripción, se debe seleccionar el sistema operativo de Cisco adecuado para tal propósito, para nuestro caso se utilizó el sistema operativo IOS rsp-jsv40-mz.m3, el cual soporta la encripción de datos.

En la siguiente descripción solamente se presentará la configuración para el router de Encripción Principal, ya que la configuración es la misma para el router Secundario. También se presenta la configuración del servidor de acceso remoto RAS y la configuración del PIX Firewall.

Las configuraciones incluyen los aspectos más importantes, como son: las prioridades de los equipos dentro de la red, la traslación de direcciones para acceder a la Red Interna y la forma de realizar la autentificación de los usuarios que accesan a la Red Financiera del Banco. Estas configuraciones típicas se describen en los siguientes apartados:

5.2.1. Configuración del Router de Encripción Principal

```
¡
Current configuration:
!
! Last configuration change at 21:02:15 CDT Mon Sep 1 2003 by Admin1
! NVRAM config last updated at 21:02:21 CDT Mon Sep 1 2003 by Admin1
!
version 12.0
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service linenumber
no service udp-small-servers
no service tcp-small-servers
!
hostname Encrip_ Princ
!
boot system flash slot0:rsp-jsv40-mz.m3
enable secret 5 $1$/7r4$BqhCzowl3CmtDX2wewJRi1
enable password 7 0707D204256001A0A
ip tcp synwait-time 5
no ip domain-lookup
ip classless
!
clock timezone CDT –6
clock summer-time CDT recurring
ntp clock-period 17179648
ntp server 190.90.12.130
!
aaa new-model
aaa authentication local-override
aaa authentication login default tacacs+ lenable
aaa authentication exec if-autenticated tacacs+ none
aaa authentication commands 15 tacacs+ none
aaa accounting commands 0 wait-start tacacs+
aaa accounting commands 15 wait-start tacacs+
aaa accounting system stop-only tacacs+
aaa accounting suppress null-username
tacacs-server host Encrip_Princ
tacacs-server key Secret Ingenieria03
snmp-server community FIngenieria RW
username root privilege 15 password 7 00261B1539417
ip subnet-zero
ip tcp synwait-time 5
crypto cisco entities 20
!
```

```
ip host Lan Principal 190.90.42.152
ip host Lan Secundario 190.90.52.132
ip host Wan Principal 190.90.42.154
ip host Wan Secundario 190.90.52.134
!
!
crypto cisco connections 34
!
crypto cisco key-timeout 1350
!
named-key Intermediario1 signature
key-string
8B49340E 271F5B86 F74C7443 6788DE02 DF2852ED F8BF17F4 6AD22981
C0C75EC7 8CDA969D C12FCB5C DE43B65F B12A24C3 7410E468 BF67CEFC
72CAC51C5 2 D15A8D9
quit
!
!
named-key Intermediario2 signature
key-string
!
1FBDB4C8 5C7C93C 4EBC6107 C88F2BD8 6788DE02 D29017D6 2A01A227
B7F87E407 5F724EB0 246FA23F 1D15A8D9 A76751D9 F42BB00D 06863F78
F231A521
quit
!
named-key Intermediario3 signature
key-string
8B49340E 271F5B86 F74C7443 6788DE02 DF2852ED F8BF17F4 6AD22981
C0C75EC7 65f761EBA C12FCB5C DE43B65F B12A24C3 7410E468 BF67CEFC
72CAC51C5 2 D15A8D9
quit
!
named-key Intermediario19 signature
key-string
6B134270 98A58D57 2F80EFF5 3C2682C6 E7CB95F3 2EE16065 54BCDA4A
F4A4F9E4 8CDA969D E4AAA0C6 40D7EDAF 776204FB 823316B1 BFE12D43
6E731088 DE835295
  quit
!
named-key Intermediario20 signature
key-string
6FB4C9FC B05DE9C0 B2FA8A51 FFCC4277 448F8BD4 4F6FFE50 9EB47A3B
BC3272A8 382E721E 61AD4A70 320D99D6 0E072858 BDC209E9 742DC3A9
37223168 F4B6440B
  quit
!
```

!
!
!
crypto key pubkey-chain dss
!
!
named-key Sucursal1 signature
serial-number 36402539
key-string
4A2362BB AACDC6F5 CA2E4E3E 70A5D87D B6E733EF 34A90831 1F4535AD 5681E494 4FA87E06 EA771A84 342A4EC DC22BB 98 125F7A19 75DOC5F3 50A23DF1 B725B627
quit
!
!
!
named-key Sucursal2 signature
serial-number 05489765
key-string
E9E3E9BC 5B5567AF 11AF1876 3E97F796 92FA093C 6D62AA92 3770C760 C410327F 523D66E3 5651238A CA00F9BD 67E69295 AC4D4A09 22B36810 12319C4A 7D4D3D7A
quit
!
!
!
named-key Sucursal3 signature
serial-number 052687910
key-string
C6ACF1EF F9E8A5F2 8FBC209D 8D932643 9DA20B7A 5E49D2C6 BD0DD351 98A45FF3 4E7C3A31 103EFD25 C687B584 536BAD35 5EB66CD2 450F5FDB 70DD3FF6 3A3F7322
quit
!
!
!
named-key Sucursal 13 signature
serial-number 012476034
key-string
ED43BAAC EFFACBA1 08D66F1F F02C86FD 4D213CB7 5F2005C0 B65F770C B80BD76A AAD5B6C3 C1EB708E 878B57AF 8FE21FA7 684DED85 77231280 6CB99CFF AF94F41B
Quit
!
named-key Sucursal14 signature
serial-number 072584691
key-string

6163499E A7700C97 4AB62DA0 4208C4C7 25DA7A8A 4364E09F 48A75F7E 27DCED23 FE578DA1 B1C8228E 149A7AE4 11C28AB6 D4729F7F 0AE4704C DA9BE800 3DD2A16A
quit
!
!
!
clock timezone CDT -6 4
clock summer-time CDT recurring
!
!
!
interface FastEthernet4/0/0
description enlace con el router Wan Principal
ip address 190.90.90.112 255.255.255.252 Principal
ip address 190.90.90.113 255.255.255.252
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
full-duplex
no cdp enable
!
interface Hssi4/1/0
description interfaz hacia el IGX Principal
ip address 190.90.42.134 255.255.255.0 Secondary
ip address 190.90.42.135 255.255.255.0
no ip directed-broadcast
encapsulation frame-relay
no ip route-cache
no ip mroute-cache
frame-relay lmi-type ansi
frame-relay broadcast-queue 120 256000 72
hold-queue 150 in
!
no ip classless
ip host Lan Principal 190.90.42.152
ip host Lan Secundario 190.90.52.132
ip host Wan Principal 190.90.42.154
ip host Wan Secundario 190.90.52.134
!
!
ip route 190.90.90.0 255.255.255.0 190.90.90.112
ip route 190.90.25.4 255.255.255.255 190.90.90.112
ip route 190.90.26.7 255.255.255.255 190.90.90.112
ip route 190.90.22.19 255.255.255.255 190.90.90.112
ip route 190.90.90.0 255.255.255.0 190.90.90.112
!

```
!
!
interface Tunnel1
ip unnumbered FastEthernet5/1/0
bandwidth 64
tunnel source FastEthernet5/1/0
tunnel destination 190.90.42.1
!
interface Tunnel2
ip unnumbered FastEthernet5/1/0
bandwidth 64
tunnel source FastEthernet5/1/0
tunnel destination 190.90.42.2
.
.
interface Tunnel21
ip unnumbered FastEthernet5/1/0
bandwidth 64
tunnel source FastEthernet5/1/0
tunnel destination 190.90.42.21
.
.
interface Tunnel40
ip unnumbered FastEthernet5/1/0
bandwidth 64
tunnel source FastEthernet5/1/0
tunnel destination 190.90.42.40
!
¡
ip access-list extended Sucursal1
permit gre host 190.90.0.2 host 190.90.42.1
ip access-list extended Sucursal 2
permit gre host 190.90.0.2 host 190.90.42.2
ip access-list extended Sucursal 3
permit gre host 190.90.0.2 host 190.90.42.3
.
.
ip access-list extended Sucursal 13
permit gre host 190.90.0.2 host 190.90.42.13
ip access-list extended Sucursal 14
permit gre host 190.90.0.2 host 190.90.42.14
!
!
ip access-list extended Intermediario1
permit gre host 190.90.0.2 host 190.90.42.21
ip access-list extended Intermediario2
permit gre host 190.90.0.2 host 190.90.42.22
```

```
ip access-list extended Intermediario3
permit gre host 190.90.0.2 host 190.90.42.23
.
.
ip access-list extended Intermediario19
ip permit gre host 190.90.0.2 host 190.90.42.39
ip access-list extended Intermediario20
permit gre host 190.90.0.2 host 190.90.42.40
!
!
interface FastEthernet2/0/0
description Interfaz al router Wan principal
ip address 190.90.42.154 255.255.255.252 secondary
ip address 190.90.52.134 255.255.255.252
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
full-duplex
no cdp enable
!
interface Hssi4/1/1
description Interfaz hacia el IGX Secundario
ip address 190.90.90.122 255.255.255.0 secondary
ip address 190.90.90.134 255.255.255.0
no ip directed-broadcast
encapsulation frame-relay
no ip route-cache
no ip mroute-cache
frame-relay lmi-type ansi
frame-relay broadcast-queue 120 256000 72
hold-queue 120 in
!
logging trap warnings
logging 170.70.32.16
logging 190.90.32.15
logging 170.70.32.14
access-list 10 permit 190.90.90.123
access-list 10 permit 190.90.90.124
access-list 10 permit 190.90.90.125
access-list 10 permit 190.90.90.127
access-list 10 permit 190.90.90.126
access-list 10 permit 190.90.90.128
access-list 101 permit gre host 190.90.90.112 host 190.90.42.1
access-list 102 permit gre host 190.90.90.112 host 190.90.42.2
access-list 103 permit gre host 190.90.90.112 host 190.90.42.3
access-list 104 permit gre host 190.90.90.112 host 190.90.42.4
access-list 105 permit gre host 190.90.90.112 host 190.90.42.5
```

```
access-list 106 permit gre host 190.90.90.112 host 190.90.42.6
access-list 107 permit gre host 190.90.90.112 host 190.90.42.7
access-list 133 permit gre host 190.90.90.112 host 190.90.42.39
access-list 134 permit gre host 190.90.90.112 host 190.90.42.40
no cdp run
snmp-server community 08fdhtyañopc23 RW 30
snmp-server location Principal
snmp-server enable traps config
snmp-server enable traps envmon
snmp-server enable traps frame-relay
snmp-server enable traps syslog
snmp-server host 190.90.90.125 traps fimex01
snmp-server host 190.90.90.127 traps fimex01
snmp-server host 190.90.90.126 traps fimex01
snmp-server host 190.90.90.128 traps fimex01
!
tacacs-server host 190.90.90.95
tacacs-server host 190.90.90.97
tacacs-server key secret 28768
privilege exec level 1 send
privilege exec level 7 traceroute
privilege exec level 7 ping
privilege exec level 1 terminal monitor
privilege exec level 1 terminal
privilege exec level 1 show line
privilege exec level 7 show frame-relay pvc
privilege exec level 7 show frame-relay map
privilege exec level 7 show frame-relay
privilege exec level 7 show protocols
privilege exec level 1 show ip eigrp neighbors
privilege exec level 7 show ip eigrp
privilege exec level 7 show ip route
privilege exec level 7 show ip
privilege exec level 7 show interfaces
privilege exec level 1 show startup-config
privilege exec level 1 show running-config
privilege exec level 7 show
privilege exec level 1 clear ip route *
privilege exec level 7 clear ip route
privilege exec level 7 clear ip
privilege exec level 7 clear arp-cache
privilege exec level 7 clear
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
```

transport input all
stopbits 1
flowcontrol hardware
line vty 0 4
access-class 7 in
exec-timeout 0 0
password 7 071A2F455D100A
line vty 5 10
access-class 7 in
exec-timeout 0 0
password 7 057B4C827F349E
ntp clock-period 17179753
ntp server 190.90.13.86
end

5.2.2. Configuración del RAS actual

!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec localtime
service password-encryption
service linenumber
service internal
!
hostname RASactual
!
logging buffered warnings
no logging console
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization network default group tacacs+ local
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
enable secret 5 1Dyl9$lMO4MYxhgcYvKgih3e6sF
!
username fimex1 password 7 085D5435071B0015
username fimex2 password 7 9050B061005E1081C5C
username fimex3 password 7 104C1316045F1E
username fimex5 password 7 11041617161E580E
username fimex6 password 7 6011A80E1314051D54
!
username Jgarcia password 7 1191218F053A10
username Nmazas password 7 A1C1710E141D241F
username Smorales password 7 104C08125C51

```
username Eavila password 7 121E1A0C151916057E
username Ovaldiviezo password 7 1C514840419F4A
!
username fimex39 password 7 11041617161E580E
username fimex40 password 7 6011A80E1314051D54
!
spe 1/0 1/9
firmware location system:/ucode/mica_port_firmware
!
resource-pool disable
!
clock timezone CDT -6
clock summer-time CDT recurring
ip subnet-zero
ip tcp synwait-time 5
no ip domain-lookup
!
ip address-pool local
chat-script offhook "" "ATH1" OK
chat-script callback ABORT ERROR ABORT BUSY "" "ATZ" OK "ATDT \T" TIMEOUT
30 CONNECT \c
!
controller E1 2
framing NO-CRC4
clock source line primary
 ds0-group 1 timeslots 1-14,20-31 type r2-digital r2-compelled
 cas-custom 1
  country mexico use-defaults
 category 2
 answer-signal group-b 1
!
controller E1 2
clock source line Secondary 1
!
controller E1 3
!
controller E1 4
!
interface Loopback0
ip address 190.13.5.134 255.255.255.0
!
interface Ethernet0
ip address 190.90.35.134 255.255.255.0
ip nat outside
no ip route-cache
no ip mroute-cache
!
```

```
interface FastEthernet0
description interfaz de acceso remoto externo
ip address 190.90.90.154 255.255.255.0
ip access-group 149 in
no ip route-cache
no ip mroute-cache
duplex full
speed 100
!
interface Group-Async1
ip unnumbered Loopback0
ip nat inside
encapsulation ppp
dialer in-band
dialer idle-timeout 900
dialer map ip 190.90.90.1 name fimex1 #52#
dialer map ip 190.90.90.2 name fimex2 #89#
dialer map ip 190.90.90.3 name fimex3 #37#
.
.
.
dialer map ip 190.90.90.12 name fimex12 #24#
dialer map ip 190.90.90.13 name fimex13 #15#
dialer map ip 190.90.90.14 name fimex14 #32#
dialer map ip 190.90.90.20 name Jgarcia #26#
dialer map ip 190.90.90.21 name nmazas #11#
dialer map ip 190.90.90.22 name smorales #26#
dialer map ip 190.90.90.23 name eavila #34#
dialer map ip 190.90.90.24 name ovaldiviezo #43#
.
.
dialer map ip 190.90.90.39 name usuario39 #22#
dialer map ip 190.90.90.40 name usuario40 #12#
!
dialer-group 2
async default routing
async mode dedicated
peer default ip address pool default
no cdp enable
ppp callback accept
ppp authentication pap chap
group-range 1 60
!
ip local pool default 190.90.90.2 190.90.90.24
ip nat inside source static 192.90.10.111 190.90.90.5
ip nat inside source static 192.90.10.2 190.90.90.112
ip nat inside source static 192.90.10.3 190.90.90.113
```

```
ip nat inside source static 192.90.10.4 190.90.90.114
ip nat inside source static 192.90.10.5 190.90.90.115
ip nat inside source static 192.90.10.6 190.90.90.116
ip nat inside source static 192.90.10.7 190.90.90.117
ip nat inside source static 192.90.10.8 190.90.90.118
ip nat inside source static 192.90.10.9 190.90.90.119
ip nat inside source static 192.90.10.1 190.90.90.110
ip nat inside source static 192.90.10.1 190.90.90.6
ip nat inside source static 192.90.10.12 190.90.90.12
ip nat inside source static 192.90.10.13 190.90.90.13
ip nat inside source static 192.90.10.14 190.90.90.14
ip nat inside source static 192.90.10.15 190.90.90.15
ip nat inside source static 192.90.10.16 190.90.90.16
ip nat inside source static 192.90.10.17 190.90.90.17
ip nat inside source static 192.90.10.18 190.90.90.18
ip nat inside source static 192.90.10.19 190.90.90.19
ip nat inside source static 192.90.10.20 190.90.90.20
ip nat inside source static 192.90.10.9 190.90.90.9
ip nat inside source static 192.90.10.120 190.90.90.120
ip nat inside source static 192.90.10.8 190.90.90.8
ip nat inside source static 192.90.10.7 190.90.90.7
ip nat inside source static 192.90.10.12 190.90.90.12
ip nat inside source static 192.90.10.1 190.90.90.1
ip nat inside source static 192.90.10.4 190.90.90.4
ip nat inside source static 192.90.10.214 190.90.90.214
ip nat inside source static 192.90.10.215 190.90.90.215
ip nat inside source static 192.90.10.216 190.90.90.216
no ip classless
!
!
ip route 0.0.0.0 0.0.0.0 190.90.83.20
ip route 190.90.0.0 255.255.0.0 190.90.90.112
ip route 190.90.13.0 255.255.255.0 190.90.90.112
ip route 190.90.90.0 255.255.0.0 190.90.90.112
no ip http server
!
access-list 23 permit 190.90.27.254
access-list 23 permit 190.90.28.218
access-list 23 permit 190.90.1.192
access-list 23 permit 190.90.1.151
access-list 23 permit 190.90.31.125
access-list 23 permit 190.90.21.110
access-list 23 permit 190.90.70.25
access-list 23 permit 190.90.90.1.8
access-list 23 permit 190.90.90.118
access-list 23 permit 190.90.33.4
access-list 23 permit 190.90.21.50
```

access-list 23 permit 190.90.31.28
access-list 23 permit 190.90.27.3
access-list 23 permit 190.90.41.48
access-list 100 permit ip any any
access-list 101 permit ip 190.90.90.0 0.0.0.255 host 190.90.90.112
access-list 101 permit ip 190.90.90.0 0.0.0.255 190.90.90.2 0.0.0.255
access-list 101 permit ip 190.90.90.0 0.0.0.255 190.90.90.10 0.0.0.255
access-list 101 permit ip 190.90.90.0 0.0.0.255 148.243.228.0 0.0.0.255
access-list 101 permit icmp 190.90.90.1 0.0.0.255 host 190.90.90.2.0 echo
access-list 101 permit icmp 190.90.90.1 0.0.0.255 host 190.90.90.2.0 echo-reply
access-list 101 permit icmp 190.90.90.1 0.0.0.255 host 190.90.90.10.0 echo
access-list 101 permit icmp 190.90.90.1 0.0.0.255 host 190.90.90.10.0 echo-reply
access-list 101 permit icmp 190.90.90.1 0.0.0.255 host 148.243.228.0 echo
access-list 101 permit icmp 190.90.90.1 0.0.0.255 host 148.243.228.0 echo-reply
access-list 101 permit icmp 190.90.90.1 0.0.0.255 host 190.90.90.112echo
access-list 101 permit icmp 190.15.1.0 0.0.0.255 host 190.90.90.112 echo-reply
access-list 101 permit icmp any 190.90.0.0 0.0.255.255 echo
access-list 101 permit icmp any 190.90.0.0 0.0.255.255 echo-reply
access-list 101 permit ip any 190.90.90.110 0.0.0.255
access-list 101 permit ip any 190.90.35.0 0.0.0.255
access-list 105 deny icmp any any
access-list 105 permit ip any any
access-list 149 permit gre any host 190.90.90.174
access-list 149 permit esp any host 190.90.90.174
access-list 149 permit udp any eq isakmp host 190.90.90.174
dialer-list 2 protocol ip list 107
tacacs-server host 190.90.32.16
tacacs-server timeout 20
snmp-server community 08fdhtyañopc23 RW 30
snmp-server community public view v1default RO
snmp-server location RAS actual
snmp-server enable traps snmp
snmp-server enable traps isdn call-information
snmp-server enable traps config
snmp-servsnmp-server enable traps isdn layer2
snmp-server enable traps hsrp
er enable traps entity
snmp-server enable traps envmon
snmp-server enable traps frame-relay
snmp-server enable traps rtr
snmp-server enable traps syslog
line con 0
transport input none
line 1 60
exec-timeout 0 0
 autoselect ppp
 script callback callback

```
 refuse-message ^CC [!NMM!] Modem no disponible
 modem InOut
 modem autoconfigure type mica
 transport preferred none
 transport input all
 autohangup
line aux 0
line vty 0 4
 exec-timeout 0 0
 password 7 092341B4152C5D65752A20
!
end
```

5.2.3. Configuración del PIX Firewall

```
PIX Version 6.2
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 DMZ-Slot:2 security10
enable password 1kfhrm47cKloqtvN encrypted
hostname PIX_UNO
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
fixup protocol ftp strict 21
no names
access-list vpn permit ip 190.90.27.0 255.255.255.0 any
access-list CSM-acl-DMZ-Slot:2 permit ip any any
access-list CSM-acl-inside permit icmp any any echo-reply
access-list CSM-acl-inside permit tcp host 190.90.13.61 host 190.90.13.6 eq 1467
access-list CSM-acl-inside permit ip host 190.90.21.50 any
access-list CSM-acl-inside permit ip host 190.90.28.172 any
access-list CSM-acl-inside permit ip host 190.90.28.159 any
access-list CSM-acl-inside permit ip host 190.90.3.151 any
access-list CSM-acl-inside permit ip host 190.90.3.17 any
access-list CSM-acl-inside permit ip host 190.90.3.192 any
access-list CSM-acl-inside permit ip host 190.90.3.20 any
access-list CSM-acl-inside permit ip host 190.90.3.200 any
access-list CSM-acl-inside permit ip host 190.90.28.218 any
!
```

!
access-list CSM-acl-inside permit tcp host 190.90.5.113 host 190.90.32.2 eq smtp
access-list CSM-acl-inside permit tcp host 190.90.18.114 host 190.90.32.2 eq smtp
access-list CSM-acl-inside permit tcp host 190.90.5.116 host 190.90.32.2 eq smtp
access-list CSM-acl-inside permit tcp host 190.90.5.128 host 190.90.32.2 eq smtp
access-list CSM-acl-inside permit tcp host 190.90.21.225 host 190.90.32.1 eq ftp
access-list CSM-acl-inside permit tcp host 190.90.6.201 host 190.90.32.1 eq ftp
access-list CSM-acl-inside permit tcp host 190.90.9.128 host 190.90.32.1 eq ftp
access-list CSM-acl-inside permit tcp host 190.90.9.138 host 190.90.32.1 eq ftp
access-list CSM-acl-inside deny ip any any
access-list CSM-acl-outside permit icmp any any echo-reply
access-list CSM-acl-outside permit udp host 190.90.84.100 host 190.90.13.61 eq syslog
access-list CSM-acl-outside permit tcp host 190.90.90.201 host 190.90.90.238 eq 2030
access-list CSM-acl-outside permit tcp host 190.90.90.202 host 190.90.90.238 eq 2030
access-list CSM-acl-outside permit tcp host 190.90.90.200 host 190.90.90.250 eq 6505
access-list CSM-acl-outside permit tcp host 190.90.90.200 host 190.90.90.250 eq 6550
access-list CSM-acl-outside permit tcp host 190.90.90.253 host 190.90.32..3 eq tacacs
access-list CSM-acl-outside permit tcp any host 190.90.90.124 range 1020 1070
access-list CSM-acl-outside permit tcp any host 190.90.90.124 eq 124
access-list CSM-acl-outside permit tcp any host 190.90.90.124 eq netbios-ssn
access-list CSM-acl-outside permit tcp any host 190.90.90.124 eq pop3
access-list CSM-acl-outside permit tcp any host 190.90.90.124 eq smtp
access-list CSM-acl-outside permit tcp any host 190.90.90.230 eq www
access-list CSM-acl-outside permit icmp any host 190.90.90.240 echo
access-list CSM-acl-outside permit tcp any host 190.90.90.240 eq telnet
access-list CSM-acl-outside permit tcp any host 190.90.90.232 eq pop3
access-list CSM-acl-outside permit tcp any host 190.90.90.232 eq smtp
access-list CSM-acl-outside deny ip any any
access-list CSM-acl-DMZ-Slot:2 permit tcp host 192.168.3.1 any range 4035 4072
access-list CSM-acl-DMZ-Slot:2 permit tcp host 192.168.3.1 any range 3054 3056
access-list CSM-acl-DMZ-Slot:2 permit tcp host 192.168.3.2 any range 3021 3022
access-list CSM-acl-DMZ-Slot:2 permit tcp host 192.168.3.2 any range 5600 5601
access-list CSM-acl-DMZ-Slot:2 permit icmp any any echo-reply
access-list CSM-acl-DMZ-Slot:2 permit icmp host 190.90.32.5 any echo
access-list CSM-acl-DMZ-Slot:2 permit icmp host 190.90.32.1 any echo
access-list CSM-acl-DMZ-Slot:2 permit icmp 190.90.32.2 255.255.255.254 any echo
access-list CSM-acl-DMZ-Slot:2 deny ip any any
no pager
logging on
logging timestamp
logging trap debugging
logging history debugging
logging host inside 190.90.13.61
logging host DMZ-Slot:2 190.90.90.134
logging host inside 190.90.25.25
logging host inside 190.90.25.92
logging host inside 190.90.31.20

no logging message 302013
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
icmp permit any echo-reply outside
icmp deny any outside
icmp permit any echo-reply inside
icmp deny any inside
icmp permit any echo-reply DMZ-Slot:3
icmp deny any DMZ-Slot:2
icmp permit any echo-reply DMZ-Slot:3
icmp deny any DMZ-Slot:3
mtu outside 1500
mtu inside 1500
mtu DMZ-Slot:2 1500
mtu DMZ-Slot:3 1500
ip address outside 190.90.90.129 255.255.255.0
ip address inside 190.90.13.6 127 255.255.255.0
ip address DMZ-Slot:2 190.90.90.134 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool clientpool 190.90.90.210 190.90.90.219
failover
failover timeout 0:00:07 failover poll 5
failover ip address outside 190.90.90.122
failover ip address inside 190.90.35.6
failover ip address DMZ-Slot:2 190.90.32.124
pdm history enable
arp timeout 14400
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
nat (DMZ-Slot:2) 0 0.0.0.0 0.0.0.0 0 0
alias (inside) 190.90.32.2 190.90.32.2 255.255.255.255
alias (inside) 190.90.32.3 190.90.32.3 255.255.255.255
alias (inside) 190.90.32.1 190.90.32.1 255.255.255.255
alias (inside) 190.90.32.5 190.90.32.5 255.255.255.255
static (DMZ-Slot:2,outside) 192.90.2.1 190.90.32.1 netmask 255.255.255.0
static (DMZ-Slot:2,outside) 192.90.2.2 190.90.32.2 netmask 255.255.255.0
static (DMZ-Slot:2,outside) 190.90.32.3 190.90.32.3 netmask 255.255.255.0
static (inside,outside) 190.90.90.244 190.90.13.57 netmask 255.255.255.0
static (inside,outside) 190.90.13.61 190.90.13.61 netmask 255.255.255.0
static (inside,outside) 190.90.90.248 190.90.32.12008 netmask 255.255.255.0
static (inside,outside) 190.90.90.224 190.90.16.98 netmask 255.255.255.0
static (inside,outside) 190.90.90.225 190.90.16.99 netmask 255.255.255.0
static (inside,outside) 190.90.90.249 190.90.7.152 netmask 255.255.255.0
static (inside,outside) 190.90.90.242 190.90.21.105 netmask 255.255.255.0
static (inside,outside) 190.90.90.238 190.90.91.24 netmask 255.255.255.0

static (inside,outside) 190.90.90.207 190.90.13.35 netmask 255.255.255.0
static (inside,outside) 190.90.90.206 190.90.5.119 netmask 255.255.255.0
access-group CSM-acl-outside in interface outside
access-group CSM-acl-inside in interface inside
access-group CSM-acl-DMZ-Slot:2 in interface DMZ-Slot:2
route outside 0.0.0.0 0.0.0.0 190.90.90.253 1
route inside 190.90.5.0 255.255.255.0 190.90.32.120 1
route inside 190.90.19.0 255.255.255.0 190.90.32.120 1
route inside 190.90.7.0 255.255.255.0 190.90.32.120 1
route inside 190.90.21.0 255.255.255.0 190.90.32.120 1
route inside 190.90.22.0 255.255.255.0 190.90.32.120 2
route inside 190.90.23.0 255.255.255.0 190.90.32.120 2
route inside 190.90.28.0 255.255.255.0 190.90.32.120 2
route inside 190.90.31.0 255.255.255.0 190.90.32.120 1
route inside 190.90.33.0 255.255.255.0 190.90.32.120 2
route inside 190.90.38.0 255.255.255.0 190.90.32.120 2
route inside 190.90.91.0 255.255.255.0 190.90.32.120 2
route inside 190.90.92.0 255.255.255.0 190.90.32.120 1
timeout xlate 5:00:00
timeout conn 3:00:00 half-closed 0:12:00 udp 0:07:00 rpc 0:12:00 h323 0:07:00 sip 0:35:00 sip_media 0:02:00
timeout uauth 4:00:00 absolute uauth 0:05:00 inactivity
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa-server ACSTokenCards protocol tacacs+
aaa-server ACSTokenCards (DMZ-Slot:2) host 190.90.32.5 tokensfm4568 timeout 5
aaa-server tacacs+ protocol tacacs+
aaa-server CiscoSecure protocol tacacs+
aaa-server CiscoSecure (DMZ-Slot:2) host 190.90.32.3 ciscosecure timeout 5
aaa authentication include tcp/0 outside 190.90.32.16 255.255.255.255 0.0.0.0 0.0.0.0 ACSTokenCards
http server enable
snmp-server host inside 190.90.13.5
snmp-server host inside 190.90.13.8
snmp-server location facultad de Ingenieria
snmp-server community fimex1
snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set vpn esp-3des esp-sha-hmac
crypto dynamic-map uno 10 match address vpn1
crypto dynamic-map dos 10 set transform-set vpn1 vpn2
isakmp enable outside
isakmp key ******** address 0.0.0.0 netmask 0.0.0.0
isakmp identity address

```
isakmp client configuration address-pool local clientpool outside
isakmp policy 12 authentication pre-share
isakmp policy 12 encryption 3des
isakmp policy 12 hash md5
isakmp policy 12 group 3
isakmp policy 12 lifetime 86400
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 4
isakmp policy 10 lifetime 86400
vpngroup uno address-pool clientpool
vpngroup dos split-tunnel vpn
vpngroup uno idle-time 1800
telnet 190.90.32.2 255.255.255.255 inside
telnet 190.90.28.1 255.255.255.255 inside
telnet 190.90.70.2 255.255.255.255 inside
telnet 190.90.2.5 255.255.255.255 inside
telnet 190.90.3.1 255.255.255.255 inside
telnet 190.90.3.192 255.255.255.255 inside
telnet 190.90.3.17 255.255.255.255 inside
telnet 190.90.3.2 255.255.255.255 inside
telnet 190.90.12.7 255.255.255.255 inside
telnet 190.90.28.1 255.255.255.255 inside
telnet 190.90.28.9 255.255.255.255 inside
telnet 190.90.23.5 255.255.255.255 inside
telnet 190.90.13.10 255.255.255.255 inside
telnet timeout 5
ssh 190.90.31.28 255.255.255.255 inside
ssh timeout 60
terminal width 80
: end
[OK]
```

5.3. Configuración del Cliente de VPN

Para que un usuario se pueda conectar al banco a través de Internet, por medio de una conexión VPN, se necesita instalar un programa en su computadora llamado cliente de VPN. Para el sistema en cuestión estaremos utilizando el cliente de Cisco versión 4.0.1

El proceso de instalación es similar al de cualquier otro programa, en donde se da la bienvenida, se pide el fólder donde se instalará el programa, se instala y se finaliza el proceso. El aspecto importante es la configuración del cliente, y para ello

mostraremos las pantallas correspondientes, indicando los parámetros importantes para establecer la conexión.

En la primera pantalla de las opciones de configuración, como se muestra en la *Figura 5.14,* se deben proporcionar los datos que ahí se solicitan, para nuestro caso se proporcionaron: Banco, Conexión al Banco y dirección IP. En este servidor se debe dar de alta un grupo de acceso con su clave de acceso asociada. Estos datos deben ponerse en los campos “Name”, “Password” y “Confirm Password”.

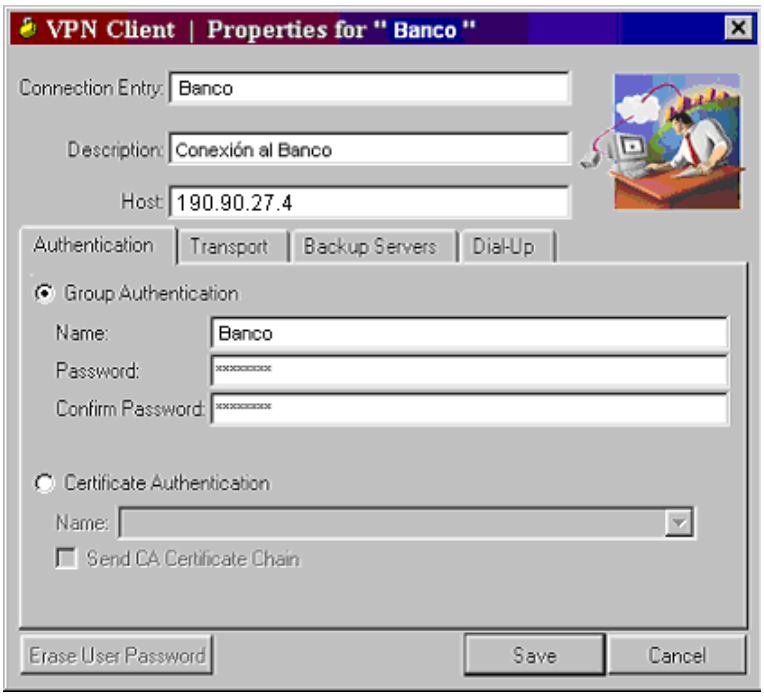

Figura 5.14. Configuración del cliente de VPN (Autentificación).

En la *Figura 5.15,* vemos las opciones de transporte. En esta ventana se especifica la opción de permitir la creación de un túnel transparente y la manera de funcionar del protocolo IPSEC, si va a funcionar con UDP o sobre TCP. En caso de funcionar sobre TCP, se debe especificar el puerto, en este caso escogimos el 10000. También se pregunta si se va a permitir el acceso de la red LAN y un tiempo permitido de respuesta (timeout).

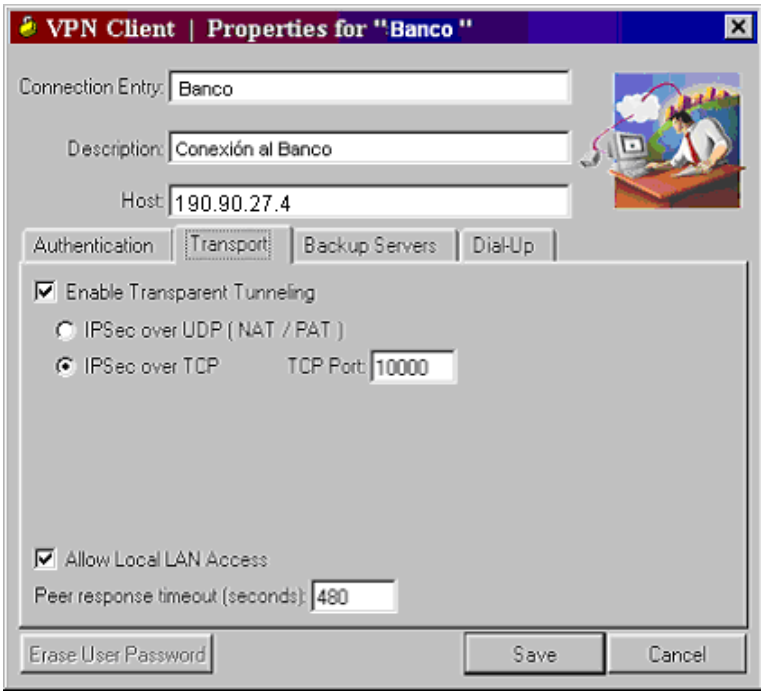

Figura 5.15. Configuración del cliente de VPN (Transporte).

En la *Figura 5.16,* se presenta la pantalla donde se especifican los servidores de respaldo, en nuestro caso no tenemos.

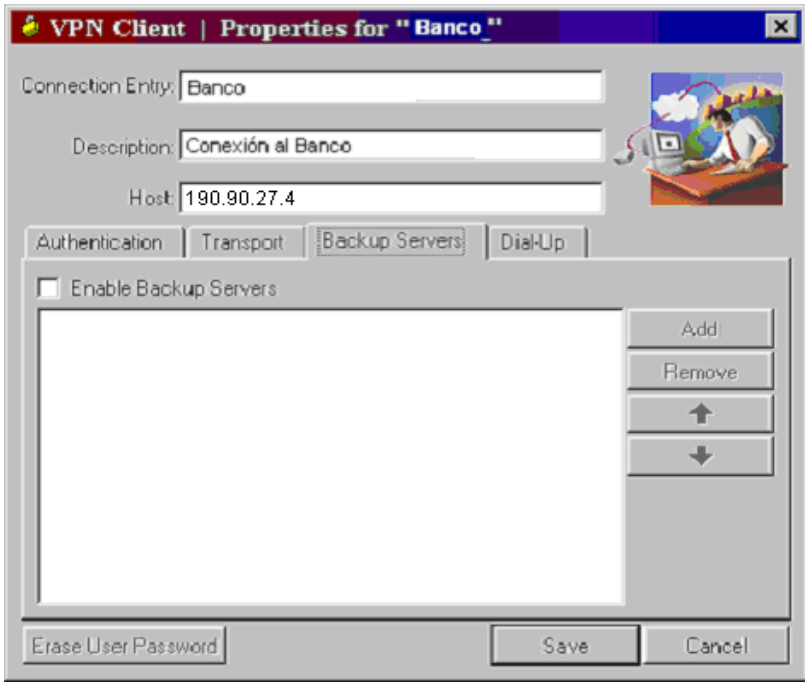

Figura 5.16. Configuración del cliente de VPN (Servidores de Respaldo).

En la *Figura 5.17,* se especifica la opción de marcar un teléfono vía Dial-up, para conexión a Internet antes de tratar de establecer la conexión al servidor de VPNs y si se desea ejecutar alguna aplicación para este propósito.

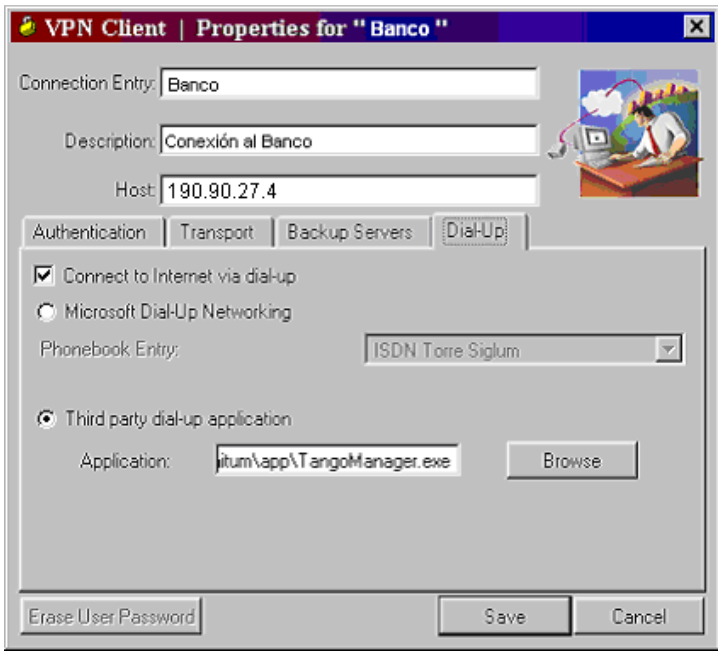

Figura 5.17. Configuración del cliente de VPN (Conexión a Internet).

Una vez configurada la conexión a Internet, podemos verla en la ventana del programa de configuración que se muestra en la *Figura 5.18.* En ella observamos que la conexión a “Banco” ya fue realizada, como se muestra en la barra de estado. La figura del candado en posición de cerrado y la conexión en negritas significa que ya está conectado.

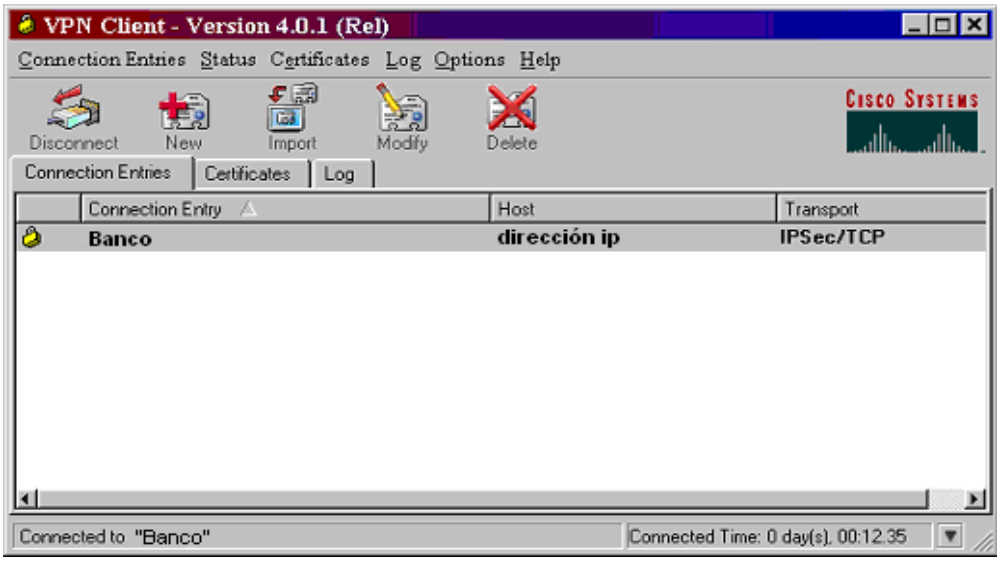

Figura 5.18. Cliente de VPN conectado.

Mediante la selección de la pestaña de *Log* podemos ver paso a paso el estado de la conexión, desde que se abrió, como lo muestra la *Figura 5.19.*

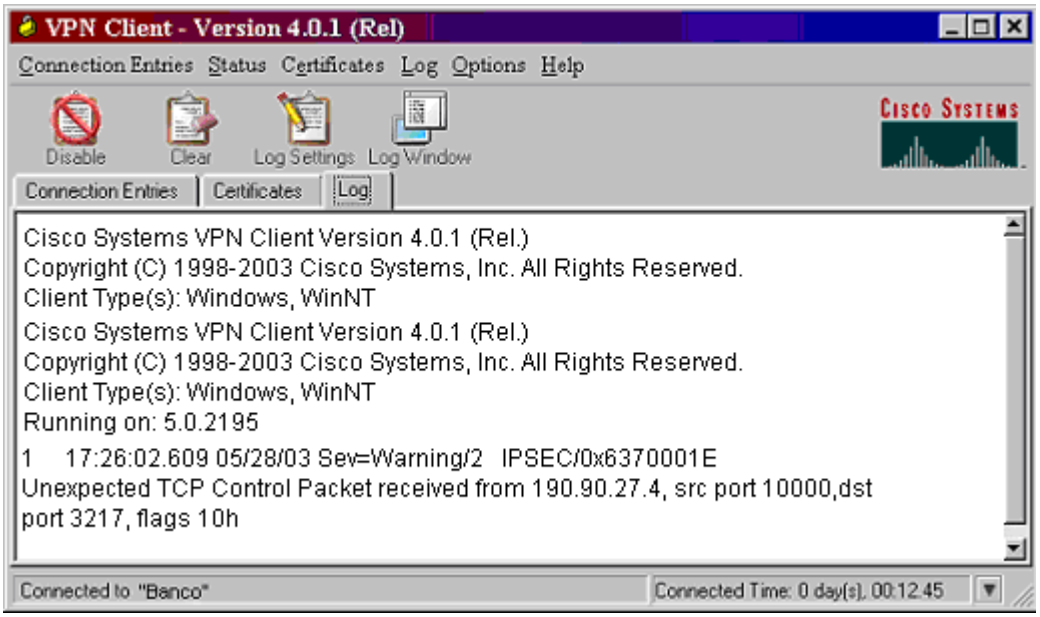

Figura 5.19. Estatus de la conexión del cliente de VPN.

Una vez conectado el cliente de VPN, se puede trabajar como si se estuviera dentro de la red LAN.

5.4. Pruebas

Una vez que se han configurado los routers, se realizaron pruebas con el medio de transmisión. En este punto no sólo se probo la calidad del medio, si no también su disponibilidad y el uso del ancho de banda, específico para cada Intermediario Financiero y sucursal del banco. De acuerdo a lo anterior, para cada nuevo usuario se tiene que crear un circuito virtual permanente en ambos IGX de la red.

5.4.1. Procedimiento para verificación de PVCs

Una vez que se ha implementado el sistema, se procede a su verificación, siendo una primera etapa la verificación del PVC, los cuales como se mencionó en el capítulo anterior, se crean en ambos switches de Frame Relay IGX para tener redundancia.

Dentro de la configuración de las líneas y puertos de los equipos, hay parámetros que son configurados con respecto al E1, proporcionado por el proveedor de servicios de RDSI. Para la creación de los puertos y la configuración de éstos, sólo se dará un ejemplo, ya que la configuración de los demás se realiza de forma análoga.

En la configuración se toman como referencia los datos proporcionados por el proveedor de servicios para el E1, como son: *Line Coding (Código de Línea): HDB3 (Hight Density Bipolar of Orden 3 / Alta Densidad Bipolar de Orden 3)*, el cual es utilizado para troncales E1 y E2; este código de línea se refiere a la ocurrencia de un pulso con la misma polaridad que el pulso anterior, sin que el código de señalización esté en cero; la ocurrencia de esta señal indica que un error ha ocurrido: *Line Signaling (Señalización de Línea): CCS (Comond Channel Signaling / Señalización de Canal Común*); e Impedancia: 75 + GND.

De acuerdo a la información anterior, para configurar los puertos de señalización de Frame Relay, se utiliza la dirección del *DLCI (Data Link Control Identifier / Identificador de Control de Enlace*). El DLCI es una conexión lógica que se utiliza en circuitos virtuales de Frame Relay para conectar a dos routers (dispositivos DTE); Frame Relay utiliza el DLCI para distinguir entre diferentes circuitos virtuales de la red de trabajo.

Para la creación de puertos de Frame Relay sobre las líneas del proveedor de servicios, se utiliza el comando *addport número de puerto* y DLCI; por ejemplo, para el enlace hacia el Site Principal del Intermediario1, le corresponde el número 1, y la configuración es como sigue:

addport 10.1 1.1 64

Una vez configurado el puerto, se dará de alta el enlace de Frame Relay, utilizando el comando: *upport Número de puerto*, para nuestro ejemplo se utilizó:

upport 10.1

Se prosigue con la configuración del puerto, donde se especifica el valor máximo de la cola de transmisión en Bytes (Port Queue Depth), el valor de umbral del sistema para generar la bandera de congestión (ECN Queue Theshold), se habilita el protocolo de señalización con una "*s"* (el protocolo de señalización que utiliza cisco para Frame Relay es Cisco *LMI (Logical Management Interface / Interfaz de Administración Logica)),* se habilita la opción de recibir datos en forma asíncrona, se proporciona el periodo de verificación del puerto (Sep-live), se especifica el número de veces que recibe una verificación de estado errónea; después de este valor se marca como puerto fallido (N392 error Theshold), se determina el número de veces que el sistema espera para una respuesta de estado (N393 Monitored Events count9). Se especifica también la prioridad del dispositivo conectado al puerto (Comunicate priority), se establece el número de veces que no se recibe información antes de habilitar la alarma (Upper RNR Threshold), se declaran cuantos paquetes deben arribar desde el puerto local al puerto remoto, después de haber generado una alarma de fuera de servicio "Bit=0" (OAM Pkt Threshold), y se propone el número mínimo de bandera de inicio de la trama de Frame Relay (Min/Flags Frame).

Ya que la configuración de los puertos en el IGX es la misma para todos los puertos que conforman a la red, sólo se mostrará la configuración realizada en el IGX descrita para un puerto remoto definido como 10.1, que corresponde al Intermediario 1, y se presenta a continuación, de acuerdo con *la Tabla 5.1.*

addport 10.1 1.1 64
upport 10.1
cnfport 10.1

Port Queue Depth	65435
ECN Queue Threshold	65435
DE Threshold	100%
Signalling Protocol	s
Asyncronous Status	yes
T392 Polling Verif Timer	15
N392 error Threshold	4
N392 Monitored Events count	5
Comunicate Priority	no
Upper RNR Theshold	75
Lower RNR Threshold	35
OAM Pkt Threshold	4
Min/ Flags Frame	1
EFCI Mapping Enable	no
CLLM Enable/TX Timer	no
IDE to DE mapping	yes

Tabla 5.1. Configuración del puerto local en el IGX.

Para la configuración del PVC local en el IGX Principal, utilizaremos la línea 9, y en el caso del ejemplo, además de la configuración anterior, se agregará la configuración del tipo de puerto (port type), el ancho de banda del puerto en kbps (speed), el reloj normal proporcionado por el equipo hacia el router, y la dirección IP del puerto para su identificación global dentro de la red (Port ID). Con base en lo anterior, la configuración para el Intermediario 1 quedará como se muestra en la *Tabla 5.2*:

addport 9 1.1 64
upport 9.1
cnfport 9.1

Port type	DCE
Speed	8192
Clocking	Normal
port ID	1000
Port Queue Depth	65435

Tabla 5.2. Configuración del puerto remoto en el IGX (Continúa).

ECN Queue Threshold	65435
De Threshold	100%
Signaling Protocol	s
Asyncronous Status	yes
T392 Polling Verif Timer	15
N392 error threshold	4
N392 Monitored Events count	5
Comunicate Priority	no
Upper RNR Theshold	75
Lower RNR Threshold	35
OAM Pkt Threshold	4
Min/ Flags Frame	1
EFCI Mapping Enable	no
CLLM Enable/TX Timer	no
IDE to DE mapping	Yes

Tabla 5.2. Configuración del puerto remoto en el IGX.

La verificación del estatus del PVC se puede realizar desde la estación de monitoreo definida como Strataview+, utilizando los comandos que a continuación se mencionan:

dspport Num. Puerto.

Con esta instrucción se verifica el estatus del puerto, como se muestra en la pantalla de la *Figura 5.20.*

Como se puede observar en la parte superior de la pantalla, *Figura 5.20,* se encuentra el estatus del puerto en cuestión. Para el ejemplo mostrado corresponde al Intermediario Financiero 1 y se indica que está en **ACTIVE**, con lo cual se garantiza que a nivel de Frame Relay o de capa 1, la red se encuentra operando correctamente. En esta figura también se observa el canal que le corresponde a cada enlace que estamos considerando a través del desplegado *Channel Range (Rango de Canal),* dicho canal corresponde a su conexión física dentro de los 30 canales que forman al E1. Además, el rango de canal debe ser el mismo que la dirección IP asignada al enlace correspondiente. En nuestro ejemplo, (*Figura 5.20) se* observa que el Channel Range es 10, por lo tanto, el puerto seleccionado debe estar conectado en el slot 10 del IGX y debe pertenecer al E1-1, con una dirección IP asignada 190.90.42.10.

En la misma figura, se despliega la velocidad del enlace definida como *Channel Speed (Velocidad del Canal)*, que para nuestro ejemplo es de 64 kbps.

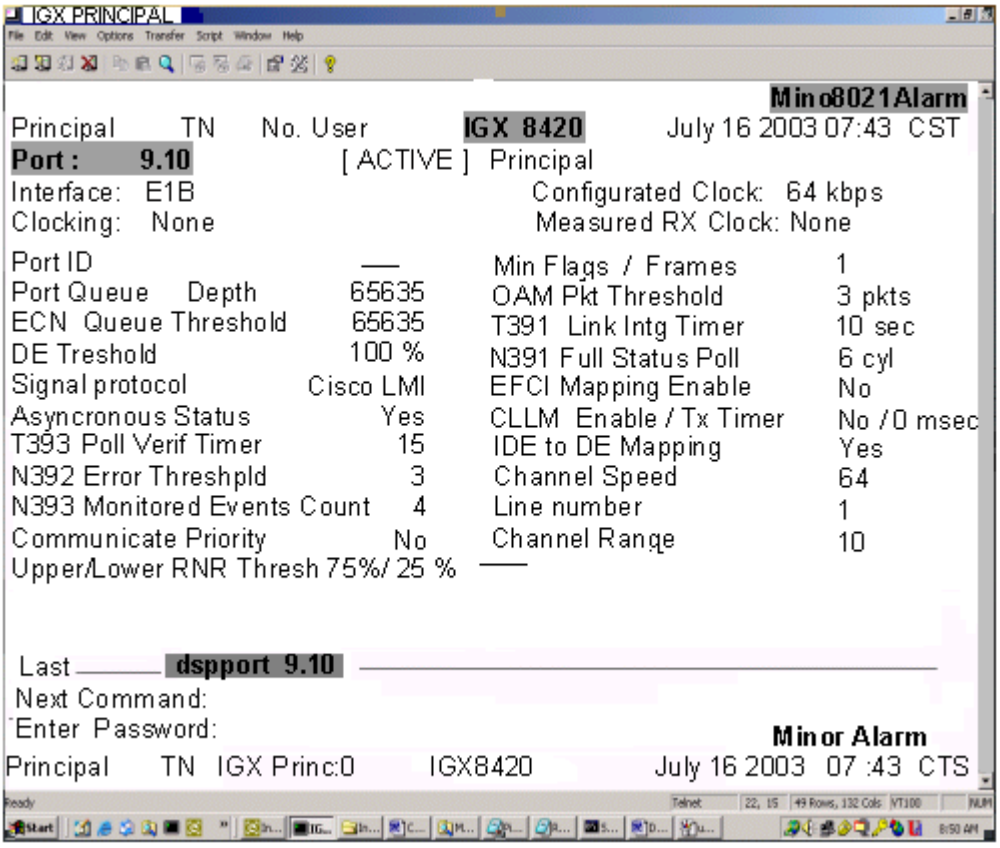

Figura 5.20. Verificación del puerto en el IGX Principal.

Sin embargo, si el PVC se encontrara activo pero se tuvieran intermitencias en el canal, será necesario verificar las estadísticas del puerto utilizando el siguiente comando:

dspportstats Num. Puerto 1.

Esta instrucción permite verificar las estadísticas del puerto correspondiente al enlace WAN del router seleccionado cada segundo. Las estadísticas son mostradas en la *Figura 5.21*. En esta pantalla será necesario poner atención en los *Timeouts*, ya que si éstos se incrementan, será un indicador de que existen problemas con dicho puerto y con la interfaz que conecta al enlace WAN del router que estamos analizando; en esta situación se tendrá que realizar una revisión más exhaustiva con dicho puerto (la revisión consistirá en cambiar el cable V.35 DTE en el router remoto a otro puerto, configurarlo y observar en el IGX si el enlace levanta, es decir, si el puerto esta en ACTIVE y si existe transmisión en el medio, esto es posible observando en la *Figura 5.21,* si la sección correspondiente a frames los valores aumentan), en caso de que el enlace permanezca en FAIL, se tendrá que cambiar físicamente el módulo del puerto serial del router remoto.

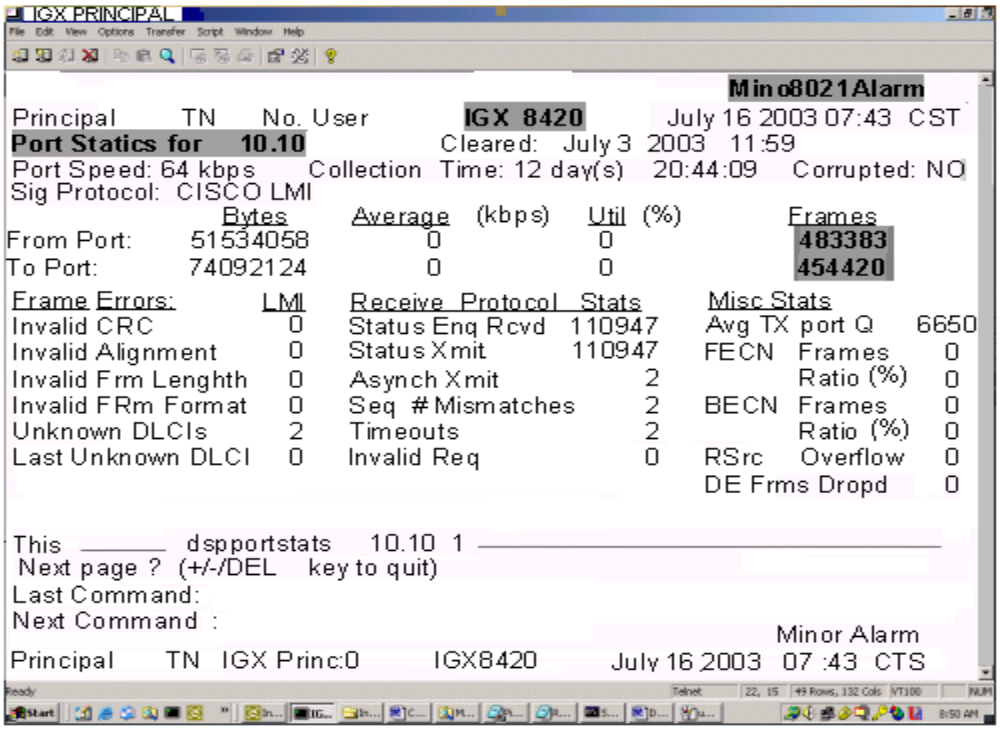

Figura 5.21. Verificación del estatus del puerto cada segundo.

Por otro lado, las líneas de Invalid CRC e Invalid Alignment, desplegadas en la *Figura 5.21,* deberán estar en 0 para indicar que no se tienen errores en el medio. Si la situación fuese la contraria, es decir, que se tengan cantidades mayores a 5, el enlace del router será reportado al proveedor de servicios como errores en el medio de transmisión.

5.4.2. Pruebas de calidad del medio de transmisión

En el caso de que existan errores en el medio de transmisión, las líneas Invalid CRC e Invalid Alignment tendrán un valor diferente de cero, con esta situación se realizarán las pruebas correspondientes con el proveedor de servicios, para verificar el estatus del enlace en cada punto de la trayectoria del mismo. En este caso se debe configurar en el switch de Frame Relay IGX, la opción correspondiente a CLLM Enable /TX Timer con la palabra ***YES***, ver *Figura 5.22,* la activación de este parámetro permitirá poder percibir en el IGX los *Loops (Lazo cerrado),* que son el medio con el que el proveedor de servicio realizará la prueba de calidad en el medio de transmisión. Estos loops son un puente lógico realizado mediante software en los equipos que conforman la red del proveedor de servicios, y es una herramienta utilizada por los técnicos encargados de configurar los enlaces en cada una de las centrales que forman los enlaces RDSI de los prestadores de servicios, para poder definir en donde se encuentra una falla en su enlace.

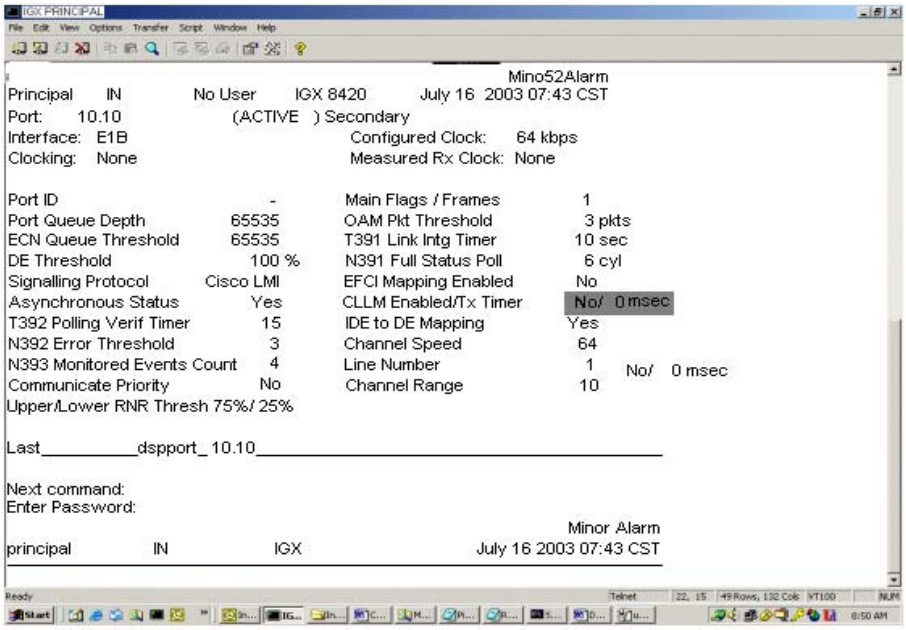

Figura 5.22. Configuración del puerto para recibir Loops.

Para observar una respuesta correcta de esta prueba se debe tener la misma cantidad en las tramas que se envían y en las que se reciben. Esta situación se debe revisar en cada una de las centrales que conforman la trayectoria del enlace desde su origen ya sea en el Site Principal o en el Site Secundario, hasta su destino en las oficinas del Intermediario Financiero. La validación de un loop en la trayectoria se presenta en la sección sombreada de la *Figura 5.23.*

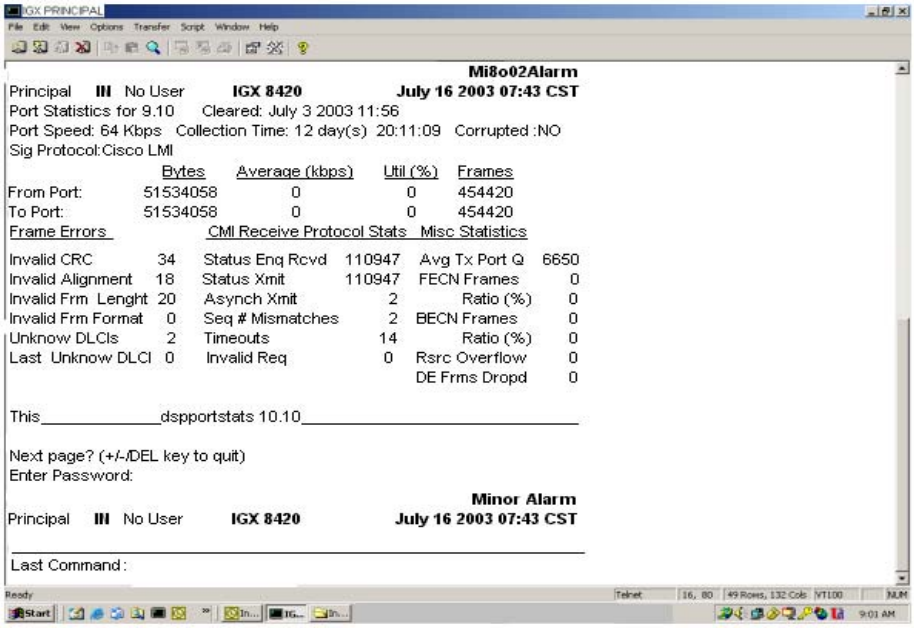

Figura 5.23. Verificación del estatus del puerto utilizando Loops.

Estos Loops son un puente lógico realizado mediante software en los equipos que conforman la red del proveedor de servicios, para poder definir en donde se encuentra una falla en su enlace. Para observar una respuesta correcta de esta prueba se debe tener la misma cantidad en las tramas que se envían y en las que se reciben.

5.4.3. Prueba para verificar Encripción de los datos

Para probar la encripción en los datos transmitidos y recibidos, será necesario ejecutar los siguientes comandos en los Routers de encripción:

Encrip_Princ.#show crypto connections ↵

En este punto se tiene que verificar que la conexión en las interfaces donde se aplicó la encripción, sección Conn_id mostrada en la *Figura 5.24,* no sea negativa. Como puede observarse, se utiliza el algoritmo de encripción DES_40_CFB64

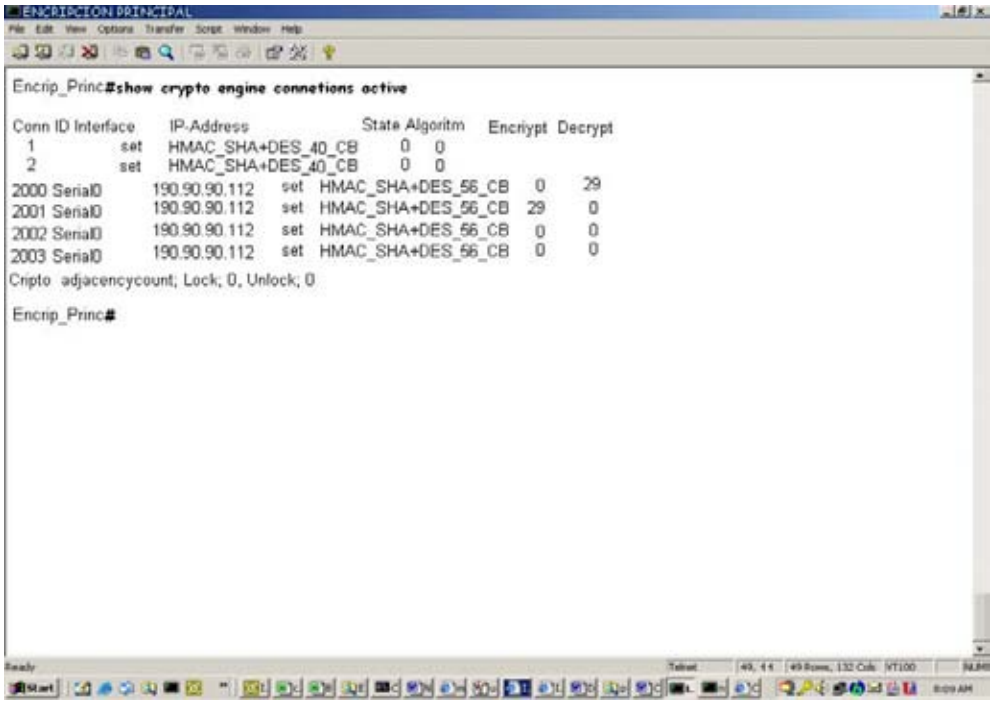

Figura 5.24. Encripción de datos utilizando show crypto engine connections active.

También se debe verificar, en el mismo router de encripción, que los paquetes encriptados y desencriptados aumenten, conforme se trasmite información. En esta sección los paquetes que son enviados a través de los túneles se incrementarán; esta situación se puede corroborar utilizando el siguiente comando:

Encrip_Princ.#show crypto engine connections active ↵

El aumento en los paquetes se puede observar en la *Figura 5.25,* en las columnas correspondientes Encrypt, Decrypt.

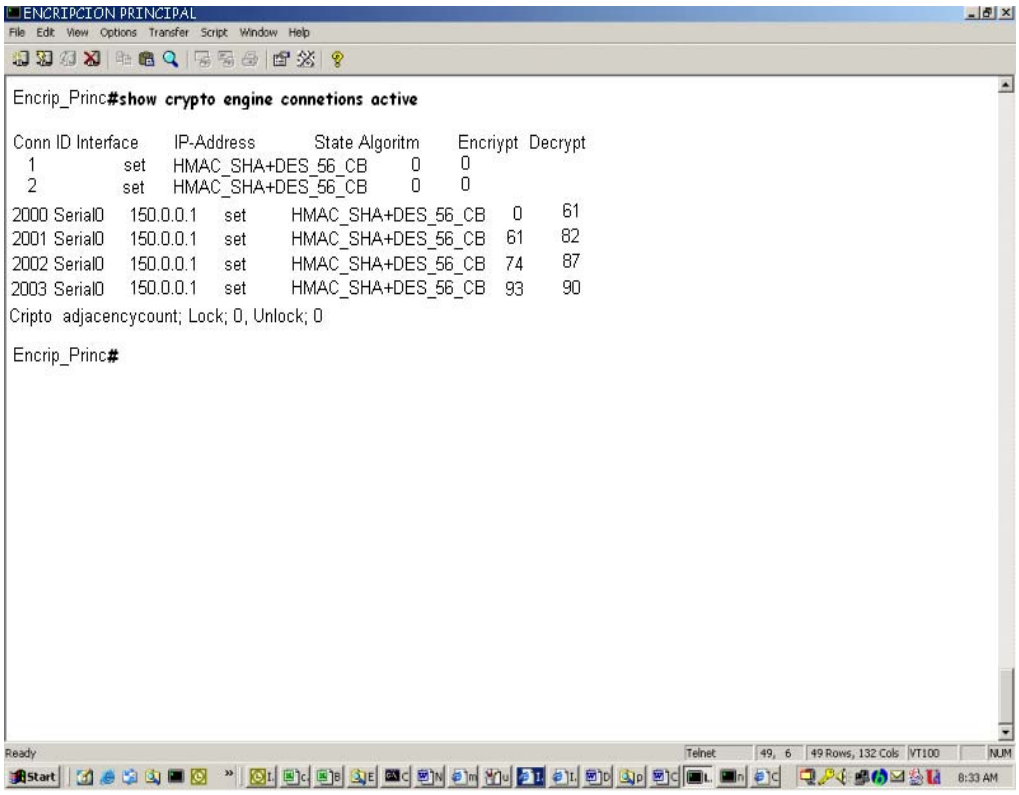

Figura 5.25. Aumento de los paquetes de encripción de datos.

5.4.4. Procesamiento y utilización del ancho de banda en los routers remotos

En la siguiente gráfica se presenta como es utilizado el ancho de banda en los enlaces hacia el Site Principal y hacia el Site Secundario, tomando como base los datos obtenidos para los equipos de sucursales que se muestra en la *Tabla. 5.3*.

Serial Interface Performance Report				
Date:	7/14/2003 10:14			
Model Name:	**SUCURSAL_1**			
IP Address:	0.0.0.0			
Location:	RedFinanciera/Sucursal1			
Interface Number:	3			
Type:	23			
Bandwidth:	384000			
Physical Address:				
Network Address:	170.70.224.142			

Tabla 5.3. Datos de utilización de carga en la Sucursal 1 del Banco (Continúa).

Poll Time	Load	Packet Rate	Error Rate	Discard
8/19/2003 7:04	3	9	0	0
8/19/2003 7:20	6	27	0	0
8/19/2003 7:30	5	34	0	0
8/19/2003 7:40	4	35	0	0
8/19/2003 7:50	6	39	0	0
8/19/2003 8:01	11	74	0	0
8/19/2003 8:11	12	53	0	0
8/19/2003 8:21	6	25	0	0
8/19/2003 8:31	5	17	0	0
8/19/2003 8:47	7	26	0	0
8/19/2003 8:58	5	17	0	0
8/19/2003 9:15	4	79	0	0
8/19/2003 9:30	10	109	0	0
8/19/2003 9:45	9	82	0	0
8/19/2003 10:06	13	73	0	0
8/19/2003 10:21	8	99	0	0
8/19/2003 10:35	10	134	0	0
8/19/2003 10:50	11	140	0	0
8/19/2003 11:03	7	121	0	0
8/19/2003 11:18	8	96	0	0
8/19/2003 11:33	10	102	0	0
8/19/2003 11:47	13	156	0	0
8/19/2003 12:01	12	233	0	0
8/19/2003 12:13	12	139	0	0
8/19/2003 12:29	16	180	0	0
8/19/2003 12:41	14	184	0	0
8/19/2003 12:55	20	76	0	0
8/19/2003 13:07	31	196	0	0
8/19/2003 13:21	26	176	0	0
8/19/2003 13:36	14	208	0	0
8/19/2003 13:48	13	187	0	0
8/19/2003 14:01	15	143	0	0
8/19/2003 14:15	13	88	0	0
8/19/2003 14:30	13	84	0	0
8/19/2003 14:44	14	114	0	0
8/19/2003 14:56	11	132	0	0
8/19/2003 15:09	19	125	0	0
8/19/2003 15:21	72	182	0	0
8/19/2003 15:32	96	239	0	0
8/19/2003 15:44	96	218	0	0
8/19/2003 15:55	96	185	0	0
8/19/2003 16:07	73	212	0	0
8/19/2003 16:19	7	76	0	0
8/19/2003 16:31	10	175	0	0
8/19/2003 16:49	5	84	0	0
8/19/2003 17:01	7	143	0	0
8/19/2003 17:14	9	134	0	0
8/19/2003 17:26	5	68	0	0

Tabla 5.3. Datos de utilización de carga en la Sucursal 1 del Banco. (Continúa)

8/19/2003 17:51	10	113	0	0
8/19/2003 18:04	10	167	0	0
8/19/2003 18:16	13	72	0	0
8/19/2003 18:28	5	47	0	0
8/19/2003 18:41	7	23	0	0
8/19/2003 18:53	8	39	0	0
8/19/2003 19:06	5	27	0	0
8/19/2003 19:18	3	16	0	0
8/19/2003 19:31	6	24	0	0
8/19/2003 19:43	6	24	0	0
8/19/2003 20:01	5	17	0	0
8/19/2003 20:13	7	42	0	0
8/19/2003 20:25	12	90	0	0
8/19/2003 20:36	9	55	0	0
8/19/2003 20:47	5	38	0	0
AVERAGE	15.7812	100.391	0	0

Tabla 5.3. Datos de utilización de carga en la Sucursal 1 del Banco.

La Gráfica de la *Figura 5.26,* nos presenta la utilización del ancho de banda de la interfaz serial 1/1 para la Sucursal 1. Como podemos observar, el porcentaje de carga que se presenta en el periodo de las 07:00 a las 12:29 hrs. Del 19 de Agosto del 2003, se comportó más o menos estable, con una utilización alrededor del 20% de la capacidad de utilización del enlace; de las 15:09 a las 16:19 presentó el porcentaje de utilización más alto, del 96% de la capacidad total del enlace. Esto significa que a esta hora la utilización del enlace fue mayor, debido a que la mayoría de los usuarios accedieron a los servicios del banco o que se transfirió una gran cantidad de datos en ese tiempo.

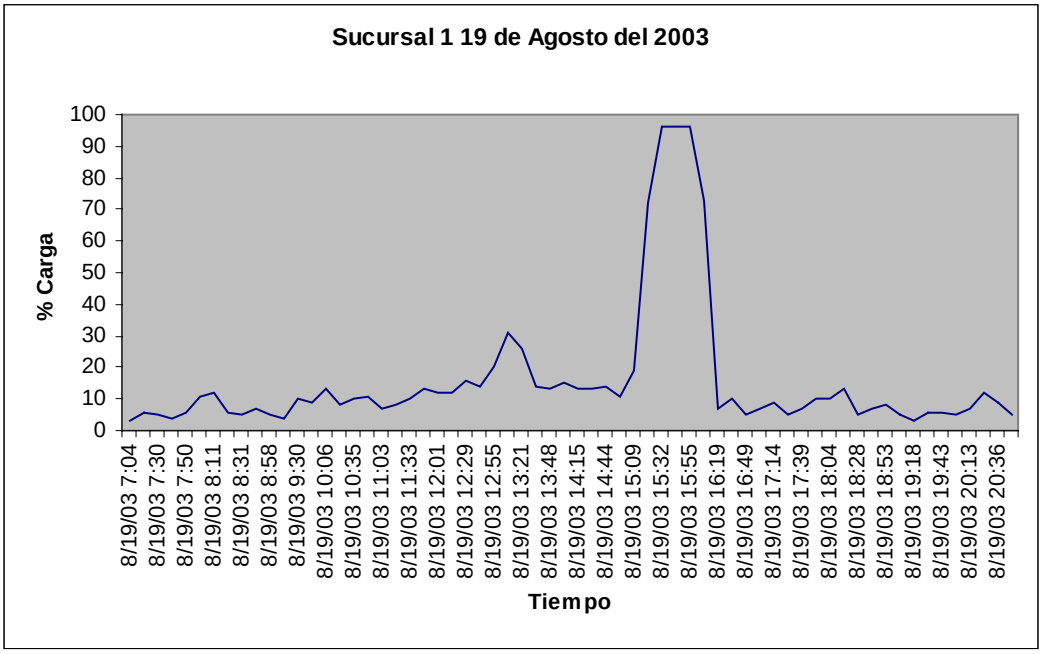

Figura 5.26. Gráfica de utilización de carga en la sucursal 1.

La Gráfica de la *Figura 5.27.* nos presenta la utilización del ancho de banda de la interfaz serial 1/1 para un Intermediario Financiero1. Como podemos observar, el porcentaje de carga que se presenta en el periodo de las 12:20 hasta las 13:53 hrs. Del 19 de Agosto del 2003, presentó el porcentaje de utilización más alto, del 99% de la capacidad total del enlace. Esto significa que a esta hora, la utilización del enlace fue mayor, debido a que la mayoría de los usuarios accedieron a los servicios del banco o que se transfirió una gran cantidad de datos en ese tiempo.

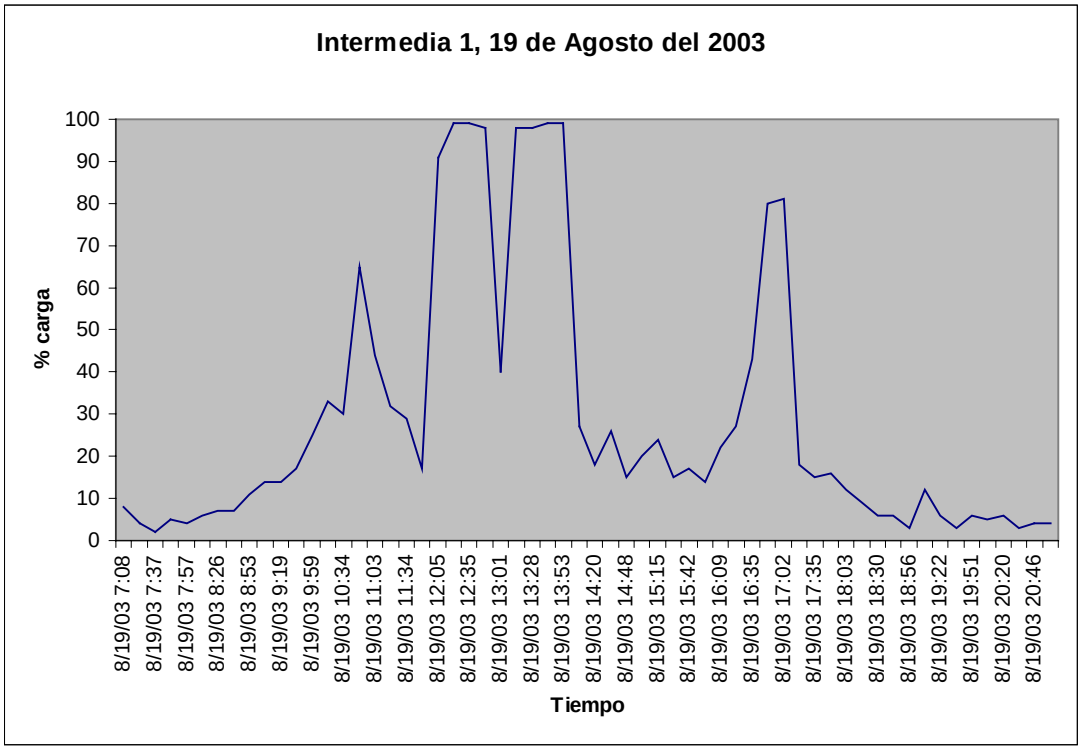

Figura 5.27. Gráfica de utilización de carga del Intermediario Financiero 1.

Otro de los puntos importantes en cuanto al monitoreo y el acceso a los servicios queda definido a través de los cambios realizados en la configuración. Cisco Secure posee nos provee de una herramienta que nos permite saber quien ingresa al equipo, desde que máquina lo hizo y a que fecha y hora ingreso al mismo y que fue lo que realiza. En este sentido se tiene el control de los accesos permitidos en una bitácora que se actualiza con los eventos que ocurren dentro de los equipos que conforman la red. Una muestra de este tipo de información se presenta en la *Tabla 5.6.*

Dispositivo	Terminal	IP asociada	Usuario	Fecha	Hora (time)	Acción realizada
190.90.90.154	33	Async33 async start	Fimex1	07/08/2003	11:19:01	cmd=no access-list 199 <cr>
190.90.90.154	33	Async33 async update	Fimex1	07/08/2003	11:19:49	disc-cause-ext=1011
190.90.90.154	33	Async33 async stop	Fimex1	07/08/2003	11:46:20	cmd=logout <cr>
190.90.52.74	128	190.90.32.124	Nmazas	07/08/2003	11:46:41	cmd=undebug all <cr>
190.90.52.74	128	190.90.32.124	Nmazas	07/08/2003	11:46:57	cmd=undebug all <cr>
190.90.52.74	128	190.90.32.124	Nmazas	07/08/2003	11:47:32	cmd=dialer-list 1 protocol ip list 199
190.90.52.74	125	190.90.0.112	Nmazas	07/08/2003	11:52:30	cmd=no access-list 199 <cr>
190.90.52.74	125	190.90.0.112	Eavila	07/08/2003	11:52:47	cmd=debug <cr>
190.90.52.74	125	190.90.0.112	Eavila	07/08/2003	11:52:53	cmd=dialer-list 1 protocol ip list 199
190.90.52.74	125	190.90.0.112	Eavila	07/08/2003	11:56:28	cmd=undebug all <cr>
190.90.90.154	125	190.90.0.112	Eavila	07/08/2003	11:56:30	disc-cause-ext=1020
190.90.90.15	125	190.90.0.112	Eavila	07/08/2003	11:56:52	cmd=ip route 190.90.4.0 255.255.255.0 190.90.90.15
190.90.90.15	125	190.90.0.112	Eavila	07/08/2003	11:57:06	cmd=access-list 15 permit 190.90.4.0 0.0.0.255
190.90.52.114	125	190.90.0.112	Eavila	07/08/2003	11:57:17	cmd=access-list 15 permit 190.90.4.0 0.0.0.255
190.90.90.154	10	Async10 start	Smorales	07/08/2003	12:01:32	cmd=login
190.90.90.154	10	Async10 stop	Smorales	07/08/2003	12:02:00	disc-cause-ext=1011
190.90.42.152	125	190.90.0.112	Ovaldivie	07/08/2003	12:02:54	cmd=no permit 190.90.8.0 0.0.0.255
190.90.42.152	125	190.90.0.112	Ovaldivie	07/08/2003	12:22:14	cmd=access-list 22 permit 190.90.8.0 0.0.0.255
170.70.23.16	125	190.90.0.112	Jgarcia	07/08/2003	12:22:15	cmd=interface FastEthernet 0 0 <cr>
170.70.23.16	125	190.90.0.112	Jgarcia	07/08/2003	12:47:34	cmd=interface FastEthernet 0 0 <cr>
170.70.23.16	125	190.90.0.112	Jgarcia	07/08/2003	13:02:23	cmd=cdp enable <cr>
170.70.23.16	125	190.90.0.112	Jgarcia	07/08/2003	13:02:38	cmd=cdp enable <cr>
190.90.520.132	125	190.90.0.112	Ovaldivie	07/08/2003	13:02:50	cmd=no permit 190.90.4.0 0.0.0.255
190.90.42.152	125	190.90.0.112	Jgarcia	07/08/2003	13:02:58	cmd=interface FastEthernet 5 1 0 <cr>
190.90.42.152	125	190.90.0.112	Jgarcia	07/08/2003	13:03:05	cmd=cdp enable <cr>
190.90.42.152	125	190.90.0.112	Jgarcia	07/08/2003	13:03:07	cmd=interface Serial 5 0 0 <cr>
190.90.42.152	125	190.90.0.112	Jgarcia	07/08/2003	13:03:12	cmd=cdp enable <cr>
190.90.42.152	125	190.90.0.112	Jgarcia	07/08/2003	13:03:15	cmd=interface FastEthernet 1 1 0 <cr>
190.90.42.152	125	190.90.0.112	Jgarcia	07/08/2003	13:03:21	cmd=cdp enable <cr>
190.90.90.5	125	190.90.0.112	Smorales	07/08/2003	13:03:34	cmd=interface FastEthernet 0 0 <cr>
190.90.90.5	125	190.90.0.112	Smorales	07/08/2003	13:03:37	cmd=cdp enable <cr>
190.90.240.114	125	190.90.0.112	Smorales	07/08/2003	13:03:44	cmd=hostname Intermediario 5 <cr>
190.90.240.114	125	190.90.0.112	Smorales	07/08/2003	13:04:01	cmd=interface Serial 0 0 <cr>
190.90.240.114	125	190.90.0.112	Smorales	07/08/2003	13:04:08	cmd=snmp-server host 190.90.32.6 fimex 01
190.90.240.114	125	190.90.0.112	Smorales	07/08/2003	13:04:12	cmd=ip route 190.90.90.125 255.255.255.255 190.90.124.21

Tabla 5.4. Cambios en la configuración de los equipos de la red Financiera (Continúa).

190.90.52.132	125	190.90.0.112	Nmazas	07/08/2003	15:26:38	cmd=interface FastEthernet 1 1 0 <cr>
190.90.22.18	125	190.90.0.112	Nmazas	07/08/2003	15:26:48	cmd=cdp enable <cr>
190.90.52.132	125	190.9092.18	Nmazas	07/08/2003	15:26:58	cmd=cdp run <cr>
190.90.52.132	125	190.9092.18	Admin2	07/08/2003	15:37:42	cmd=interface FastEthernet 4 1 0 <cr>
190.90.52.132	125	190.9092.18	Admin2	07/08/2003	15:38:03	cmd=cdp enable <cr>
190.90.90.5	125	190.9092.18	Admin2	07/08/2003	15:43:39	cmd=disable <cr>
190.90.90.5	125	190.9092.18	Admin2	07/08/2003	15:43:43	cmd=interface FastEthernet 0 0 <cr>
190.90.90.5	125	190.9092.18	Admin2	07/08/2003	15:43:53	cmd=cdp enable <cr>
190.90.20.25	129	190.90.42.154	Admin1	08/08/2003	15:44:03	cmd=no username admin <cr>
190.90.20.25	129	190.90.42.154	Admin1	08/08/2003	15:44:12	cmd=username root privilege 15 password 7 195HJ12N5C7D23 <cr>
190.90.20.25	129	190.90.42.154	Admin1	08/08/2003	15:44:16	cmd=username admin privilege 15 password 7 25DGHF14255R537L
190.90.240.118	129	190.90.42.154	Nmazas	08/08/2003	15:48:17	cmd=username teledin privilege 7 password 7 078H9KU2S7B56785210
190.90.240.118	129	190.90.42.152	Nmazas	08/08/2003	16:17:51	cmd=access-list 5 permit 197.20.118.0 0.0.0.25
190.90.240.118	129	190.90.42.152	Nmazas	08/08/2003	16:17:57	cmd=shutdown <cr>
190.90.90.154	129	async stop	Nmazas	08/08/2003	16:18:10	disc-cause-ext=1020
190.90.520.132	129	190.90.42.154	Nmazas	08/08/2003	16:18:14	cmd=router ospf 1 <cr>
190.90.520.132	129	190.90.42.154	Eavila	08/08/2003	16:19:49	cmd=no network 190.90.4.0 0.0.0.255 area 0
190.90.42.152	129	190.90.42.154	Eavila	08/08/2003	16:24:07	cmd=router ospf 1 <cr>
190.90.42.152	129	190.90.42.154	Eavila	08/08/2003	16:24:55	cmd=no network 190.90.76.0 0.0.0.255 area
190.90.42.152	129	190.90.42.154	Eavila	08/08/2003	16:24:58	cmd=no network 190.90.87.0 0.0.0.255 area
190.90.240.116	129	190.90.42.154	Jgarcia	08/08/2003	16:24:58	cmd=interfac
190.90.52.28	125	190.90.0.112	Eavila	09/08/2003	15:05:50	cmd=access-list 120 permit ip any any log
190.90.90.154	125	async stop	Eavila	09/08/2003	15:14:44	disc-cause-ext=1020
190.90.52.83	125	190.90.0.112	Eavila	09/08/2003	15:15:01	cmd=dialer-list 1 protocol ip list 199
190.90.52.66	125	190.90.0.112	Eavila	09/08/2003	15:15:14	cmd=ip access-list extended 105 <cr>
190.90.52.66	125	190.90.0.112	Eavila	09/08/2003	15:40:18	cmd=no deny ip any any <cr>
190.90.52.66	125	190.90.0.112	Eavila	09/08/2003	15:40:29	cmd=permit ip host 192.15.126.156 any
190.90.52.66	125	190.90.0.112	Eavila	09/08/2003	15:40:36	cmd=ip access-list extended 105 <cr>
190.90.52.66	125	190.90.0.112	Eavila	09/08/2003	15:41:07	cmd=no deny ip any any log <cr>
190.90.52.39		190.90.0.112	Eavila	09/08/2003	15:41:16	cmd=interface Ethernet 0 0 <cr>
190.90.52.39	125	190.90.0.112	Eavila	09/08/2003	15:42:22	cmd=ip access-group INTERMEDIARIO 5 in
190.90.52.39	125	190.90.0.112	Eavila	09/08/2003	15:42:27	cmd=no shutdown <cr>
190.90.52.28	125	190.90.0.112	Jgarcia	09/08/2003	15:47:35	cmd=interface Ethernet 0 <cr>
190.90.52.28	125	190.90.0.112	Jgarcia	09/08/2003	15:47:45	cmd=ip access-group 105 in <cr>
190.90.240.116	125	190.90.0.112	Ovaldivie	09/08/2003	15:47:47	cmd=interface Ethernet 0 0 <cr>
190.90.240.116	125	190.90.0.112	Ovaldivie	09/08/2003	15:48:05	cmd=no ip access-group 105 in <cr>
190.90.240.116	125	190.90.0.112	Ovaldivie	09/08/2003	15:49:00	cmd=no access-list 105 <cr>
190.90.240.116	125	190.90.0.112	Ovaldivie	09/08/2003	15:49:53	cmd=access-list 105 permit icmp any any
190.90.90.154	Aíncrona 33	Async33 async start	Nmazas	10/082003	11:19:01	cmd=no access-list 199 <cr>

Tabla 5.4. Cambios en la configuración de los equipos de la Red Financiera

Con estas pruebas hemos verificado los siguientes aspectos de la implementación del sistema:

- Su correcta funcionalidad.
- La calidad del medio de transmisión.
- La correcta configuración de los equipos.
- La encripción de la información.
- La validación de los usuarios que se conectan a través de VPN.

Con esto damos por concluido nuestro trabajo de investigación y para el siguiente capítulo se comentarán las conclusiones a las que llegamos.

CAPÍTULO 6

RESULTADOS Y CONCLUSIONES

A lo largo de este trabajo surgieron aspectos que, por cuestiones de tiempo, no se tratan a detalle, sólo se lograron cubrir aquellos que se encontraban mas ligado a esta investigación, como fueron los aspectos administrativos, de disponibilidad, seguridad de la información y el de realizar esta integración con los servicios que proporciona el banco en cuestión.

Al principio del presente trabajo se plantearon varios objetivos que fueron:

1. Controlar la seguridad en el acceso remoto a la Red Financiera del Banco.
2. Establecer las tecnologías, tipos de protocolo y equipos de comunicaciones a utilizar.
3. Implementar la validación del acceso remoto a los servicios del Banco.
4. Instaurar un Site Central en donde se puedan realizar tareas de administración, configuración, control y solución de una gran variedad de problemas en la Red remotamente evitando la necesidad de trasladarse al sitio en cuestión.
5. Definir prioridades para acceso a la información confidencial y a los servicios dentro de la Red Financiera del Banco.
6. Dadas las necesidades, implementar el software necesario y la llave para que el usuario que intenta acceder remotamente a los servicios del Banco pueda lograr su conexión.
7. Especificar el tipo de cableado necesario para conexión en el sitio, el uso de fibra óptica y necesidades de respaldo.
8. Especificar el equipo requerido de seguridad y la necesidad de encripción para evitar conexiones no deseadas para seguridad del Banco.

De los objetivos numerados, el número 7 fue el único que no se pudo cumplir, debido a que finalmente lo que se refiere a la instalación del cableado estructurado no fue tema de desarrollo en el trabajo; sin embargo, no quisimos pasar por alto este objetivo e incluimos un apéndice, en el cual se da un panorama muy general de lo que constituye el cableado estructurado, puntualizando que con ello procuramos no dejar un sólo objetivo sin cumplir.

Debemos señalar que las modificaciones hechas a la red, satisfacen las necesidades de la Institución Bancaria y mejoraron en gran medida su funcionamiento con lo cual, cada una de las soluciones planteadas en el presente trabajo ayudó a cumplir las expectativas planeadas desde un inicio y que detallaremos a continuación, brindando los comentarios y conclusiones respectivas de cómo se llevó a cabo.

Una vez que se identificaron los puntos precisos de la presente investigación, se realizó un comparativo de equipos para poder seleccionar el que más se adaptaba a nuestras necesidades. De los aspectos encontrados, nos dimos cuenta que existen diversos equipos que si bien no cumplían con la mayoría de los requerimientos, sí eran accesibles en cuanto al precio, pero se debían comprar varios de diferentes modelos para satisfacer nuestras necesidades. El único que cumplió de cierta forma con la mayoría de estas necesidades fue el de la compañía Cisco Systems. A pesar de que es un equipo costoso, el Banco cuenta con un contrato de adquisición de productos con

esta empresa, ante esto, se tomó la decisión de adquirir el equipo de Cisco Systems. Cabe mencionar que otra de las cosas que nos llevaron a decidir la adquisición de estos equipos, fue la conveniencia de homogeneizar el equipo con el que se cuenta; también porque su actualización al momento de configurarlo es dinámica, pues no es necesario reinicializar el equipo, su método de encripción único es una buena característica, así como una forma de programación más práctica, tal es el caso de los routers y Firewalls.

El planteamiento de seguridad en los datos de la Red Financiera es uno de los puntos más importantes que se decidió mejorar, al igual que la disponibilidad de los servicios prestados por el Banco. Para tal caso se propuso establecer la encripción de los datos que se transmiten por la red y que son enviados a través de los enlaces que la componen. La encripción de los datos planteó diferentes problemas, uno de ellos fue cómo asegurar la validez de los datos y la autentificación de las personas que acceden a los servidores de la red interna del Banco. Con el propósito de implementar la encripción tanto en los routers de encripción como en los routers remotos, se propusieron dos técnicas de encripción, la primera de ellas basada en listas de acceso y la segunda en túneles GRE. Dentro de la implementación de la encripción con listas de acceso se tuvieron muchos problemas, ya que su aplicación implica que todos los equipos utilizados en la red estén homologados y soporten dicha técnica. Este punto no estaba respaldado en la estructura de la red, ya que la técnica de encripción con listas de acceso se basa en tener un sólo destino y una sola fuente, sin embargo en la estructura de la red, los Intermediaros Financieros pueden acceder a los servidores del Banco por dos destinos diferentes, ya sea por el Site Principal o por el Site Secundario. Dicho comportamiento de la red acarreó varios problemas con respecto a qué lista de acceso se aplicaba primero, presentándose bloqueos en los equipos tanto locales como remotos. Si bien es cierto que se pudo implementar la encripción con listas de acceso, también es cierto que el sistema funcionó sólo por unos días, situación por la cual se decidió complementarla con la técnica de túneles GRE.

En esta técnica de encripción con túneles GRE, se construyeron túneles tanto en los routers de encripción como en los routers remotos. En esta técnica se necesita que por cada túnel configurado en los routers de encripción, tengamos su respectivo túnel configurado en el router del Intermediario Financiero. En los routers remotos se tienen que construir dos túneles, uno hacia el Site Principal y otro hacia el Site Secundario. Este sistema implementado, aunque presenta algunos problemas con la pérdida de los enlaces y la propagación de las tablas de ruteo, el tiempo de recuperación de las mismas es mínimo, por lo que decidimos utilizar este sistema de encripción en la Red Financiera del Banco.

En lo que respecta a la disponibilidad de los servicios prestados por el Banco a las sucursales, se realizó un estudio de mercado para evitar la pérdida de información proporcionada por el Banco cuando los enlaces DS0 hacia el Site Secundario y el respaldo por modem vía Dial-up fallan. En primera instancia se propuso arrendar un nuevo enlace DS0 ó RDI, realizando un comparativo tanto de características como de precio de los mismos, resultando ser el enlace a través de RDSI de 64 kbps el que mejor cumplía con nuestras necesidades. Sin embargo, ya que en la estructura

implementada estaba soportada por enlaces DS0 independientes, la decisión final de cambiar dicha estructura quedó como una posible mejora a futuro. Para cubrir la necesidad de comunicación vía Dial-up cuando el enlace hacia el RAS actual falle, se propuso contar con una línea telefónica pública para enlazar a cada sucursal con un nuevo RAS, que se ubicó en el Site Principal y que soporta tanto a las sucursales como a los Intermediarios Financieros. Cabe aclarar que la configuración de la conexión hacia el nuevo RAS en los routers remotos solo implica agregar una línea en la configuración actual de los mismos, y que se puede utilizar la misma línea telefónica de la infraestructura existente.

La validación y autentificación de los usuarios en el nuevo RAS será autorizada tanto en el RAS como en los servidores que se conectan con los servicios prestados por el Banco.

Otro punto importante se relacionó con proteger el acceso de los usuarios una vez que han ingresado a la red interna. Si bien es cierto que los filtros establecidos en los routers WAN y LAN a través de listas de acceso y rutas estáticas limitan el acceso, un PIX Firewall fue colocado con la finalidad de proteger dicho acceso. El PIX permitió que sólo los usuarios autorizados pudieran acceder a los servicios del Banco y en algunos casos modificar algún servicio, siempre y cuando estuviera autorizado tanto en los routers del Backbone como en los servidores de autentificación Cisco Secure y Cisco Works. El PIX permitió también establecer las prioridades de acceso hacia la red pública de los diferentes usuarios internos, estableciendo prioridades como son acceso a Internet, corrreo, FTP, etc.

La utilización de un enlace nuevo DS0 ó RDSI permitirá, si así se decide, mejorar el ancho de banda de los servicios, ya que en esta estructura se tiene un enlace de 64 kbps a través de un enlace de Frame Relay hacia cada uno de los sites que componen a la red. En el estudio de mercado que realizamos para la adquisición de un nuevo enlace, se vio que el enlace RDSI es más conveniente para el Banco por tener un menor costo de instalación y proporcionar un mayor ancho de banda. Esta opción se menciona como un servicio a futuro. En el caso de las sucursales, se sugiere implementar el protocolo PPP multilink con la finalidad de ampliar el ancho de banda disponible en cada enlace y evitar que se sature, logrando que el ancho de banda de nuestro enlace se duplique. Otro de los puntos que se puede mejorar es utilizar cuatro switches en el Backbone, ya que en la estructura actual solamente se tienen dos y en caso de que estos fallen, la conmunicación se perderá. La propuesta es colocar dos switches más en ambos Sites de la red. Uno de ellos enlazará a los routers WAN y LAN Principal y el otro enlazará a los routers WAN y LAN Secundario respectivamente. En la estructura propuesta se establece la conmutación automática de los switches en caso de falla, de forma transparente para el usuario.

En cuanto a la integración de servicios, existía la necesidad de implementar la conexión por Dial-up, además de contar con un medio de comunicación para los usuarios que se encontraban fuera de las oficinas y en distintos puntos geográficos. Por ello se implementó el acceso a través de enlaces Dial-up, ya sea por modem ó utilizando la línea telefónica pública o por medio de enlaces arrendados VPN. Este

proceso de acceso a la red es validado por medio del servidor de acceso remoto RAS y autentificado tanto en PIX como en los servidores de Cisco Secure y de Cisco Works. El acceso de los usuarios utilizando VPN se establece proporcionando el número de identificación del empleado del banco y una clave de seguridad, que se le proporciona de tal forma que sólo los usuarios autorizados se puedan conectar a la red interna del Banco.

Finalmente lo que nos dejó este proyecto de investigación fue el retomar, reforzar y ampliar nuestros conocimientos sobre redes, así como conocer mas de los aspectos en cuanto a la privacidad de la información cuando se trata de redes financieras, y tomar conciencia de los problemas que ocasionaría si se llegara a tener acceso a la información de una red privada por personas ajenas a la institución. Además, el hecho de que en esta área se necesita de constante actualización, pues siempre surgen nuevas tecnologías de diversas compañías dedicadas a las telecomunicaciones, que compiten por brindar mayor seguridad contra ataques externos, cada vez más comunes. Lo que requiere de una gran infraestructura y conocimientos que debemos tomar en cuenta para formar o llegar a formar parte de una institución como ésta.

APÉNDICE

Tipos de Cables

Es importante conocer las características de los cables, para elegir el que mejor se adapte a nuestras necesidades en cada situación. Aquí se presentan estas características para los cables más usados actualmente para la comunicación entre redes.

Conforme la tecnología avanza, la velocidad de transmisión de información es cada vez mayor, y para ello se hace necesario mejorar la calidad de los medios por los que se transmite.

Actualmente existe una gran cantidad de tipos de cables, para diferentes topologías de red y con diferentes especificaciones. A continuación se mencionarán brevemente, los principales tipos de cables con sus características.

7.1 Cable Coaxial

Es un cable compuesto, desde adentro hacia afuera, por un alambre que se mantiene fijo en un medio aislante. Este medio está protegido por una cubierta metálica. Ésta a su vez está rodeada de una malla entrelazada de hilos de cobre o aluminio. Esta malla tiene como finalidad evitar que las señales de otros cables, o la radiación electromagnética externa, afecte la información que conduce el hilo central. Finalmente se tiene una cubierta plástica, generalmente de color negro como se muestra en la *Figura 7.1.*

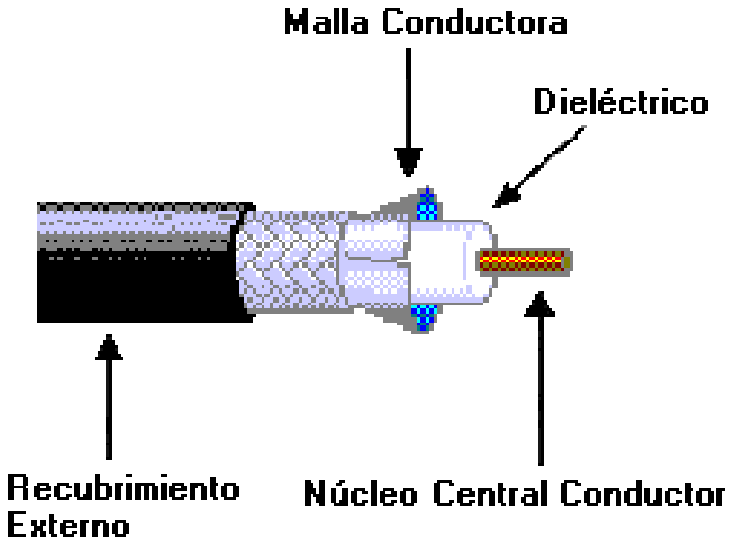

Figura 7.1. Cable Coaxial.

Este tipo de cable se utiliza en la topología de bus lineal. A continuación se describen los tipos de cables coaxial más empleados en redes.

10base5

Conocido también como cable *coaxial grueso (Thick coaxial)* y sirve como Backbone para una red tipo LAN. Para conectarse a otros dispositivos utiliza transceptores (o transceivers) con conectores tipo BNC y *AUI (Attachment Unit Interface / Interfaz de Unidad Anexa)*. Sus principales características son:

- Velocidad de transmisión: 10 Mbps.
- Longitud máxima: 500 metros por segmento.
- Impedancia: 50 ohms.
- Diámetro del conductor: 2.17 mm.
- Nodos por segmento: 100.

10base2

Conocido también como cable coaxial delgado (Thin coaxial), empleado en redes tipo LAN. Utiliza conectores tipo BNC para conectar la tarjeta de red con el backbone.

- Tasa de transmisión: 10 Mbps
- Longitud máxima: 180 metros por segmento
- Impedancia: 50 ohm
- Diámetro del conductor: 0.9 mm
- Nodos por segmento: 30

7.2 Par Trenzado

El cable par trenzado está compuesto de conductores de cobre aislados por plástico y trenzados en pares. Esos pares también se trenzan en grupos llamados unidades, y estas unidades se cubre por lo general por plástico. El trenzado es en promedio de tres trenzas por pulgada. Para mejores resultados, el trenzado debe ser variado entre los diferentes pares. El trenzado de los pares de cable y de las unidades disminuye el ruido de interferencia, mejor conocido como diafonía. Los cables de par trenzado tienen la ventaja de no ser caros, ser flexibles y fáciles de conectar, entre otras. Como medio de comunicación tiene la desventaja de tener que usarse a distancias limitadas, ya que la señal se va atenuando y puede llegar a ser imperceptible; es por eso que a determinadas distancias se deben emplear repetidores que regeneren la señal.

Para la utilización de este tipo de cableado es necesario instalar un concentrador para que haga la función de repartidor de señales, por eso se denomina topología en estrella.

Existen dos tipos de cable par trenzado, el *UTP (Unshielded Twisted Pair Cabling / Cable de Par Trenzado Sin Blindaje)* y el cable *STP (Shielded Twisted Pair Cabling / Cable Par Trenzado Blindado)*.

Cable UTP

Como el nombre lo indica es un cable que no tiene revestimiento o blindaje entre la cubierta exterior y los cables. El UTP se utiliza comúnmente para aplicaciones de Redes Ethernet. El término UTP generalmente se refiere a los cables con categoría 3, 4 y 5, especificados por el estándar TIA/EIA 568-A.

Las categorías 5e, 6 y 7 también han sido propuestos para soportar velocidades más altas. El cable UTP comúnmente incluye 4 pares de conductores (ver *Figura 7.2.*). Los cables 10baseTx, 100baseTX, y 100baseT2 sólo utilizan 2 pares de conductores, mientras que 100baseT4 y 100baseT requieren de todos los 4 pares.

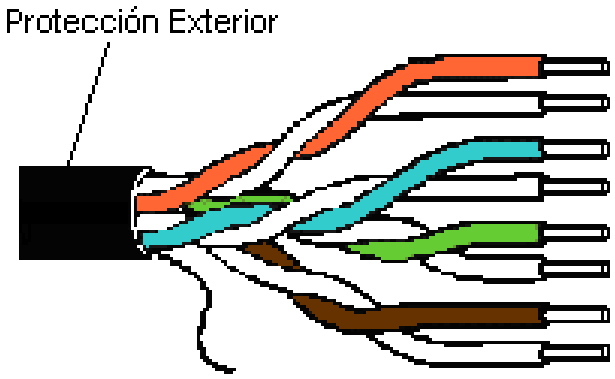

Figura 7.2. Cable de Par Trenzado de Cuatro Pares.

En la Tabla 7.1., se lista el uso de las categorías de cable UTP.

Tipo	Uso
Categoría 1	Voz solamente (cable telefónico) < 1 Mbps
Categoría 2	Datos hasta 4 Mbps (LocalTalk [Apple])
Categoría 3	Datos de 10 hasta 16 Mbps (Ethernet)
Categoría 4	Datos de 16 hasta 20 Mbps (Token Ring)
Categoría 5	Datos hasta 100 Mbps (Fast Ethernet) con 2 pares
Categoría 5e mejorada	Datos hasta 600 Mbps (Fast Ethernet) con 4 pares
Categoría 6	Datos hasta 1 Gbps (Fast Ethernet) y Bidirecccional
Categoría 7	Datos > 1 Gbps (Fast Ethernet) y Bidirecccional

Tabla 7.1. Categorías de Cable UTP.

Cable STP

El cable STP tiene un blindaje especial que forra a los 4 pares (ver *Figura 7.3*) y comúnmente se refiere al cable par trenzado de 150 ohms definido por IBM, utilizado en redes Token Ring. El blindaje está diseñado para minimizar la *radiación electromagnética (EMI, electromagnetic interference)* y la diafonía. Los cables STP de 150 ohms no se usan para Ethernet, sin embargo, puede ser

adaptado a 10Base-T, 100Base-TX, y 100Base-T2 Ethernet, instalando un convertidor de impedancias que convierten 100 ohms a 150 ohms de los STPs.

La longitud máxima de los cables de par trenzado está limitada a 90 metros, ya sea para 10 o 100 Mbps.

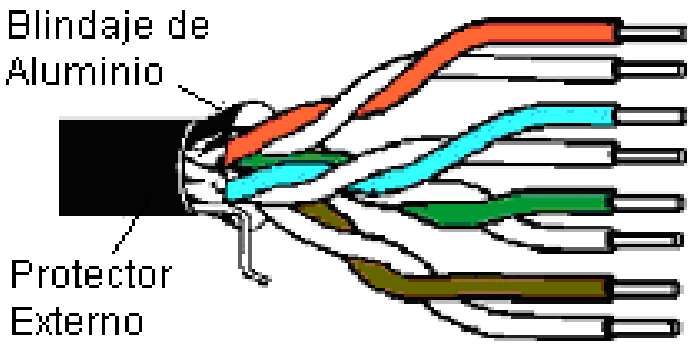

Figura 7.3. Cable de Par Trenzado Blindado de Cuatro Pares.

Fibra Óptica

Para disminuir el efecto de la radiación electromagnética de muy alta frecuencia, en el intervalo de la luz visible e infrarroja, se utiliza un cable de fibra de vidrio que causa muy poca pérdida de energía luminosa a través de largas distancias. El diámetro de la fibra debe ser muy pequeño, con el fin de minimizar la transmisión reflectora. La fibra transmisora central es de vidrio de baja pérdida y con índice de refracción relativamente alto (ver *Figura 7.4.*).

La fibra óptica se cubre con vidrio de mayor pérdida, con menor índice de refracción, para soporte y absorción de rayos que puedan escapar de la fibra central. La fuente de luz en el transmisor puede ser un diodo emisor de luz (LED) o un láser. El detector en el otro extremo es un fotodiodo o un fototransistor.

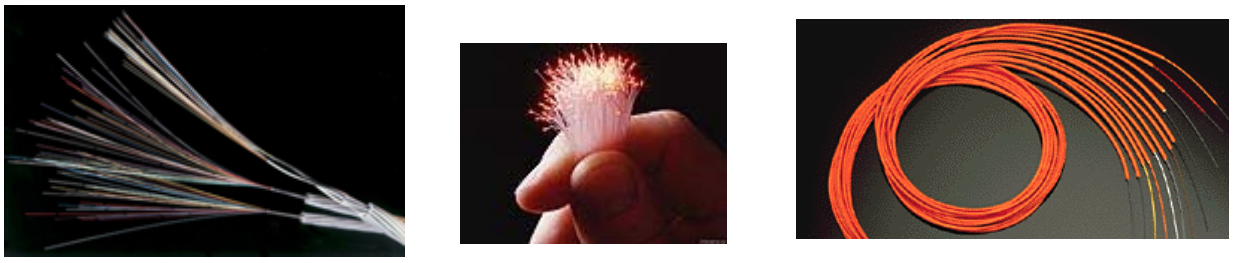

Figura 7.4. Fibra Óptica.

La transmisión óptica involucra la modulación de una señal de luz (usualmente apagando, encendiendo y variando la intensidad de la luz) sobre una fibra muy estrecha de vidrio (llamado núcleo). En la *Figura 7.5*, se muestran diferentes tipos de Conectores para la Fibra Óptica, de estos los que mas

destacan son los conocidos como ST (Conector del tipo clavija guía (BNC) con Cuerpo metálico y terminal cerámico) y SC (Conector del tipo “Push-Pull” con Cuerpo plástico y terminal cerámico).

Figura 7.5. Conectores de Fibra Óptica.

La otra capa concéntrica de vidrio que rodea el núcleo se llama revestimiento. Después de introducir la luz dentro del núcleo ésta es reflejada por el revestimiento, lo cual hace que siga una trayectoria zigzag a través del núcleo. La tecnología de la fibra óptica ha avanzado rápidamente. Existen en la actualidad dos métodos básicos (aunque se han desarrollado muchos más) para transmitir a través de un enlace por fibra y son conocidas como: transmisión en modo simple (monomodo) y transmisión multimodo, las cuales se describen a continuación.

Modo simple

Involucra el uso de una fibra con un diámetro de 5 a 10 micras. Esta fibra tiene muy poca atenuación y por lo tanto se usan muy pocos repetidores para distancias largas. Por esta razón es muy usada para troncales con un ancho de banda aproximadamente de 100 GHz por kilómetro (100 GHz-km).

Una de las aplicaciones más común de las fibras monomodo es para troncales de larga distancia, en donde se emplea para conectar una o más localidades, las ligas de enlace son los Backbone.

Multimodo

Existen dos tipos para este modo que son Multimodo / índice fijo y Multimodo / índice gradual. El primer tipo es una fibra que tiene un ancho de

banda de 10 a 20 MHz y consiste de un núcleo de fibra rodeado por un revestimiento que tiene un índice de refracción de la luz muy bajo, el cual causa una atenuación aproximada de 10 dB/km. Este tipo de fibra es usado típicamente para distancias cortas menores de un kilómetro. El cable mismo viene en dos tamaños 62.5/125 micras. Debido a que el diámetro exterior es de 1 mm, lo hace relativamente fácil de instalar y hacer empalmes. El segundo tipo Índice Gradual es un cable donde el índice de refracción cambia gradualmente, esto permite que la atenuación sea menor a 5 dB/km y pueda ser usada para distancias largas. El ancho de banda es de 200 a 1000 MHz, el diámetro del cable es de 50/125 micras, el primer número es el diámetro del núcleo y el segundo es el diámetro del revestimiento.

Los empalmes utilizados para conectar ambos extremos de las fibras causan también una pérdida de la señal en el rango de 1 dB. Así también los conectores o interfaces incurren también en pérdidas de 1 dB o más. Los haces de luz (LED) son transmitidos en el orden de 150 Mbps. El láser en cambio transmiten en el orden de Gbps. Los LEDs son típicamente más confiables que el láser, pero el láser en cambio provee más energía a una mayor distancia. Debido a que el láser tienen una menor dispersión son capaces de transmitir a velocidades muy altas en el modo de transmisión simple. Sin embargo, el láser necesita estar térmicamente estabilizado y necesita ser mantenido por personal más especializado.

La pérdida de luz en la transmisión es llamada atenuación. Varios factores influyen en ello, tales como la absorción por materiales dentro de la fibra, disipación de luz fuera del núcleo de la fibra y pérdidas de luz fuera del núcleo causado por factores ambientales. La atenuación en una fibra es medida al comparar la potencia de salida con la potencia de entrada. La atenuación es medida en decibeles por unidad de longitud. Generalmente está expresada en decibeles por kilómetro (dB/km). En la *Tabla 7.2*. se muestran características típicas de LEDs y lásers.

Características	LED	Laser
Ancho espectral	20-60 nm	0.5-6 nm
Corriente	50 mA	150 mA
Potencia de salida	5 mW	100 mW
Apertura numérica	0.4	0.25
Velocidad	100 MHz	2 GHz
Tiempo de vida	10,000 hrs.	50,000 hrs.
Costo	$1.00- $1500 USD	$100 - $10000 USD

Tabla 7.2. Características Típicas de los LEDs y los Lásers.

Conectores RJ45

El conector RJ45 o RJ48 de 8 hilos (o posiciones) es el más empleado para aplicaciones de redes (El término RJ viene de *Registered Jack / Conector de Registro*). También existen Jacks de 4 y 6 posiciones (e.g. el jack telefónico de 4 hilos conocido como RJ11). Los conectores de 8 posiciones están numerados del 1 a 8, de izquierda a derecha, cuando el conector es visto desde la parte posterior al ganchito (la parte plana de los contactos), tal como se muestra en la *Figura 7.6.*

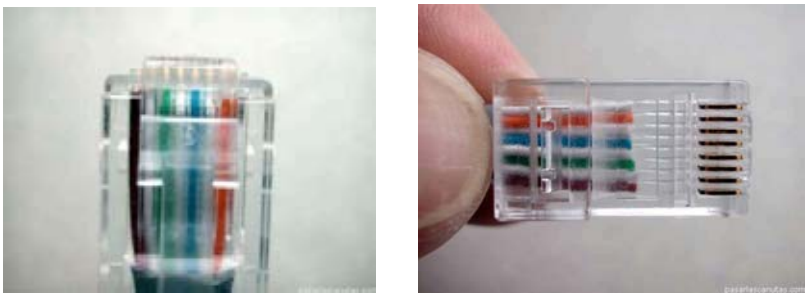

Figura 7.6. Conector RJ45.

Cualquier configuración puede ser usada para ISDN y aplicaciones de alta velocidad. Las categorías de cables transmisión 3, 4, 5, 5e y 6 son sólo aplicables a este tipo de grupos de pares. Para aplicaciones de Red, (e.g. Ethernet 10/100BaseT o Token Ring) sólo son usados dos pares, los 2 pares restantes se utilizarían para otro tipo de aplicaciones, voz, por ejemplo. En la Figura 7.7, se muestran las diversas configuraciones para las Redes.

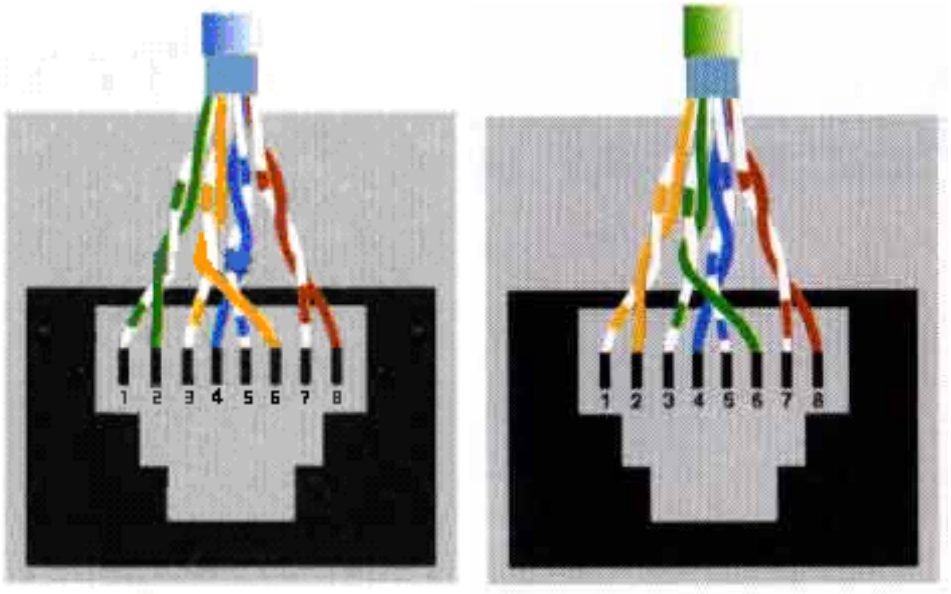

Figura 7.7. Configuración de Cables. (Continuación)

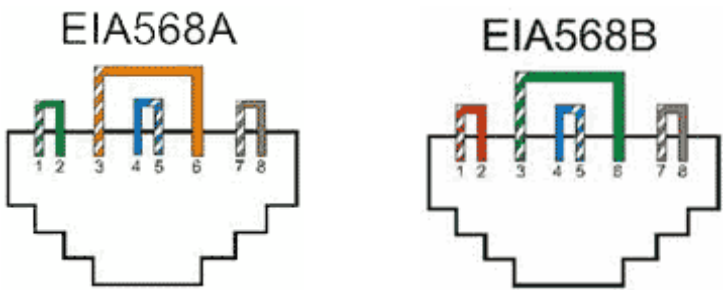

Figura 7.7. Configuración de Cables.

Un cable directo sirve para conectar la tarjeta de red de una computadora a un Hub o a un Switch, mientras que un cable cruzado sirve para conectar dos computadoras entre sí, dos hubs o switches entre sí. Algunos hubs o switches pueden tener enchufes que cambien de directo a cruzado mediante un interruptor, otros tienen un enchufe especial para ese propósito, marcado con "X". En la Figura 7.8, se muestran estos tipos de conexión en los cables.

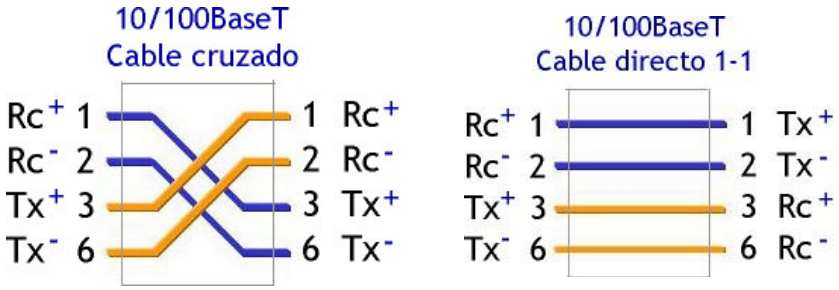

Figura 7.8. Configuración de Cables Directo y Cruzado.

En la *Tabla 7.3,* se presenta un resumen de las especificaciones de cable Ethernet.

Especificación	Tipo de Cable	Longitud Máxima
10BaseT	UTP	100 metros
10Base2	Thin Coaxial	185 metros
10Base5	Thick Coaxial	500 metros
10BaseF	Fibra Óptica	2000 metros
100BaseT	UTP	100 metros
100BaseTX	UTP	220 metros

Tabla 7.3. Sumario de Cable Ethernet.

8. BIBLIOGRAFÍA

Libros:

- *Albritton, John*
  Cisco IOS Essentials CCIE #2833
  Ed. Mcgraw-Hill
  New York EE.UU., 1999

- *Caballero, José Manuel*
  Redes de Banda Ancha
  Ed. AlfaOmega
  México D.F., 1998

- *Caballero Gil, Pino*
  Seguridad Informática,
  Técnicas Criptográficas
  Ed. AlfaOmega
  México D.F., 1997

- *Constantino, Cathy A.*
  Diseño de Sistemas para Enfrentar Conflictos
  Ed. Granica
  Barcelona España, 1997

- ***Comer Douglas E.***
  Stenes David L.
  Interconectividad de Redes con TPC/IP: Diseño e Implementación Volumen III, 3° Ed.
  Ed. Person Educación
  México D.F., 2000

- *Esteve Domingo, Manuel*
  Diseño de Redes Corporativas
  Ed. Universidad Politecnica de Valencia, Servicio de Publicaciones
  Valencia España, 1997

- *Herrera Pérez, Enrique*
  Introduccion a las Telecomunicaciones Modernas
  Ed. Limusa-Noriega
  México D.F., 1998

- *Huidrobro Moya, José Manuel*
  Redes de Comunicaciones
  Ed. Paraninfo
  Madrid España, 1992

- *James Thomas, Martin*
  Las Telecomunicaciones y las Computadoras
  Ed. Diana
  México D.F., 1972

- *Laden Hyman, Nathaniel*
  Diseño de Sistemas de Cómputo
  Ed. Limusa.
  México D.F., 1971

- *Molina Mateos, José Maria*
  Seguridad, Información y Poder: una perspectiva conceptual y jurídica de la criptología
  Ed. Incipit
  Madrid España, 1994

- *Nombela, Juan José*
  Seguridad Informática
  Ed. Paraninfo
  Madrid España, 1997

- *Odon Sean*
  Nottingham Hanson
  Cisco Switching
  Ed. Coriolisis
  Scottsdale Arizona, 2001

- *Rudenko Innokenty*
  Cisco Routers for IP, Networking Black Book
  Ed. Coriolisis
  Scottsdale Arizona, 2000

- *Rovert T, Dave*
  Protocolos de Internet
  Ed. Paraninfo
  Madrid España, 1997

- *Sánchez López Rafael.*
  Sistema Electrónicos Digitales
  Editorial Alfaomega.
  México D.F., 1993.

- *Slotz, Kevin*
  Todo Acerca de las Redes de Computadoras
  Ed. Prentice Hall – Hispanoamericana
  México D.F., 1995

- *William Stallings*
  Comunicaciones y Redes de Computadoras 6° Ed.
  Ed. Prentice – Hall
  Madrid-México, 2000

- *Wilson Narváez*
  Michelle Brahm
  iPass Interoperability:
  iPass RoamServer and
  CiscoSecure ACS

- *Wilson Narváez*
  Michelle Brahm
  Configuration Instructions for Interoperability of
  iPass RoamServer™ and CiscoSecure Access
  Control Server™ v3.0 for Windows NT/2000

Artículos y Manuales:

- *Cisco System, Inc.* Cisco Secure PIX Firewall, Student Guide. Cisco. USA, 2001.
- Cisco System, Inc. Cisco Secure Intrusion Detection System, Student Guide. Cisco USA, 2001.
- Cisco Systems, Inc, Interconexión de Dispositivos de Red Cisco. México, 2001.

Cursos:

- La necesidad de VPNs Autenticación y Encripción de datos.
  Los retos reales de implementar VPNs
  Autor: OVL

- 3800 Bridge Parkway
  Redwood Shores, California
  94065 USA

- Cronología de la telefonía en México
  Tomada de la Historia de la Telefonía en México
  1878 - 1991. Teléfonos de México, Subdirección de Comunicación Social.

- Del Mar College
  ITSC 1391 - Internetworking Technologies
  Instructor: Michael P. Harris, CCNA

Páginas WEB:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/
Internetworking Technology Handbook, Cisco System

http://www.cft.gob.mx/html/la_era/info_tel2/hist2.html
Cronología de la Telefonía en México

http://www.bizinetworks.com/index.html?referrer=genericnetwork
BIZI International

http://www.cisco.com/en/US/products/hw/routers/ps341/prod_quick_installation_guide09186a00800a93b6.html
Cisco 7200 Series VXR Quick Start Guide

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/qsg30/501quick.pdf
Cisco PIX 501 Firewall Quick Start Guide

http://www.delmar.edu/Courses/ITSC1391/Sem3/6ACLs.htm
Cisco Sem3 Lesson 6, ACLs

http://www.signus-web.com/networkers/archivos/ccna.htm#bibliograf
Cisco Certified Network Associate

http://tejo.usal.es/~nines/d.alumnos/modems/p1.htm
Protocolos de Enlace de Datos: Introducción

http://www.newdevices.com/tutoriales/tcp-udp/1.html
Capa de transporte del protocolo TCP-IP

http://www.nodo50.org/manuales/internet/protocolos.htm
Protocolos

http://www.monografias.com/trabajos/redesconcep/redesconcep.shtml
Conceptos Básicos de Comunicación de Datos

http://www.itlp.edu.mx/publica/tutoriales/redes/tema12.htm
Modelo OSI

www.cisco.com
Cisco Systems

www.3com.com
3Com Systems

www.lucent.com
Lucent Technologies

www.nortelnetworks.com
Nortel Networks

http://www.vermicelli.pasta.cs.uit.no/ipv6/students/vegars/Bibliography/icpdf.pdf
Cisco Secure VPNs Client, Solutions Guide