ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UNA VPN EN UNA EMPRESA COMERCIALIZADORA UTILIZANDO IPSEC

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA
MENCIÓN: REDES DE INFORMACIÓN

EDISON RAFAEL TRUJILLO MACHADO

DIRECTOR: ING. EDGAR TORRES

Quito, marzo del 2006

DECLARACIÓN

Yo, Edison Rafael Trujillo Machado, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Edison Rafael Trujillo Machado

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Edison Rafael Trujillo Machado, bajo mi supervisión.

_____

Ing. Edgar Torres
DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Agradezco a Confiteca por brindarme las facilidades para poder realizar el Proyecto de Titulación.

Al director del proyecto Ing. Edgar Torres, quien me guió con sus conocimientos y experiencia en la elaboración de la tesis.

A la Escuela Politécnica Nacional por haberme permitido obtener en sus aulas mi sueño de ser un profesional de la República.

DEDICATORIA

Este trabajo esta dedicado con mucho cariño y entrega a mis padres, quienes con su esfuerzo y sacrificio siempre me apoyaron en mis estudios.

A mis hermanos por su ayuda y como un ejemplo de superación.

A mis hijas y esposa por ser la motivación en mi vida.

CONTENIDO

INDICE DE FIGURAS

CAPITULO 1

CAPITULO 2

CAPITULO 3

CAPITULO 4

INDICE DE TABLAS

RESUMEN

El presente trabajo comprende el diseño e implementación de una VPN en una empresa comercializadora utilizando IPSec.

Ha sido estructurado en 5 capítulos, a continuación se muestra una visión de los contenidos de cada sección:

Capítulo 1. Presenta una reseña de la evolución del Internet, los diferentes tipos de conexión, los proveedores de este servicio en el Ecuador, y las tecnologías de conexión WAN que se han utilizado hasta la actualidad.

Capítulo 2. Comprende todo lo relacionado con las Redes Privadas Virtuales como son los tipos, arquitectura, tecnologías de tunneling. También se analiza las funcionalidades y aplicaciones del protocolo IPSec dentro de las VPN.

Capítulo 3. Se hace un estudio de la situación organizacional y tecnológica de la empresa comercializadora tomada como caso de estudio para este trabajo, y sus posibles implementaciones VPN.

Capítulo 4. Se documenta la implementación de un prototipo VPN dentro de la empresa comercializadora, se hace un análisis de costos, ventajas, desventajas con respecto a las líneas dedicadas.

Capítulo 5. Consta de las conclusiones y recomendaciones.

Finalmente las referencias bibliográficas y los anexos.

PRESENTACIÓN

En los últimos años la popularidad de las Redes Privadas Virtuales ha crecido, debido a que las empresas buscan la forma de reducir los costos que representan las conexiones de líneas dedicadas entre sus diferentes agencias.

El presente proyecto está desarrollado con el propósito de que sea una fuente de consulta para todos los estudiantes y profesionales de carreras de Sistemas, Redes y Telecomunicaciones.

Orientado específicamente al análisis de las Redes Privadas Virtuales implementadas con el protocolo IPSec, se toma en cuenta el factor económico que siempre será crítico en cualquier organización, sin dejar a un lado el rendimiento de la red y las aplicaciones.

El protocolo IPSec es un estándar de seguridad que han adoptado la mayoría de fabricantes de software y hardware, lo que hace más factible utilizar este protocolo en una VPN sin necesidad de adquirir una marca específica de dispositivo o sistema operativo.

Se plantean algunos escenarios de implementación con sus respectivos elementos necesarios, para disponer de varias opciones a la hora de escoger la mejor.

Se implementa un prototipo práctico donde se puede visualizar la funcionalidad de la VPN y se analiza los resultados de las pruebas realizadas, para cuantificar los elementos que serían utilizados en la implementación a gran escala.

1. TECNOLOGÍAS DE ACCESO A INTERNET Y ENLACES PRIVADOS

1.1. INTRODUCCIÓN

Internet es la red de computadoras más grandes de todo el mundo, de la que forman parte miles de redes distribuidas por todo el planeta. Su origen tuvo lugar a finales de 1960 con la red ARPANET (una red formada por más de 60.000 computadoras) desarrollada por el Advanced Research Proyects Agency del Departamento de Defensa de los Estados Unidos, en los setenta llega a las universidades. Posteriormente se desarrolló una nueva tecnología conocida como Packet Switching (conmutación de paquetes) que recibió el nombre de Transmission Control Protocol e Internet Protocol (TCP/IP). A finales de los ochenta Internet fue expandiéndose por todo el mundo abandonando la red ARPANET en 1990.

A partir de esta fecha se consideró como núcleo de la Internet a National Science Foundation (NSF). En 1995 la NSF entregó la espina dorsal de la red a empresas de telecomunicaciones tales como Sprint, American y Pacific Bell. Actualmente se estima que existan aproximadamente 3 200 000 computadoras en todo el mundo conectadas a la red.

Múltiples son las ventajas que brinda Internet. Permite compartir recursos de información de diferentes tipos como: estadística, tecnológica, económica, comercial, política y social, científica y cultural ubicados en bibliotecas, universidades y otras. A esta información se puede acceder mediante distintos servidores tales como Gopher, protocolo de transferencia de archivos (FTP), conexión remota (TELNET) y WWW. Además mejora la comunicación a través del correo electrónico, TALK (hablar en tiempo real), IRC (Internet Relay Chat), permitiendo que personas con intereses comunes, ubicadas en diferentes áreas geográficas puedan interrelacionarse entre sí.

Miles de millones de personas se conectan diariamente a Internet ya sea para revisar el correo electrónico, leer las noticias del día o chatear unos minutos con amigos.

1.2. LA EVOLUCIÓN DE INTERNET

Las mayores aportaciones tecnológicas de Internet se centran en la aparición de los navegadores, la simplicidad y potencia de los protocolos utilizados, y el uso de los lenguajes de programación en red, que han provocado la aparición de nuevos modelos de servicios.

1.2.1. MODELOS DE SERVICIOS Y PROTOCOLOS

El protocolo utilizado en 1969 para interconectar los ordenadores de la red DARPA se conoció con el nombre de Network Communication Protocol (NCP) y en poco tiempo daría paso al más conocido Transmission Control Protocol/Internet Protocol (TCP/IP). En este protocolo se propone un modelo de interconexión de redes, mediante gateways, que adaptan dinámicamente la información a los requisitos de cada subred que interconectan. Constituyen un protocolo extremo a extremo, que es transparente a las particularidades de cada subred; esto le permite utilizar redes heterogéneas en cada comunicación. Estos protocolos se basan en un modelo de servicios “best effort”, donde la red ofrece un servicio de tipo datagrama cuya principal atención se dirige a la entrega de paquetes.

La simplicidad de estos protocolos ha sido sin duda uno de los factores determinantes en su éxito como tecnología para redes de datos. Sin embargo, resultan insuficientes para soportar nuevas aplicaciones como por ejemplo telefonía o videoconferencia, que necesitan obtener ciertas garantías de calidad de servicio de la red, especialmente si se tiene presente que el ancho de banda va a seguir estando limitado, incluso con el despliegue de las futuras redes de banda ancha.

En julio de 1994, la Internet Engineering Task Force (IETF) acordó introducir una serie de cambios sobre el protocolo de interconexión de redes hasta entonces utilizado en Internet. En 1995 se publicaron las RFC’s o recomendaciones que servirían como especificación para la implementación del protocolo Internet Protocol Next Generation (IPng), cuyo nombre formal es IPv6, frente al utilizado en la actualidad que es IPv4. El nuevo protocolo es compatible con el anterior, a fin de que su introducción no cause problemas en Internet. Se trata de un

protocolo diseñado tanto para redes de grandes anchos de banda (ATM) como para pequeños anchos de banda (radio). Asimismo, IPv6 proporciona un mayor direccionamiento de elementos conectados a la red, pues pasa de direcciones de 32 bits en la actualidad a direcciones de 128 bits.

Junto a la propuesta de IPv6, diversos grupos de trabajo del IETF plantearon extender la arquitectura del modelo de red datagrama, con el objeto de que pueda soportar tanto aplicaciones en tiempo real como los servicios tradicionales de datos.

El resultado es una arquitectura integrada de servicios, en cierta medida paralela al modelo de servicios de la RDSI. Está constituida por un modelo de servicio basado en mecanismos de reserva de recursos de red que garantiza a las aplicaciones diversos parámetros de calidad de servicio como, por ejemplo, ancho de banda, latencia. Actualmente, estos mecanismos se están especificando dentro del protocolo ReSerVation Protocol (RSVP), que permite reservar recursos de red a los flujos de datos dirigidos hacia la misma entidad de transporte destino (sesión de comunicaciones). El modelo de servicios también considera la asignación de prioridades a los paquetes IP, que los elementos de red pueden utilizar para controlar el tráfico y la tarificación.

Una implementación de referencia del modelo en la que se introducen nuevas funciones en los futuros elementos de red (routers IP): control de admisión, clasificador y planificador de paquetes.

En la actualidad están apareciendo, paralelamente a la definición de este nuevo modelo de servicios, nuevas tecnologías de elementos de red destinadas a soportar mejor los servicios Internet sobre infraestructuras de banda ancha ATM. Las soluciones actuales (IP clásico sobre ATM, emulación de redes de área local o ATM Multiprotocolo) se basan en el despliegue de una red superpuesta formada por routers IP. Estas soluciones son poco satisfactorias, tanto por la duplicidad de funciones entre ambas redes (encaminamiento), como por el hecho de que los routers convencionales son incapaces de aceptar un tráfico elevado de paquetes IP sobre, por ejemplo, interfaces ATM a 622 Mbps.

Un ejemplo de estas tecnologías es la denominada conmutación IP, que combina la flexibilidad del encaminamiento IP junto con las prestaciones de la conmutación hardware ATM.

Actualmente, las tecnologías de conmutación IP son propiedad registrada, si bien se han publicado los protocolos empleados en propuestas de estándar de Internet. Estas propuestas incluyen la definición de una interfaz programática de control de un conmutador ATM, con la finalidad de conseguir la separación efectiva entre las funciones de control (router IP inteligente) y las de conmutación ATM.

1.2.2. EVOLUCIÓN DEL MERCADO

Es notable la revolución que tanto socialmente como en el mundo de las telecomunicaciones, ha supuesto Internet; además los enormes crecimientos de esta red en número de usuarios y tráfico generado hacen prever que no se trata de una moda pasajera, sino que estamos ante un fenómeno cuyas primeras consecuencias ya se empiezan a ver.

En la tabla 1.1, se puede apreciar las estadísticas de usuarios del Internet en el mundo, actualizadas en febrero 3 del 2.005. [1] Las cifras de crecimiento fueron determinadas comparando el dato de usuarios actuales de Internet con los datos del año 2.000 de las estadísticas de ITU.

ESTADISTICAS MUNDIALES DEL INTERNET Y DE POBLACION						
Regiones	**Población (2005)**	**% Población Mundial**	**Usuarios, dato más reciente**	**Crecimiento (2000-2005)**	**% Población (Penetración)**	**(%) de Usuarios**
Africa	900,465,411	14.0 %	**12,937,100**	186.6 %	1.4 %	1.6 %
Asia	3,612,363,165	56.3 %	**266,742,420**	133.4 %	7.4 %	32.6 %
Europa	730,991,138	11.4 %	**230,923,361**	124.0 %	31.6 %	28.3 %
Oriente Medio	259,499,772	4.0 %	**17,325,900**	227.8 %	6.7 %	2.1 %
Norte América	328,387,059	5.1 %	**218,400,380**	102.0 %	66.5 %	26.7 %
Latinoamérica / Caribe	546,917,192	8.5 %	**55,279,770**	205.9 %	10.1 %	6.8 %
Oceanía	33,443,448	0.5 %	**15,838,216**	107.9 %	47.4 %	1.9 %
TOTAL MUNDIAL	**6,412,067,185**	**100.0 %**	**817,447,147**	**126.4 %**	**12.7 %**	**100.0 %**

Tabla 1.1. Estadísticas de usuarios de Internet en el mundo.

[1] Fuente: Exito Exportador (http://www.exitoexportador.com/stats.htm)

1.3. TIPOS DE CONEXIONES A INTERNET

Existen muchas maneras de conectarse a Internet, no todos los tipos de conexiones están disponibles en cada área geográfica, así que la elección puede estar limitada a lo que los proveedores locales pueden ofrecer al cliente.

Las conexiones más comunes en Internet son las telefónicas, pero también existen otras fórmulas de conexión.[2]

- Conexión telefónica.
- Fibra Óptica.
- Conexión Vía Satélite.
- Teléfonos Móviles.
- Internet por Televisión.
- Ondas de Radio.
- Red Eléctrica.
- Otros Sistemas.

1.3.1 CONEXIÓN TELEFÓNICA

1.3.1.1. Red Telefónica Conmutada (RTC)

La constituye la conexión telefónica convencional, (Red Telefónica Básica) para la comunicación hablada. Es la conexión tradicional analógica por la que circulan las vibraciones de voz. Estas vibraciones se traducen en impulsos eléctricos y se transmiten a través de los hilos de cobre de la red telefónica normal.

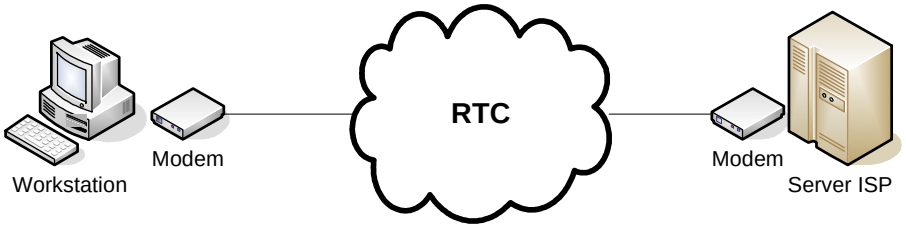

Figura 1.1. Conexión a Internet por Red Telefónica Conmutada.

[2] Fuente: http://www2.canalaudiovisual.com/ezine/books/jirnet/2net52.htm

Para acceder a la Internet es necesario tener una línea de teléfono y un módem que se encargará en convertir la señal del ordenador, que es digital, en analógica para transferir la información por la línea telefónica.

En Ecuador se utiliza ampliamente este tipo de conexión a Internet y según datos de la Superintendencia de Telecomunicaciones, se tienen 422060 usuarios dial up.[3]

Actualmente este tipo de conexiones supone muchos problemas por la velocidad del módem ya que alcanza como máximo 56 Kbps. Al ser un tipo de conexión muy lenta dificulta enormemente descargas de archivos de gran tamaño y accesos a páginas con contenidos multimedia (imagen, sonido, flash, etc).

1.3.1.2. Red Digital de Servicios Integrados (RDSI)

Permite enviar datos codificados digitalmente por medio del cable telefónico normal de cobre*.* A diferencia del anterior no necesita un módem para transformar la información en analógica, pero sí un adaptador de red, módem RDSI o tarjeta RDSI, para adecuar la velocidad entre el PC y la línea. El aspecto de esta tarjeta es muy parecido al módem interno de una conexión RTC o incluso una tarjeta de red.

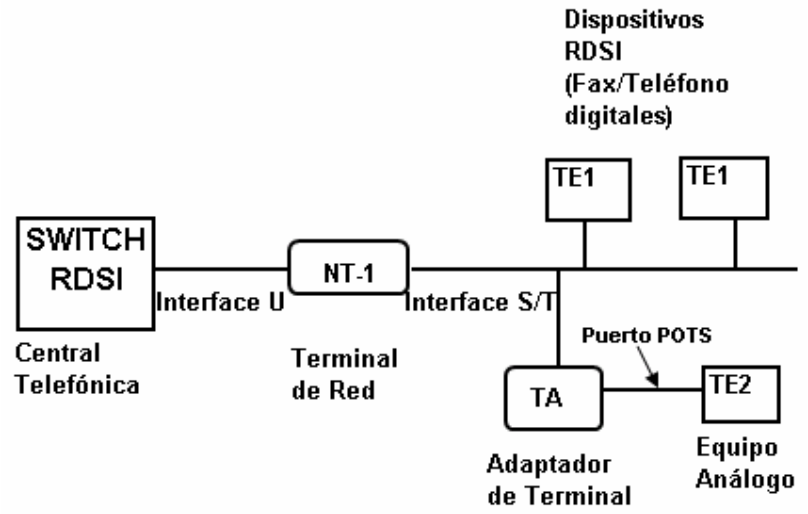

Figura 1.2. Diagrama de Interfaces y equipos en una conexión RDSI básico.[4]

[3] Fuente: http://www.supertel.gov.ec/telecomunicaciones/v_agregado/estadisticas/internet.htm
[4] Fuente: http://web.frm.utn.edu.ar/comunicaciones/isdn.html

La Red Digital de Servicios Integrados realmente ha fracasado como alternativa a las líneas de alta velocidad. Los motivos de son el elevado costo, las dificultades de instalación y un servicio deficiente por parte de las compañías telefónicas.

1.3.1.3. Asymmetrical Digital Subscriber Line (ADSL)

Línea de Abonado Digital Asimétrica, este sistema permite transmitir información en formato digital a través de las líneas normales de teléfono. Utiliza frecuencias que no utiliza el teléfono normal, por lo que es posible conectar con Internet y hablar por teléfono a la vez mediante la instalación de un splitter o filtro separador. Este dispositivo no es más que un conjunto de dos filtros: uno paso alto y otro paso bajo. La finalidad de estos filtros es la de separar las señales transmitidas por el bucle de modo que las señales de baja frecuencia (telefonía) de las de alta frecuencia (ADSL).[5]

Las velocidades que se pueden alcanzar son de hasta 8 Mbps de recepción y de hasta 1 Mbps de envío de datos. No obstante, la velocidad de transmisión también depende de la distancia del módem a la centralita, de forma que si la distancia es mayor de 3 Kilómetros se pierde parte de la calidad y la tasa de transferencia empieza a bajar.

En la figura 1.3 se observa que además de los módems situados en casa del usuario (ATU-R o "ADSL Terminal Unit-Remote") y en la central (ATU-C o "ADSL Terminal Unit-Central"), delante de cada uno de ellos está instalado el "splitter".

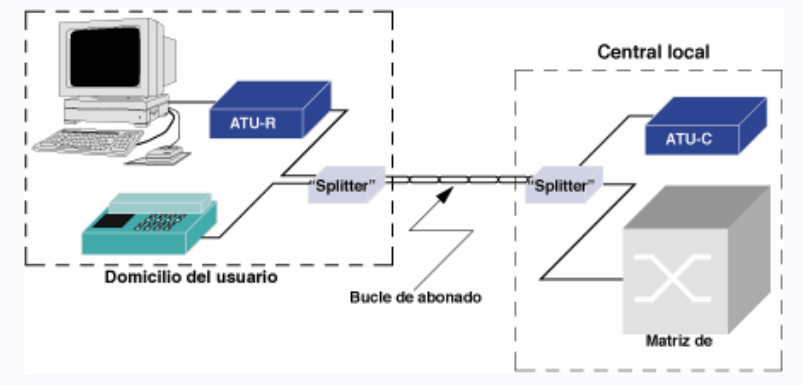

Figura 1.3. Conexión a Internet con ADSL.

[5] Fuente: http://www.wikilearning.com/que_es_el_adsl-wkccp-3389-2.htm

1.3.2. FIBRA ÓPTICA

Los usuarios de este tipo de conexión, además del Internet, tienen la posibilidad de recibir servicios como televisión de pago, video bajo demanda, telefonía, etc. Mediante la fibra óptica se pueden alcanzar velocidades teóricas de hasta 30 Mbps, pero lo normal es disponer de alrededor de 300 Kbps. Se trata de una tecnología totalmente distinta donde en lugar de establecer una conexión directa, o punto a punto, con el proveedor de acceso, se utilizan conexiones multipunto, en las cuales muchos usuarios comparten el mismo cable. Cada punto de conexión a la red o nodo puede dar servicio a entre 500 y 2000 usuarios y la distancia de éste al usuario no puede superar los 500 metros. Al tratarse de una conexión compartida.

Las posibilidades son ilimitadas: a través de tarifa plana se pueden realizar videoconferencias, petición de video; y por vía TV, seleccionar programas y canales a la carta, grabar emisiones en directo y participar en concursos interactivos.

Su mayor inconveniente es que, en la actualidad, tan solo se puede encontrar en determinadas zonas de las grandes ciudades. La velocidad de subida puede rozar la cifra de 1 Mbps; por otra parte hay que saber que es un sólo cable el que transmite los datos de abonado en abonado, repartiendo el ancho de banda entre cientos de ellos, además de las interferencias que recibe del entorno.

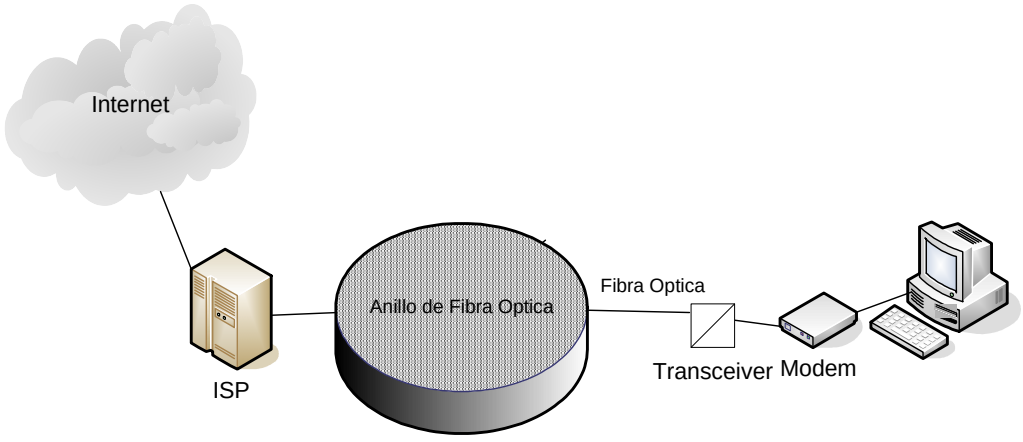

Figura 1.4. Acceso a Internet por fibra óptica.

1.3.3. CONEXIÓN VÍA SATÉLITE

Existen dos tipos de conexión vía satélite:

- Unidireccional**,** la subida o petición de datos y el envío de correo electrónico se realiza con el proveedor de Internet vía modem tradicional, pero la bajada se realiza mediante una antena parabólica orientada al correspondiente satélite y una tarjeta PCI/USB-DVB instalada en el ordenador.
- Bidireccional, las subidas y bajadas de datos se realizan vía parabólica hacia el satélite.

Por tanto para este tipo de conexión hay que tener instalada una antena parabólica digital, un acceso telefónico a Internet (utilizando un módem RTC, RDSI, ADSL o por cable), una tarjeta receptora para PC**,** un software específico y una suscripción a un proveedor de satélite.

El cibernauta envía sus mensajes de correo electrónico y la petición de las páginas Web, que consume muy poco ancho de banda, mediante un módem tradicional, pero la recepción se produce por una parabólica, ya sean programas informáticos, vídeos o cualquier otro material que ocupe muchos megas. La velocidad de descarga a través del satélite puede situarse en casos óptimos en torno a 400 Kbps. [6]

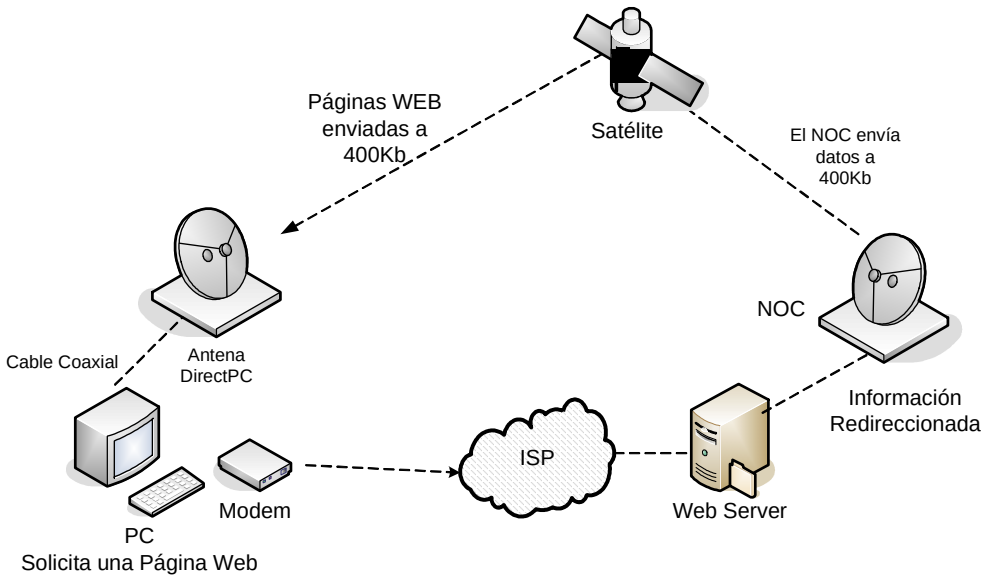

Figura 1.5. Internet por Satélite.

[6] Fuente: http://w3.cnice.mec.es/programa/usuarios/ayudas/tipo_conexion.htm

1.3.4. TELÉFONOS MÓVILES

Según datos de la International Telecommunication Union (ITU), a finales de 2001 en todo el mundo había más de 1.000 millones de teléfonos móviles, mientras que en 1993 había sólo 50 millones de móviles y 600 millones de fijos. A pesar de esta reducción del crecimiento, las estimaciones de la ITU para el año 2003, fueron de 1600 millones de móviles y 1.200 millones de fijos.

1.3.4.1. WAP (Wireless Application Protocol)

Fruto de la asociación de fabricantes como Nokia y Ericcson en 1977, este sistema permite acceder a través de dispositivos inalámbricos (como teléfonos móviles), la recepción de información está muy limitada por la velocidad de transmisión inalámbrica (9.600 bits por segundo) y por las reducidas dimensiones de la pantalla.

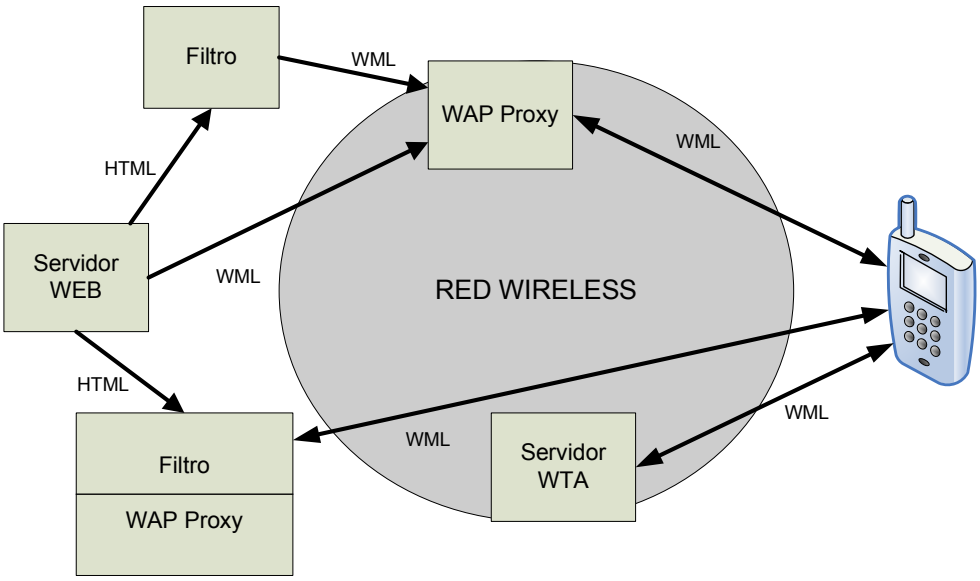

Figura 1.6. Acceso a Internet por WAP.[7]

[7] Fuente: http://www.tlm.unavarra.es/asignaturas/bi/bi99_00/mejores/bi02/

1.3.4.2. GPRS (General Packet Radio Service)

Tecnología que permite la transmisión de datos a alta velocidad a través de redes inalámbricas, proporcionando servicios como por ejemplo acceso a Internet y Correo Electrónico.

El GPRS viene a complementar el GSM, al añadirle un sistema basado en la transmisión de paquetes de datos a la red ya existente. Las operadoras GSM (Global System for Mobile Communications) mundiales están adoptando esta tecnología de transmisión de datos por paquetes denominada GPRS que permite a los usuarios de teléfonos móviles conexiones de 115 Kbps – 177,2 Kbps.

El volumen de tráfico generado por la expansión del GPRS aumenta la presión sobre la red GSM (que ambas tecnologías comparten), lo que constituye un argumento poderoso para que se ponga en marcha la nueva red UMTS.

Entre las posibilidades ofrecidas por el GPRS se incluyen:

- Chat.
- Navegación en la red.
- WAP sobre GPRS.
- Imágenes.
- E-mail.
- Audio.
- Transferencia de documentos.

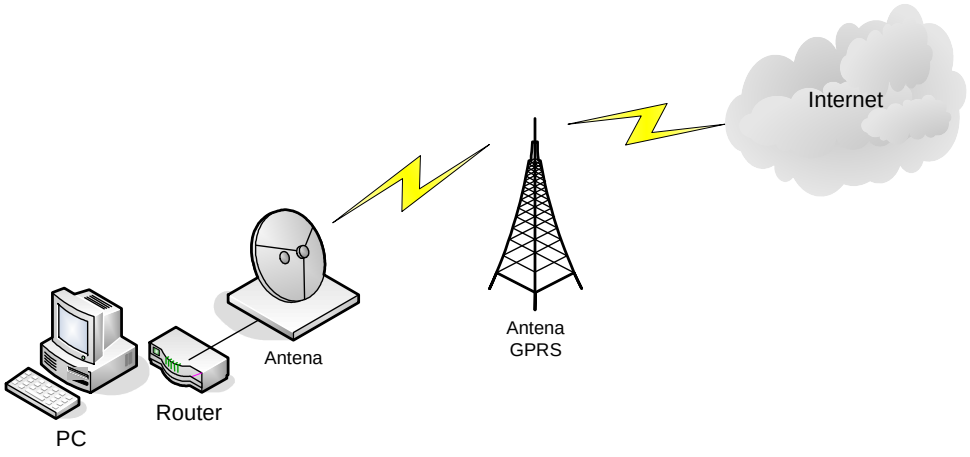

Figura 1.7. Tecnología GPRS.

1.3.4.3. UMTS (Universal Mobile Telecommunication System)

Aún no han acabado de aterrizar los WAP y ya se anuncia una nueva tecnología de transporte de voz y datos que dejará en pañales todo lo existente. El sistema UMTS (Universal Mobile Telecommunications System) permitirá el acceso a Internet a altas velocidades, descarga de páginas web completas (con imágenes, video y sonido), videoconferencia, etc.

Las razones que harán triunfar a UMTS son:

- UMTS permitirá a la Sociedad de la información del mañana, el uso de información de todo tipo a cualquier hora, el desarrollo del comercio y servicios de ocio; todo ello tanto a los usuarios de móviles conectados entre sí, como a los usuarios de móviles a través de soporte inalámbrico y soporte a través del satélite.
- UMTS hará más rápida la convergencia entre las telecomunicaciones, IT, sistemas multimedia y contenidos industriales para dar lugar a nuevos servicios y crear nuevas oportunidades.
- UMTS hará bajar los precios y aumentará la capacidad de comunicación de los móviles, ofreciendo *data rates* superiores a 2Mbit/sec. [8]

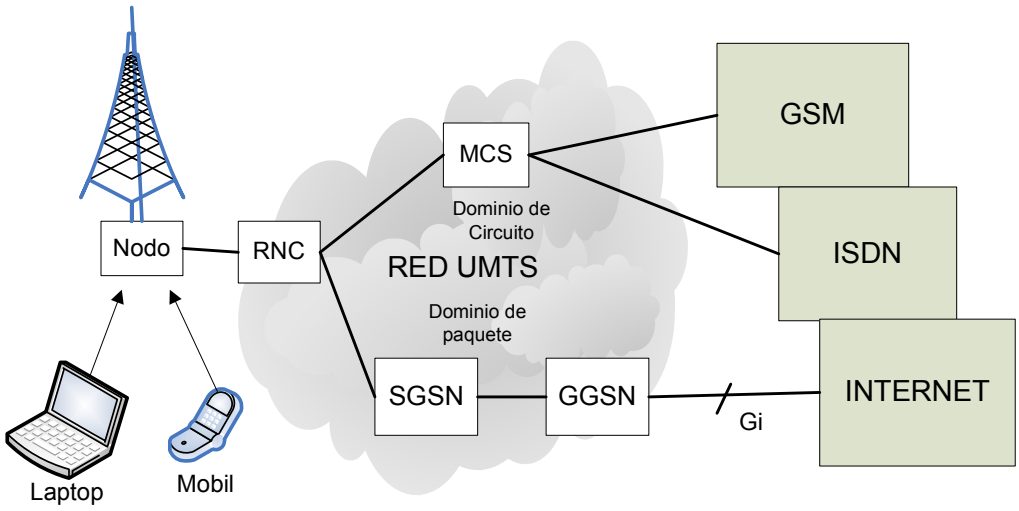

Figura 1.8. Red de transmisión UMTS.[9]

[8] Fuente: http://www.tlm.unavarra.es/asignaturas/bi/bi99_00/mejores/bi02/
[9] Fuentehttp://es.wikipedia.org/wiki/UMTS

1.3.5. INTERNET POR TELEVISIÓN

Algunas empresas que ofrecen servicios de televisión por cable, han introducido al mercado un innovador sistema que a través de un dispositivo denominado Cable módem permite conectar una computadora a Internet, con una velocidad hasta 10 veces superior a la de un sistema telefónico tradicional.[10]

Un cable-módem es un dispositivo que permite conectar el PC a una línea local de TV por cable a aproximadamente 1.5 Mbps.

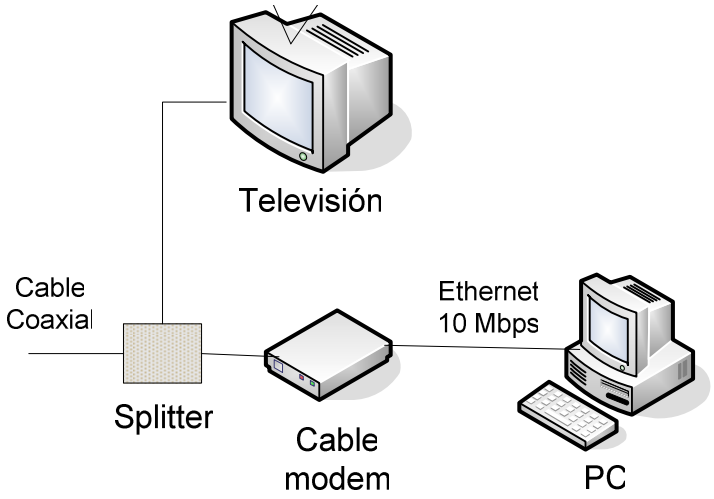

Figura 1.9. Internet por Televisión.

Un cable-módem puede ampliarse o integrarse a una caja "set top" que convierte nuestro televisor en un canal de Internet. Para conectarse al PC, la línea de cable debe dividirse de modo que parte de ella vaya al televisor y la otra parte al módem cable y al PC.

El ancho de banda real para el servicio de Internet por medio de una línea de cable de TV es de hasta 27 Mbps en el camino de bajada hacia el suscriptor, con un ancho de banda de aproximadamente 2.5 Mbps para respuestas interactivas en dirección opuesta. Pero, la tasa más verosímil de transferencia de datos estará cerca a los 1.5 Mpbs.[11]

[10] Fuente: http://ciberhabitat.gob.mx/museo/estreno/cablemodem.htm
[11] Fuente: http://www2.terra.com/informatica/que-es/cablemod.cfm

1.3.6. RED ELÉCTRICA

La idea de transmitir datos empleando la red eléctrica no es nueva pero desde hace un par de años las compañías eléctricas de Brasil, Alemania y Korea están conectando usuarios por este sistema.

PLC (*Power Line Communications*) es una tecnología que posibilita la transmisión de voz, vídeo y datos sobre las redes eléctricas. Es decir, transporta todos los servicios de una red IP (Internet) hasta la toma de corriente de los hogares u oficinas. Para ello hay que conectar la red de telecomunicaciones a la estación de transformación y desde ahí emplear la red eléctrica para llegar al cliente final.

Al usuario le basta un módem PLC conectado a cualquier enchufe para recibir la conexión de banda ancha. Este módem recibe la señal de un repetidor situado en el cuarto de contadores del edificio (que puede atender hasta 256 equipos), que está conectado a su vez a un centro de distribución del que recibe los datos a una velocidad de hasta 200 Mbps (una conexión de ADSL doméstica convencional ofrece medio megabit).[12]

En España las empresas Endesa e Iberdrola han llevado a cabo pruebas, el ancho de banda del que se puede disponer alcanza en las pruebas entre 2 y 10 Mbps según la tecnología empleada.

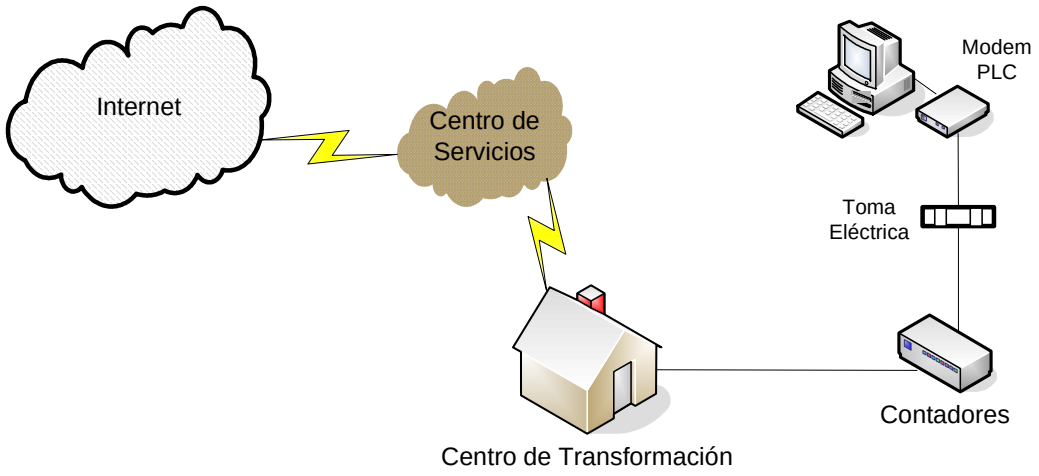

Figura 1.10. Internet por Red Eléctrica.

[12] Fuente: http://www.consumer.es/accesible/es/tecnologia/internet/2005/07/21/143900.php

1.3.7. ONDAS DE RADIO

Local Multipoint Distribution System (LMDS) es un sistema de comunicación inalámbrica de punto a multipunto, que utiliza ondas radioeléctricas a altas frecuencias, entorno a 28 y 40 GHz. Esto es una transmisión vía radio, similar a la de la telefonía móvil, pero con un mayor ancho de banda con velocidades de usuario de hasta 8 Mbps.

Este sistema de conexión da soporte a una gran variedad de servicios simultáneos: televisión multicanal, telefonía, datos, servicios interactivos multimedia.

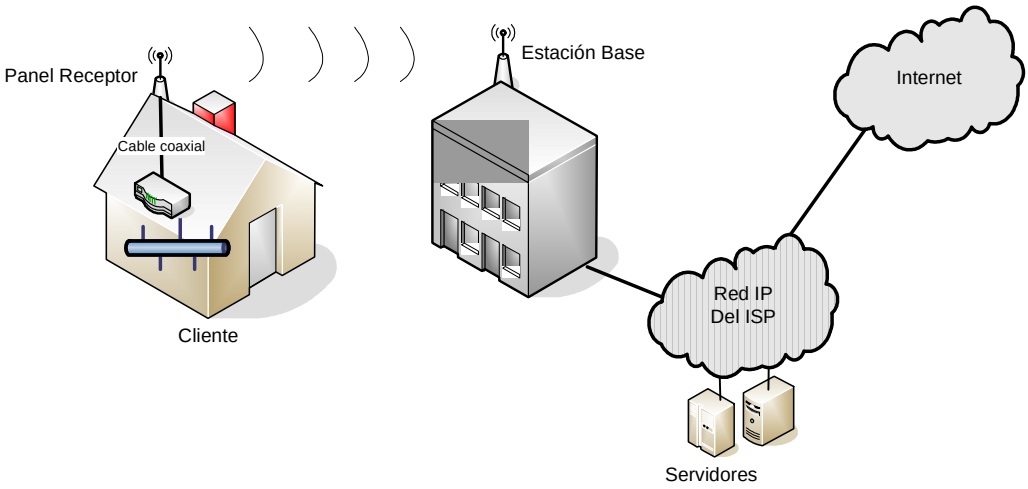

Figura 1.11. Conexión a Internet mediante LMDS.[13]

1.3.8. SIN CABLES

1.3.8.1. Wi-Fi (Wireless Fidelity)

Los estándares IEEE 802.11b para comunicaciones inalámbricas permitieron el acceso a Internet sin cableado. Al agregar radios de corto alcance para ordenadores estacionarios, los laptops, y los asistentes personales (PDA's) como Pocket PC, donde puede intercambiar información hasta en 11,000 Kbps en distancias de varios cientos de metros en interiores y hasta 16 kilómetros en exteriores.

[13] Fuente: http://lmds.donde-es.net/internet/index.htm

Los grandes negocios, ciertas universidades, aeropuertos y centros públicos como hospitales o cafeterías, inmediatamente empezaron a usar los sistemas de largo alcance del llamado sistema Wi-Fi.

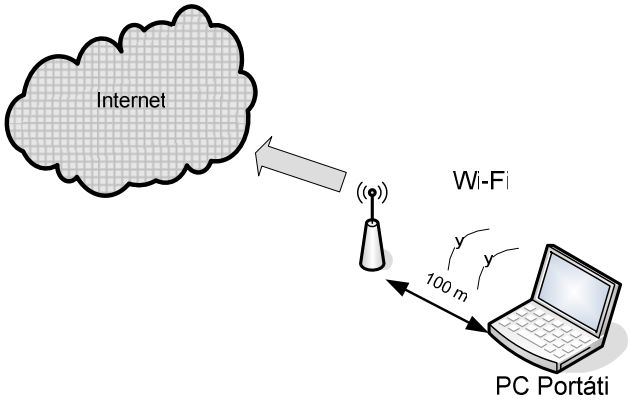

Figura 1.12. Acceso a Internet utilizando tecnología Wi-Fi.

1.3.8.2. Bluetooth

Esta es una tecnología con un rango de sólo 9 metros y una conexión más lenta de 720 a 1,000 Kbps, haciéndola adecuada para casas y pequeñas oficinas. Se puede conectar al Internet a través de teléfonos celulares y PDA's, ideal para rápidas verificaciones sobre el clima, noticias, tráfico, deportes y otras piezas digeribles de contenido del Internet.

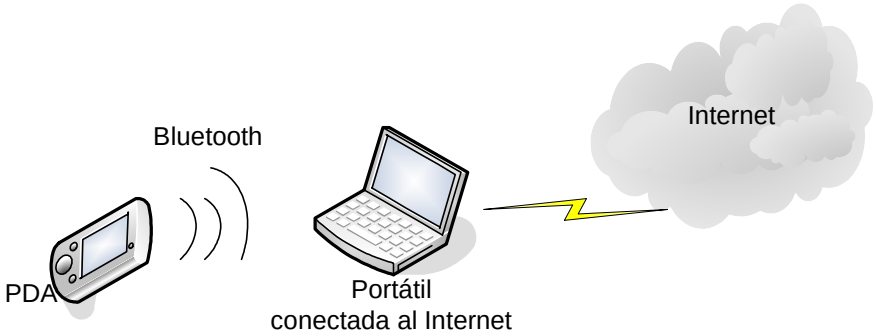

Figura 1.13. Conexión por Bluetooth.

1.3.9. OTROS SISTEMAS

- Ordenadores de automóviles.
- Agendas electrónicas (PDA's).
- Electrodomésticos como neveras y microondas.

1.4. PROVEEDORES DE SERVICIOS DE INTERNET

Un componente fundamental de la gobernanza de Internet es ejercido por la Corporación de Internet para la Asignación de Nombres y Números (ICANN - Internet Corporation for Assigned Names and Numbers). Esta organización sin fines de lucro que opera a nivel internacional, coordina la distribución mundial de nombres de dominio de primer nivel (tanto los globales *".com", ".net", ".org", ".aero"*, etc; como los nacionales *".br", ".iq", ".fr",* entre otros), a través de la gestión de los servidores raíz que permiten asociar tales dominios a direcciones IP, y de esta manera, localizar los computadores respectivos en cualquier parte de Internet. La organización coordina al mismo tiempo, la distribución mundial de las direcciones IP y la adopción de los protocolos de comunicación utilizados por la red. Este conjunto de atribuciones de la ICANN es lo que se puede llamar como "gobernanza de la infraestructura lógica" de Internet.

Aunque en un principio estos servicios los desempeñaba Internet Assigned Numbers Authority (IANA) y otras entidades bajo contrato con el gobierno de EE.UU., actualmente son responsabilidad de ICANN.[14]

El Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC), es la organización que administra el espacio de direcciones IP, Números de Sistemas Autónomos (ASN), Resolución Inversa y otros recursos para la región de América Latina y el Caribe (LAC) en nombre de la comunidad Internet.

LACNIC es una organización sin fines de lucro, basada en membresía y establecida jurídicamente en el Uruguay. [15]

En Ecuador, el Registro de Nombres de Dominio bajo el ccTLD .EC (Country Code Top Level Domain o Código de País de Dominio de Nivel Superior), es administrado por NIC.EC, por delegación de ICANN a través de IANA.

Los nombres de dominio en .EC se pueden registrar directamente bajo .EC, como dominios de segundo nivel y también pueden ser registrados dominios de tercer nivel bajo los dominios de segundo nivel predefinidos .com.ec, .info.ec, .net.ec, .fin.ec, .med.ec, .pro.ec, .org.ec, .edu.ec, .gov.ec, .mil.ec. Es posible que existan

[14] Fuente: http://www.vecam.org/article.php3?id_article=534&nemo=edm, http://www.icann.org/tr/spanish.html

[15] Fuente: http://lacnic.net/sp/sobre-lacnic/

otros dominios de segundo nivel que fueron utilizados en el pasado y que pueden estar activos, sin embargo no están disponibles para nuevos registros. [16]

Los Proveedores de Servicios de Internet (ISP) constantemente están abriendo nuevos negocios en el país, por lo tanto existen algunas alternativas para escoger.

En la búsqueda del proveedor ideal, siempre hay que ser extremadamente crítico sobre la capacidad de los distintos proveedores para cumplir con lo que ofrecen. Los individuos que buscan un proveedor de Internet en casa tal vez no necesiten un soporte técnico de 24 horas, pero necesitan asegurarse de que su proveedor tenga suficiente conocimiento para mantener el sistema funcionando y suministrar acceso consistente a la red.

Las organizaciones que buscan acceso de alta velocidad a Internet y los individuos con necesidades avanzadas casi ciertamente necesitan que le garanticen que el proveedor es altamente competente en materia técnica, y que está bien conectado al resto de Internet.

Hay muchos proveedores de Internet inferiores, incompetentes, que atrapan a consumidores que escogen un proveedor sin comparar las posibilidades de manera inteligente. Hay que protegerse a sí mismo contra esos proveedores inexpertos.

1.4.1 CRITERIOS DE SELECCIÓN DE UN ISP

Para escoger un Proveedor de Servicio de Internet (ISP) se podría considerar comprar la solución más costosa ejerciendo la teoría de que se consigue por lo que se paga. Sin embargo, una vez estudiado realmente el asunto, la elección correcta podría ser un sistema de rango medio de un abastecedor estable y reconocido a nivel nacional.

Las siguientes consideraciones ayudarán a tomar una buena decisión.

- Personal técnico eficiente, es el responsable de hacer que la conexión a Internet funcione en primer lugar, y después de mantenerla funcionando en el futuro, es uno de los aspectos más importantes a considerar.

[16] Fuente: http://www.nic.ec/nicec.htm

- Soporte de Alta Velocidad, si el cliente puede realmente conectarse a la velocidad establecida o tal vez es solo la planificada.
- El Centro de Operaciones de Red (NOC), deberá funcionar todos los días del año, 24 horas al día. Es preferible que siempre exista al menos una persona vigilando éste centro.
- Que la empresa proveedora sea una organización sólida y que tenga algún tiempo en el mercado.
- Hacer un análisis costo-beneficio de los servicios que prestan los diferentes proveedores, no confundirse con los nombres de los productos ofrecidos.
- Pedir referencias a clientes que ya tengan el servicio, averiguar por sus problemas y sus beneficios.

1.4.2. PROVEEDORES DE SERVICO DE INTERNET EN ECUADOR

Hasta septiembre del 2004 existían 120 empresas Proveedoras de Servicio de Internet, dan cobertura a las principales ciudades del país, pero algunas barreras, principalmente el aspecto económico, impiden el acceso masivo de la población a Internet.

El crecimiento de estos proveedores se muestra en la figura 1.14 [17]

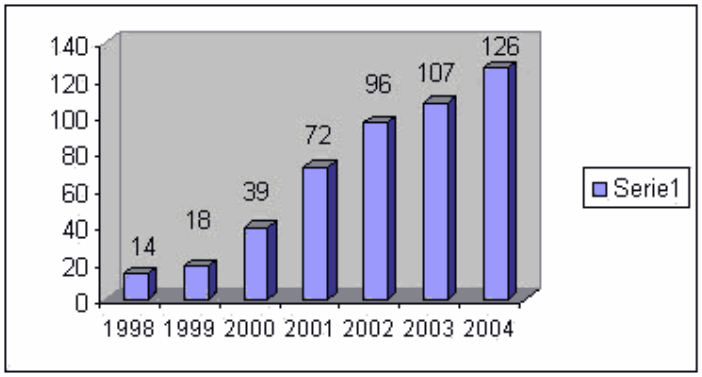

Figura 1.14. Crecimiento de los ISP en Ecuador.

[17] Fuente: Consejo Nacional de Telecomunicaciones

A continuación en la figura 1.15 se puede observar que los usuarios se encuentran concentrados en grandes cantidades en unas pocas operadoras, lo que impide un abaratamiento de los costos de acceso.

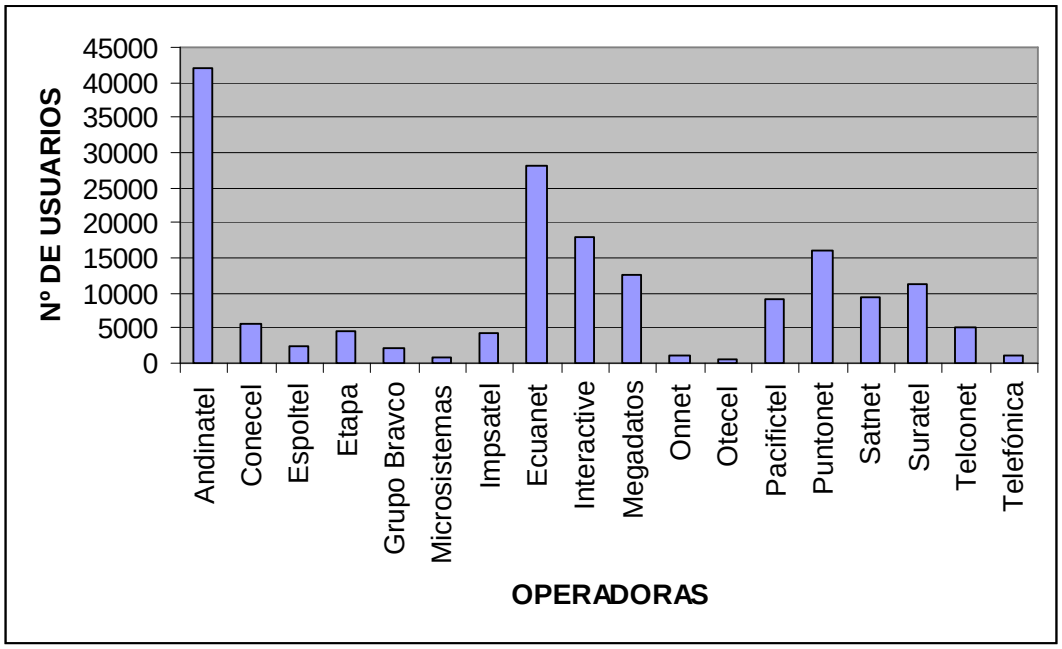

Figura 1.15. Principales operadoras vs. Número de usuarios. [18]

Dentro del sector residencial uno de los mayores inconvenientes que aquejan a los usuarios constituyen los costos de las tarifas telefónicas, imprescindible para el acceso a Internet para ciertos sectores sociales y urbano marginales. Dentro de este contexto, se ha desarrollado el proyecto de tarifación plana que busca coadyuvar en la búsqueda de la masificación de Internet. Con la adopción, implementación y ejecución de este proyecto se contribuirá de manera significativa al uso de Internet por parte de la población ecuatoriana.

[18] Fuente: Corporación ecuatoriana de Comercio Electrónico.
http://www.corpece.org.ec/guia/index.htm
http://www.proasetel.com/paginas/articulos/mercado_internet.htm

1.5. EVOLUCIÓN DE LOS ENLACES PRIVADOS

Si bien las redes LAN son muy importantes, su interconexión también ha tomado relevancia en las empresas, cuando se quiere tener todo un esquema de conexión de datos y voz entre cada sucursal u oficina remota de la empresa. Ya no es sólo tener muchas LAN, sino poderlas integrar por costos, administración, comunicación y eficiencia. Las redes WAN agrupan todas las redes de orden menor a ésta, como por ejemplo las LAN y las MAN.

El sector corporativo siempre ha requerido la implementación de enlaces privados para transportar de forma segura toda su información confidencial.

A la hora de conectar las redes, es importante también definir la forma como se ha de realizar, es decir: tecnología, protocolos a utilizar en el nivel de enlace y red, ancho de banda, entre otras variables.

Dependiendo de los dispositivos de interconexión y la tecnología utilizada, la velocidad de los enlaces puede ir desde los 9600 bps hasta el orden de los Gigabps.

Debido a que cada empresa tiene un número de usuarios y aplicaciones diferentes, se necesita una amplia gama de velocidades de enlace, de rendimiento, protocolos, opciones de flexibilidad y herramientas de gestión.

El tipo de capa física que se elija dependerá de la distancia, velocidad y del tipo de interfaz donde necesiten conectarse.

Las siguientes son las tecnologías más comunes que se han utilizado para enlazar una red a nivel WAN.

1.5.1. ENLACES SATELITALES

Es uno de los primeros sistemas de comunicación entre puntos distantes utilizados, por muchos años fue una de las soluciones más atrayentes, por su gran cobertura y fácil instalación. Esta tecnología incluye la puesta en órbita de un satélite artificial el cual sirve de puente visual entre la estación transmisora y la receptora.

Para mantener lo más fijo posible el satélite con respecto a la tierra, éste se ubica sobre una órbita geoestacionaria llamada “Cinturón de Clark”. Esta órbita está a

una altura aproximada de 36000 Km. sobre la superficie de la tierra, las comunicaciones satelitales utilizan como portadora, señales de microondas (muy pequeñas), para transmitir los datos hasta el satélite y desde éste hasta la tierra, el enlace de subida se llama “Up Link” y el de baja “Down link”.

En tierra se utiliza una estación cuyos elementos activos dependen de si se transmite datos o video, pero los elementos que no han de faltar son la antena y el alimentador o feed. Las características principales de este medio son:

- Tiene alta cobertura, con tres satélites se puede cubrir toda la superficie terrestre, esta característica lo hace ideal para zonas remotas de difícil acceso.
- Es el medio que más retardo de propagación introduce en el envío de los datos, en promedio 660 milisegundos. Cuando se tienen aplicativo sensibles al retardo, este medio se ha de descartar.
- Fácil instalación. Instalar y apuntar una estación satelital, no es una tarea complicada. Esto hace que las estaciones sirvan para transmisiones móviles de emisión masiva (broadcasting) como la televisión y la radio.
- El ancho de banda es muy costoso, lo que con lleva a analizar muy bien este factor antes de tomar una decisión por esta tecnología.

1.5.2. ENLACES MICROONDAS

Uno de los medios más utilizados por las grandes velocidades que permite, es una transmisión de radio a alta frecuencia que necesita línea de vista entre ambos puntos a enlazar. Las características más destacadas son:

- Permite llegar a grandes distancias (varios kilómetros).
- El retardo en la transmisión es bastante bajo comparado con el satelital, hasta 30 milisegundos entre ciudades.
- Requiere línea de vista, lo que lleva a colocar repetidoras en zonas muy montañosas.
- Ancho de banda más barato que el satelital.
- Más mantenimiento que el satelital. Estaciones transmisoras y repetidoras que muchas veces estén en zonas de alto riesgo.
- Velocidades de transmisión altas. El, E3, ATM.

1.5.3. LINEAS CONMUTADAS

Las líneas conmutadas, son simplemente líneas telefónicas convencionales, se dice que son conmutadas por que pasan por la red PSTN (Public service telephony network), que no es más que la red telefónica mundial basada en la conmutación de circuitos. Para poder transmitir los datos a través de este medio, es necesaria la presencia de un modem para convertir las señales digitales a análogas y ser transmitidas por la línea telefónica.

La utilización de las líneas conmutadas como medio principal de transmisión cada vez disminuye más, su principal función está orientada a servir de backup en canales de muy baja demanda de tráfico. Se utiliza bastante en los accesos conmutados a ISP (proveedores de servicios de Internet) desde cada hogar. Las características de la línea conmutada son:

- Amplia cobertura, sólo se necesita una línea de abonado de una central pública y de inmediato se tiene conectividad a cualquier sitio del mundo.
- Baja velocidad, al ser la línea telefónica un medio tan expuesto a las interferencias, la velocidad de transmisión baja hasta valores muchas veces inaceptables. Aunque la norma V.90 sugiere velocidades de hasta 56 kbps, con suerte se tendrán acceso de 33.6 kbps, pero en su mayoría de 14,4 kbps. Estos valores aunque pueden ser aceptables para un acceso a Internet, lo más posible es que no lo sea para una conexión WAN entre dos redes.
- Fácil de instalar, sólo se necesita un modem, una línea y algo de conocimientos para colocar en operación una conexión de este estilo.

1.5.4. LINEA ARRENDADA

También llamada línea dedicada o par aislado, está conformada por uno o dos pares de cobre entre dos puntos no muy distantes, provista por la compañía de teléfonos, y tener los equipos terminales. Los equipos terminales, pueden ser modems de corta distancia (hawlk), DTU/NTU, o equipos banda base para transmisiones HDSL. Con cualquiera de estos equipos se pueden llegar a

distancias de hasta 4kilómetros, muchas veces limitada por la velocidad de transmisión.

1.5.5. LÍNEA RDSI

Bien llamada “Red Digital de Servicios Integrados” o ISDN en su nombre original en inglés. Es una línea telefónica digital capaz de transportar datos, video y control simultáneamente. Esta dividida en tres interfaces U, S y R.

Interfaz U: Comprende desde la central telefónica hasta el usuario. Esta interfaz es un paso intermedio necesario para poder llegar hasta el abonado con un sólo par de cobre y no con dos como necesita la RDSI. Posee una alimentación de aproximadamente 90 VDC. Este par de cobre debe pasar pruebas muy exigentes de impedancia, capacitancia, resistencia e inductancia, para poder trabajar con una línea RDSI. Esta parte trabaja con el protocolo 2B1Q.

Interfaz STí: Es la RDSI es su formato original, formada por cuatro hilos, dos de recepción y dos de transmisión. A esta interfaz también se fe denomina RDSI nativa. Para convertir de la interfaz U a la interfaz S, se utiliza un equipo llamado NT o equipo terminal de red, la RDSI en interfaz S, puede ser recibida por cualquier equipo como multiplexor, PBX, router, que tenga puerto de RDSI nativo.

Interfaz R: Necesaria para extraer de la RDSI la información que se transmite, ya sea datos o voz. Por un lado recibe la interfaz S y por otro entrega datos en conectores V.24 (DB25) o V.35 (Winchester).

Existen dos tipos de RDSI, cuya diferencia más importante, es la cantidad de canales que pueden transportar.

1.5.6. FIBRA ÓPTICA

Es el medio más prometedor en los años venideros, su principal ventaja es el poder transmitir grandes cantidades de datos a distancias lejanas con pérdidas insignificantes. Su costo es más alto, que el de los demás medios, pero continua bajando a medida que su implementación crece. Los carriers, utilizan este medio para formar el backbone o núcleo de la red WAN de todo un país.

Sea cual sea el medio que se utilice en los casos anteriores, es importante definir que protocolo de nivel de enlace se utilizará para transportar los datos por el medio. Si los equipos de transporte son multiplexores, es posible decidirse por canales basados en la multiplexación por división de tiempo TDM o Canales Frame Relay.

1.5.7. CANALES TDM CLEAR CHANNEL

Son canales que no utilizan ninguno de los protocolos de nivel 2 estándar como PPP, Frame Relay, HDLC, entre otros. Por esta circunstancia, es un canal transparente (clear channel) que puede transportar cualquier protocolo, como los mencionados. TDM tiene una característica que puede ser ventajosa o desventajosa, dependiendo de cómo se analice, es la velocidad de acceso. Para canales TDM, sin importar si utiliza o no el ancho de banda, él esta ahí y se debe pagar por él. Por ejemplo si una empresa adquiere un canal de datos de 128 kbps y sólo utiliza 64 kbps en promedio, debe pagar por todos los 128 kbps, ya que estos están disponibles reservados todo el tiempo. Esta característica es ventajosa si se necesita que el BW esté disponible para cuando se requiera transmitir un burst de tráfico alto, como puede ser durante un cierre de mes. Pero puede resultar ser un desperdicio de dinero en muchos casos.

1.5.8. CANALES FRAME RELAY

Frame Relay es una tecnología de conmutación de tramas, donde el ancho de banda se maneja por sobre venta, jugando a la probabilidad que cuando unos no requieran BW lo liberen para ser utilizados por otros. En esta tecnología se paga por lo que se consume, lo que lleva a economías significantes cuando se compara con TDM. Otra ventaja importante de Frame Relay, es que permite conexiones de múltiple acceso sobre un solo nivel físico, esto es posible con la configuración de PVC (circuitos permanentes virtuales), que permiten tener hasta más de mil canales terminados en un solo puerto físico. Este factor permite tener un solo enlace de última milla, por ejemplo un radio, para múltiples ciudades, en vez de múltiples radio enlaces, uno para cada ciudad.

1.6. TIPOS DE ENLACES

Más específicamente, a los enlaces privados WAN se los puede clasificar como:

- Enlaces conmutados.
- Enlaces dedicados

1.6.1. ENLACES CONMUTADOS

Los enlaces conmutados son aquellos en los que se debe establecer la conexión para luego realizar la transferencia de información y finalmente terminar la conexión. El enlace es utilizado de forma parcial a requerimiento, o se puede decir también que mantienen una conexión permanente temporal.
Los enlaces conmutados se pueden dividir en dos tipos como se describe a continuación.

1.6.1.1. Enlace Conmutado por Circuito

En un enlace conmutado por circuito, se establece un enlace a nivel físico, es una conexión directa entre el origen y el destino. Se establece un circuito físico que proporciona un ancho de banda exclusivo.
Un ejemplo de enlace conmutado por circuito, es el servicio telefónico convencional donde se establece un circuito entre el origen y el destino.

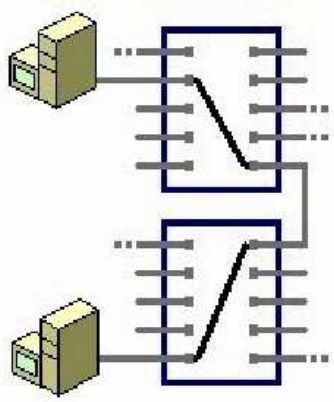

Figura 1.16. Enlace conmutado por circuito.[19]

[19] Fuente: http://descom.jmc.utfsm.cl/jderks/apoyo/apunte6.pdf#search='enlaces%20conmutados'

1.6.1.2. Enlace Conmutado por Paquete/Celda

En un enlace conmutado por paquetes o celdas se establece un circuito virtual donde se marcan los paquetes o celdas para identificarlas en los enlaces.
Por lo general los circuitos conmutados por paquetes/celdas son circuitos por los que circulan tráficos de diferentes enlaces, de ahí la importancia de marcar los paquetes para que puedan ser identificados.

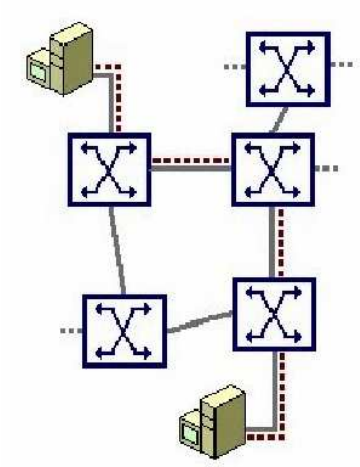

Figura 1.17. Enlace conmutado por paquete/celda.[20]

Dentro de esta categoría de enlaces, los más utilizados en conectividad WAN son ATM y Frame Relay.

1.6.1.2.1. Frame Relay

Frame Relay permite comunicaciones de datos por conmutación de paquetes a través de la interface entre dispositivos de usuario y equipos de red, a esta interfaz se le denomina FRI (Frame Relay Interface).
La red que soporta el FRI puede ser una red pública/privada por portadora o una red de equipos de propiedad del usuario sirviendo a la empresa.
Generalmente se hace uso de una operadora que disponga de dicho servicio por cuestiones prácticas.
El término “Relay” implica que la trama de datos de la capa 2 es conmutada en los nodos y/o procesada en los puntos extremos de cada enlace de red.

[20] Fuente: http://descom.jmc.utfsm.cl/jderks/apoyo/apunte6.pdf#search='enlaces%20conmutados'

En nuestros días en los que los enlaces son más seguros y las redes más fiables, el chequeo de errores no es necesario.

Frame Relay acelera el proceso de routing de paquetes a través de una serie de switches a una localización remota eliminando la necesidad de que cada switch verifique cada paquete que recibe antes de retransmitirlo al siguiente switch.

Sobre enlaces como estos, los protocolos de nivel de enlace pueden evitar el consumo de tiempo de los algoritmos de corrección de errores durante el tránsito, dejando que estas tareas sean desarrolladas por las capas altas. Una mayor eficiencia y mejores prestaciones son posibles sin sacrificar la integridad de los datos, y para ello fue diseñada. Incluye un algoritmo de chequeo de redundancia cíclico (CRC) para detectar bits deteriorados (con ello, los datos pueden ser descartados), pero no incluye ningún mecanismo de protocolo para corregir datos erróneos.

Frame Relay dispone de técnicas explícitas para el control de flujo, existentes en modo circuito virtual. Ya que muchos protocolos de capas superiores están ejecutando sus propios algoritmos de control de flujo, la necesidad de esta funcionalidad en la capa de enlace ha disminuido.

Frame Relay no incluye procedimientos de control de flujo explícitos que dupliquen los de las capas altas. En su lugar, mecanismos de notificación de congestión muy simples se soportan para permitir a una red informar a un dispositivo de usuario de que los recursos de la red están agotados cuando se alcanza un estado congestionado. Esta notificación puede alertar a los protocolos de las capas altas donde el control de flujo puede ser necesario.

Con todo esto se destaca que el chequeo de errores y control de flujo solamente son realizados en la estación destino, no en los nodos intermedios.

Algunas definiciones importantes de Frame Relay son:

Bc (Busrt comprometido): Es la ráfaga de bits que el switch Frame Relay se compromete a enviar en un PVC. La unidad se da en bits.

Tc (Tiempo comprometido): Es el tiempo en el que el switch se compromete a transmitir el Bc. La unidad se da en segundos o milisegundos.

CIR (Rata de información comprometida): Es la rata a la cual se compromete el switch para enviar los datos. Es la relación entre el Bc y el Tc. CIR=Bc/Tc. Se expresa en bits/segundo.

1.6.1.2.1.1. Dispositivos Frame Relay

Los dispositivos Frame Relay caen dentro de dos categorías generales:

- Data terminal equipment (DTE)
- Data circuit-terminating equipment (DCE)

Los DTEs generalmente son considerados para ser equipos de terminación de una red específica, ejemplos de dispositivos DTE son terminales, computadores personales, routers y bridges.

Los DCEs son dispositivos de internetworking del carrier, el propósito de un DCE es de proveer servicios de switching y reloj en una red, en la cual están los dispositivos que transmiten datos a través de la WAN, en la mayoría de los casos esos son switch de paquetes.

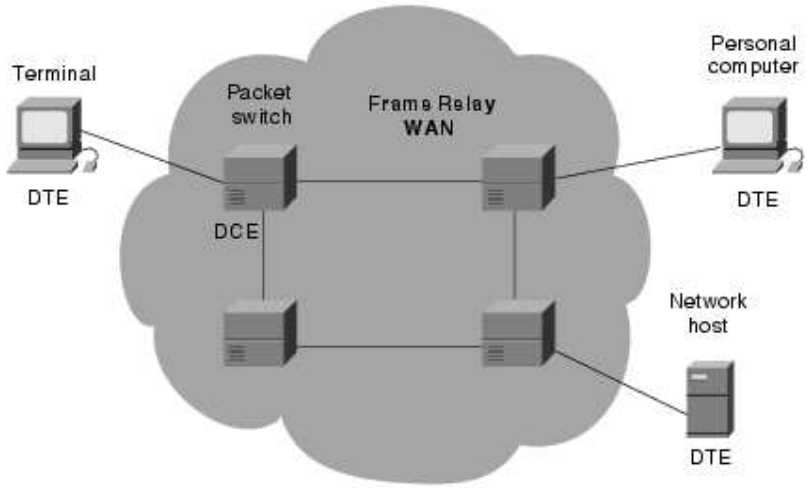

Figura 1.18. Dispositivos Frame Relay.[21]

La conexión entre un dispositivo DTE y un dispositivo DCE consiste de un componente de capa física y un componente de capa de enlace.

El componente físico define las especificaciones mecánica, eléctrica y funcional para la conexión entre los dispositivos. Una de las interfaces de capa física mas utilizadas es la especificación RS-232.

El componente de capa enlace define el protocolo que establece la conexión entre el DTE y el DCE.

[21] Fuente: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm

1.6.1.2.1.2. Extensión LMI

Además de las funciones del protocolo básico de Frame Relay para la transferencia de datos, la especificación del consorcio Frame Relay incluye las extensiones LMI (Link Management Interface) que permiten gestionar internetworks complejas más fácilmente. Algunas extensiones LMI se conocen como “comunes” y se supone que serán implementadas por todos los que adopten la especificación. Otras funciones LMI se conocen como “opcionales”.
Un sumario de las extensiones LMI son las siguientes:

- Mensajes de estado de circuito virtual (común). Proveen la comunicación y sincronización entre la red y el dispositivo del usuario. Periódicamente informan de la existencia de nuevos PVCs y el borrado de PVCs ya inexistentes y generalmente proveen información acerca de la integridad de los PVCs, los mensajes de estado de los circuitos virtuales previenen el envío de datos sobre “agujeros negros”, esto es, sobre PVCs que no existen.
- Multicasting (opcional). Permite a un transmisor, enviar una simple trama pero que sea entregada por la red a múltiples destinos. Así, multicasting requiere de mensajes de routing eficientes y procedimientos de resolución de direcciones que típicamente deben ser enviados para muchos destinos simultáneamente.
- Direccionamiento Global (opcional). Dar identificadores globales de conexión mejor que con significado local, permite que estos sean utilizados para identificar una interface especifica en toda la red Frame Relay. Las direcciones globales hacen que la red Frame Relay se comporte como una red de área local (LAN) en términos de direcciones; los protocolos de resolución de direcciones además operan sobre Frame Relay exactamente como lo harían sobre una LAN.
- Simple Control de Flujo (opcional). Provee un mecanismo de control de flujo XON/XOFF que aplican a la interfaz Frame Relay. Se hace así, ya que las capas altas no usan bits de notificación de congestión y eso necesita de algún nivel de control de flujo.

1.6.1.2.1.3. Formato de Trama

El formato de trama Frame Relay se muestra en la figura 1.19 donde constan 5 campos.

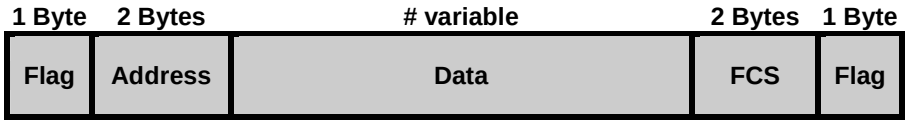

Figura 1.19. Formato de trama Frame Relay.[22]

Flags: (1 byte) delimita el comienzo y el final de la trama. Su valor es el mismo que en las tramas LAP-B / HDLC, o sea 01111110.

Address: contiene la siguiente información:

- DLCI (Data Link Connection Identifier), es la esencia de la cabecera Frame Relay.
- Extended Address (EA), campo de extensión de dirección
- C/R (Comando/Respuesta), generalmente no declarado y no es un bit utilizado por la red.
- Control de Congestión, consiste de 3 bits: FECN, BECN y DE.

Data: contiene los datos encapsulados

Frame Check Sequence: asegura la integridad de los datos transmitidos.

1.6.1.2.1.4. Data Link Connection Identifier

El valor de 10 bits de DLCI del campo dirección (Address), es el corazón de la cabecera Frame Relay y los valores van desde 16 hasta 1023. Identifica la conexión lógica que está multiplexada en el canal físico. En el modo de direccionamiento básico (que es, no extendido por el LMI), los DLCI tienen significado local.

Con el DLCI se identifica el canal lógico al que pertenece cada trama, los números de canal lógico se asignan por contratación.

[22] Fuente: http://www.ucsd.edu.do/v3/craie/documentos/Tutoriqal%20informatica%20FrameRelay.pdf

A continuación se muestra un ejemplo del uso de DLCI's en el modo de direccionamiento Frame Relay no extendido.

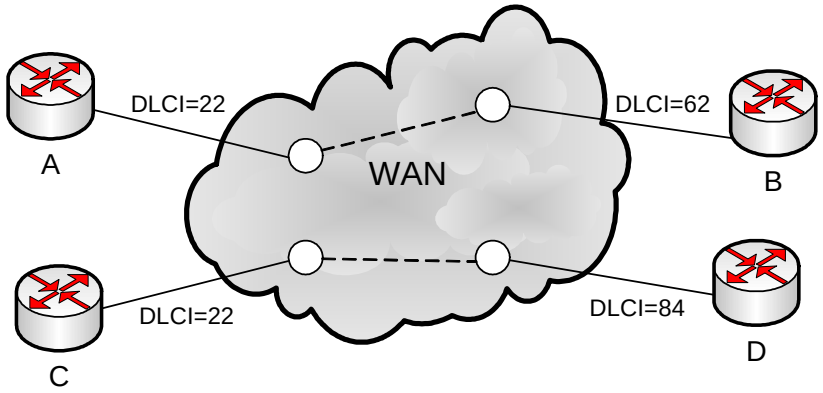

Figura 1.20. Asignación local de DLCI.[23]

En la figura 1.20 se indica que hay dos circuitos virtuales permanentes uno entre los puntos A y B, y otro entre los puntos C y D. El punto C utiliza el DLCI 22 para referirse a su PVC con el punto D, mientras D se refiere al mismo PVC con el DLCI 84.

Similarmente, A utiliza el DLCI 22 para referirse a su PVC con B. La red utiliza mecanismos internos propietarios para guardar los identificadores de ambos DLCI con significado local.

Como se comentó anteriormente, los DLCI permiten la multiplexación de varias conexiones lógicas de retransmisión de tramas a través de un único canal, el DLCI tiene significado local; cada extremo de la conexión lógica asigna su propio DLCI de acuerdo con los números libres, debiendo realizar la red, la conversión correspondiente entre ellos. Alternativamente, el uso del mismo DLCI por parte de ambos extremos requeriría algún tipo de gestión global de los valores de DLCI.

[23] Fuente: http://www.ucsd.edu.do/v3/craie/documentos/Tutoriqal%20informatica%20FrameRelay.pdf

1.6.1.2.1.5. Formatos de Mensajes LMI

Implementan funciones adicionales en la UNI (User-Network Interface), transfiere mensajes de red notificando al usuario de la presencia de un DLCI activo, o el borrado o fallo de un DLCI y provee una monitorización de estado en tiempo real del enlace físico y lógico entre la red y cada dispositivo del usuario.

El protocolo LMI consiste en el intercambio de mensajes entre el usuario y el nodo de acceso local a la red. Está basado en un esquema de "polling", el equipo del usuario (router) pide a la red información de estado para los PVCs sobre una determinada interfaz UNI. El dispositivo del usuario usa un mensaje de petición de estado y la red responde con un mensaje de estado.

Los mensajes LMI son enviados en tramas que se distinguen por un DLCI específico para LMI (definido en la especificación del consorcio como DLCI=1023). El formato del mensaje LMI se muestra en la figura 1.21.

Incluye algunas de las funciones CLLM (Consolidated Link Layer Management) para notificar información de control de congestión, en aquellos casos en que no hay tramas en sentido contrario al congestionado. Para ello utiliza las tramas XID (eXchange Identification) (equivalente a las utilizadas en HDLC) para informar de problemas en la red. Si no se utiliza Frame Relay sobre RDSI se utiliza un DLCI determinado. Independientemente de cual sea la longitud de DLCI, CLLM utiliza el DLCI que tenga todo el campo DLCI a 1.

Bytes	1	2	1	1	1	1	variable	2	1
	Flag	LMI DLCI	UI	Discriminad. Protocolo	Call Reference	Tipo de Mensaje	Elementos Informac.	FCS	Flag

Figura 1.21. Formato de trama LMI.[24]

En mensajes LMI, el cabecero de protocolo básico es el mismo que en tramas de datos normales. El mensaje actual LMI comienza con 4 bytes indispensables, seguidos de un número variable de elementos de información (IE). El formato y la codificación de los mensajes LMI esta basado sobre el estándar ANSI T1S1.

[24] Fuente: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm

1.6.1.2.1.6. Direccionamiento Global

Además de las características comunes LMI, hay varias extensiones opcionales LMI que son extremadamente útiles en un entorno de interconexión. La primera extensión opcional en importancia es el direccionamiento global. En este caso no hay direcciones que identifiquen interfaces de red, o nodos conectados a estas interfaces. Ya que estas direcciones no existen, ellas no pueden ser descubiertas por resolución tradicional de direcciones y técnicas de descubrimiento. Esto significa que con el direccionamiento normal Frame Relay, mapas estáticos deben ser creados para decirle a los routers que DLCI utilizar para encontrar un dispositivo remoto y su dirección internetwork asociada.

La extensión de direccionamiento global permite identificación de nodos, con esta extensión, los valores insertados en el campo DLCI de una trama son direcciones con significado global de dispositivos extremo de usuario individuales (por ejemplo routers).

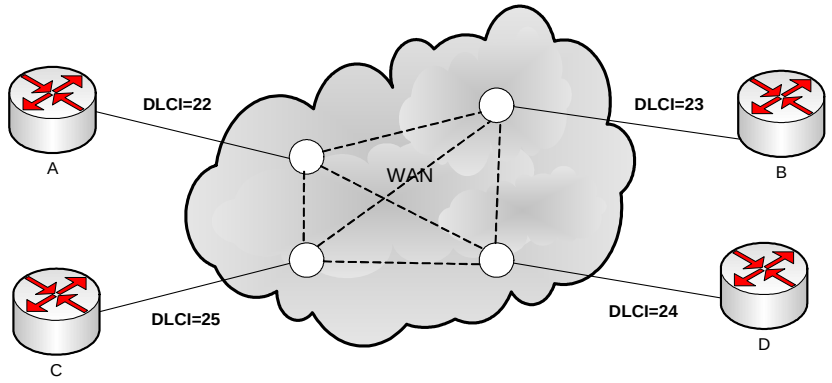

Figura 1.22. Intercambio de direccionamiento Global.[25]

Nótese que en la figura 1.22 cada interfaz tiene su propio identificador, suponiendo que el router B debe enviar una trama al router A. El identificador para A es 22, así que B coloca el valor 22 en el campo DLCI y envía la trama en la red Frame Relay. En el punto final, el contenido del campo DLCI es cambiado a 23 para reflejar el nodo fuente de la trama. Cada interfaz del router tiene un valor

[25] Fuente: http://www.ucsd.edu.do/v3/craie/documentos/Tutoriqal%20informatica%20FrameRelay.pdf

distinto como su identificador de nodo, así los dispositivos pueden ser distinguidos individualmente, esto permite un routing adaptativo en entornos complejos.
El direccionamiento global provee significativos beneficios en grandes y complejas internetworks. La red Frame Relay aparece para los routers como cualquier LAN, ningún cambio en los protocolos de capas altas se necesita para incorporar estas facilidades.

1.6.1.2.1.7. Multicasting

Multicasting es otra característica opcional destacable de LMI, los grupos multicast están designados por una serie de 4 valores reservados de DLCIs (de 1019 a 1022). Las tramas enviadas por un dispositivo usando uno de estos DLCI reservados son replicadas por la red y enviadas a todos los puntos extremos en el conjunto designado. La extensión multicast también define mensajes LMI que notifican a los dispositivos de los usuarios la adición, borrado y presencia de grupos multicast.
En redes que toman ventajas por el routing dinámico, la información de routing debe ser intercambiada a través de muchos routers. Los mensajes de routing pueden ser enviados eficientemente usando tramas con una DLCI multicast. Estos mensajes permiten ser enviados a grupos específicos de routers.

1.6.1.2.2. ATM

Asynchronous Transfer Mode (Modo de Transferencia Asíncrono) es una tecnología de switching basada en unidades de datos de un tamaño fijo de 53 bytes llamadas celdas. ATM opera en modo orientado a la conexión, esto significa que cuando dos nodos desean transferir deben primero establecer un canal o conexión por medio de un protocolo de llamada o señalización. Una vez establecida la conexión, las celdas de ATM incluyen información que permite identificar la conexión a la cual pertenecen.
En una red ATM las comunicaciones se establecen a través de un conjunto de dispositivos intermedios llamados switches.

1.6.1.2.2.1. Redes ATM

El componente básico de una red ATM es un switch electrónico especialmente diseñado para transmitir datos a muy alta velocidad, un switch típico soporta la conexión de entre 16 y 32 nodos. Para permitir la comunicación de datos a alta velocidad la conexión entre los nodos y el switch, se realizan por medio de un par de hilos de fibra óptica.

Aunque un switch ATM tiene una capacidad limitada, múltiples switches pueden interconectarse ente si para formar una gran red. En particular, para conectar nodos que se encuentran en dos sitios diferentes es necesario contar con un switch en cada uno de ellos y ambos a su vez deben estar conectados entre si.

Las conexiones entre nodos ATM se realizan en base a dos interfaces diferentes. La User to Network Interfaces o UNI, se emplea para vincular a un nodo final con un switch.

La Network to Network Interfaces o NNI, define la comunicación entre dos switches.

Los diseñadores piensan en UNI como la interfaces para conectar equipos del cliente a la red del proveedor y a NNI como una interfaces para conectar redes de diferentes proveedores.

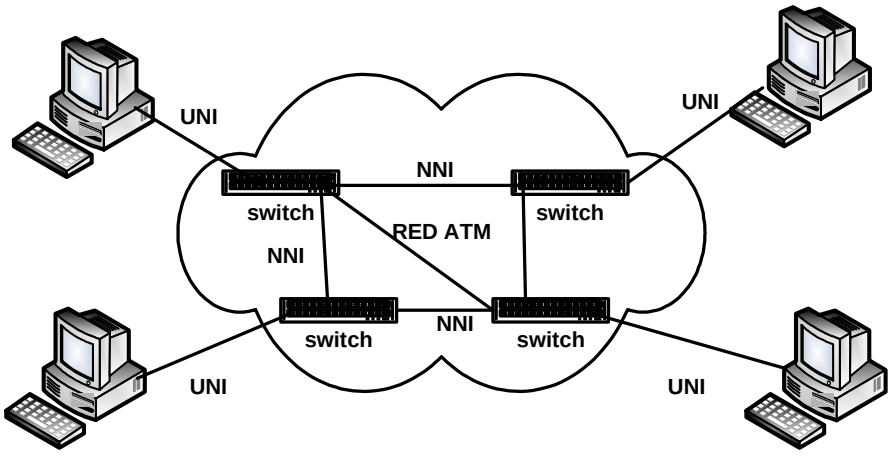

Figura 1.23. Red ATM.

1.6.1.2.2.2. Tipos de conexiones

ATM provee servicios orientados a la conexión, para comunicarse con un nodo remoto, un host debe solicitar a su switch local el establecimiento de una conexión con el destino. Estas conexiones pueden ser de dos naturalezas: Switched Virtual Circuits (SVC) o Permanent Virtual Circuits (PVC).

- **Switched Virtual Circuits**

Un SVC opera del mismo modo que una llamada telefónica convencional, un host se comunica con el switch ATM local y requiere del mismo el establecimiento de un SVC. El host especifica la dirección completa del nodo destino y la calidad del servicio requerido, luego espera que la red ATM establezca el circuito.

El sistema de señalización de ATM se encarga de encontrar el path necesario desde el host origen al host destino a lo largo de varios switches. El host remoto debe aceptar el establecimiento de la conexión.

Durante el proceso de señalización cada uno de los switches examina el tipo de servicio solicitado por el host de origen. Si acuerda propagar información de dicho host registra información acerca el circuito solicitado y propaga el requerimiento al siguiente switch de la red.

Este tipo de acuerdo reserva determinados recursos el switch para ser usados por el nuevo circuito, cuando el proceso de señalización concluye el switch local reporta la existencia del SVC al host local y al host remoto.

La interfaz UNI identifica a cada uno de los SVC por medio de un número de 24 bits. Cuando un host acepta un nuevo SVC, el switch ATM local asigna al mismo un nuevo identificador. Los paquetes transmitidos por la red no llevan información de nodo origen ni nodo destino. El host marca a cada paquete enviado con el identificador de circuito virtual necesario para llegar al nodo destino.

- **Permanent Virtual Circuits**

La alternativa al mecanismo de SVC descrito en el ítem anterior, el administrador de la red puede configurar en forma manual los switches para definir circuitos permanentes. El administrador identifica el nodo origen, el nodo destino, la calidad de servicio y los identificadores de 24 bits para que cada host pueda acceder al circuito.

1.6.1.2.2.3. Paths, Circuitos e Identificadores

ATM asigna un entero único como identificador para cada path abierto por un host, este identificador contiene menor información de la que fue necesaria para la creación del circuito. Además el identificador solo es válido mientras que el circuito permanece abierto.

El identificador es válido para un solo sentido del circuito, esto quiere decir que los identificadores de circuito obtenidos por los dos hosts en los extremos del mismo usualmente son diferentes. Los identificadores usados por la interfase UNI están formados por 24 bits, divididos en dos campos, el primero de 8 bits y el segundo de 16 bits. Los primeros 8 bits forman el llamado “Virtual Path Identifier” y los 16 restantes el “Virtual Circuit Identifier”. Este conjunto de bits suele recibir el nombre de “VPI/VCI pair”.

Esta división del identificador en dos campos persigue el mismo fin que la división de las direcciones IP en un campo para identificar la red y un segundo campo para identificar el host. Si un conjunto de VCs sigue el mismo path el administrador puede asignar a todos ellos un mismo VPI. El hardware de ATM usa entonces los VPI para funciones de ruteo de tráfico.

1.6.1.2.2.4. Transporte de celdas ATM

En cuanto al transporte de información, ATM usa tramas de tamaño fijo que reciben el nombre de celdas. El hecho de que todas las celdas sean del mismo tamaño permite construir equipos de switching de muy alta velocidad. Cada celda de ATM tiene una longitud de 53 bytes, reservándose los 5 primeros para el encabezado y el resto para datos.

Figura 1.24. Formato de celda ATM.

Dentro del encabezado se coloca el par VPI/VCI que identifica al circuito entre extremos, información de control de flujo y un CRC.
La conexión final entre dos nodos recibe el nombre de Virtual Channel Connection o VCC, una VCC se encuentra formada por un conjunto de pares VPI/VCI.

1.6.1.2.2.5. Modelo de capas de ATM

El modelo de referencia propuesto por el CCITT está constituido por tres niveles: Nivel Físico, Nivel ATM y Nivel de Adaptación ATM (AAL).

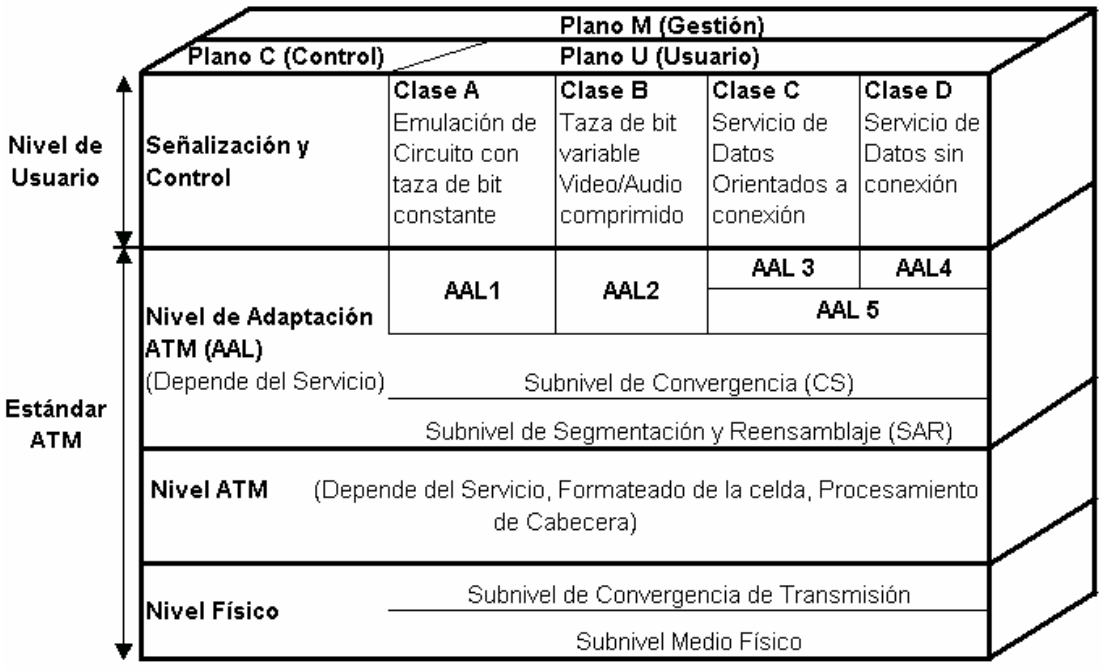

Figura 1.25. Modelo de Referencia ATM.

- **Capa Física**

Define la forma en que las celdas se transportan por la red, es independiente de los medios físicos y tiene dos subcapas

  - TC (Transmission Convergence Sublayer).
  - PM (Physical Medium Sublayer).

- **Capa ATM**

Provee un solo mecanismo de transporte para múltiples opciones de servicio, es independiente del tipo de información que es transmitida (datos, gráficos, voz. audio, video) con excepción del tipo de servicio (QOS) requerido.

Existen dos tipos de header ATM: UNI (User-Network Interface) y NNI (Network-Network Interface).

- **Nivel de Adaptación ATM**

Provee las funciones orientadas al usuario no comprendidas en la Capa ATM, permite a la Capa ATM transportar diferentes protocolos y servicios de capas superiores. Tiene dos subcapas:

  - CS (Convergence Sublayer).
  - SAR (Segmentation and Reassembly Sublayer).

Si bien ATM se maneja con celdas a nivel de capas inferiores, las aplicaciones que generan la información a ser transportada por ATM no trabajan con celdas. Estas aplicaciones interactuarán con ATM por medio de una capa llamada “ATM Adaptation Layer”. Esta capa realiza una serie de funciones entre las que se incluyen detección de errores (celdas corruptas).

En el momento de establecer la conexión el host debe especificar el protocolo de capa de adaptación que va a usar. Ambos extremos de la conexión deben acordar en el uso del mismo protocolo y este no puede ser modificado durante la vida de la conexión.

Hasta el momento solo se han definido dos protocolos de capa de adaptación para ser usados por ATM. Uno de ellos se encuentra orientado a la transmisión de información de audio y video y el otro para la transmisión de datos tradicionales.

ATM Adaptation Layer 1 (AAL1) transmite información a una tasa de bits fija, las conexiones creadas para trabajar con video deben usar ALL1 dado que requieren un servicio de tasa constante para no tener errores de parpadeo en la imagen.

La transmisión de datos tradicionales trabaja con la AAL5 para enviar paquetes de un nodo a otro. Ahora, si bien ATM trabaja con tramas o celdas de tamaño fijo. Los protocolos de capa superior generalmente manejan datagramas de longitud variable, una de las funciones de la AAL5 consiste en adaptar estas tramas a celdas, en particular la AAL5 puede recibir datagramas de hasta 64 k de longitud.

El paquete manejado por la AAL5 difiere estructuralmente de otros tipos de tramas existentes ya que la información de control se inserta al final de la misma, su longitud es de 8 bytes.

Cada una de las tramas de AAL5 debe ser fraccionada en celdas para poder ser transportadas por la red, para luego ser recombinadas en el nodo remoto. Cuando el datagrama es un múltiplo de 48 bytes el resultado de la división da un número entero de celdas, en caso contrario la última de las celdas no se encontrará completa.

Para poder manejar paquetes de longitud arbitraria, AAL5 permite que la celda final pueda contener entre 0 y 40 bytes de datos y coloca la información de control al final de la misma antecedida por los ceros de relleno necesarios. En otras palabras, la información de control se coloca al final de la secuencia de celdas donde puede ser encontrada y extraída sin necesidad de conocer la longitud del datagrama fraccionado.

1.6.2. ENLACES DEDICADOS

Si una empresa desea mantener servicios on-line, la opción correcta es el enlace dedicado, con esta conexión los usuarios pueden acceder a redes distantes a través de su equipo terminal.

Proporcionan conexión a tiempo completo y la calidad es a menudo superior a la calidad de la línea telefónica, su velocidad va desde los 56 Kbps hasta por encima de los 45 Mbps.

En los enlaces dedicados el más común es el servicio Clear Channel (canal limpio) permite ofrecer canales con velocidades desde nx64 hasta nxE1, este servicio es ideal para aquellas empresas que necesitan disponibilidad total del ancho de banda y requieren el máximo de seguridad, esta tecnología usa la misma velocidad tanto de subida como de bajada de información.

Los principales usos son: empresas con canales dedicados (matriz - sucursal), CafeNets (navegación, cabinas de comunicación, chat, etc.).

1.6.2.1. Clear Channel TDM

Son canales que no utilizan ninguno de los protocolos de nivel 2 estándar como PPP, Frame Relay, HDLC, entre otros. Por esta circunstancia, es un canal transparente (clear channel) que puede transportar cualquier protocolo, como los mencionados.

En un Clear Channel basado en tecnología TDM (Time División Multiplexing) se tiene la combinación de 30 canales de transmisión de 64 Kbps que pueden transmitirse en un solo canal transparente de 2Mbps o E1 en el cual, cada canal de 64 Kbps ocupa un "time slot" asignado a un canal de transmisión de datos.

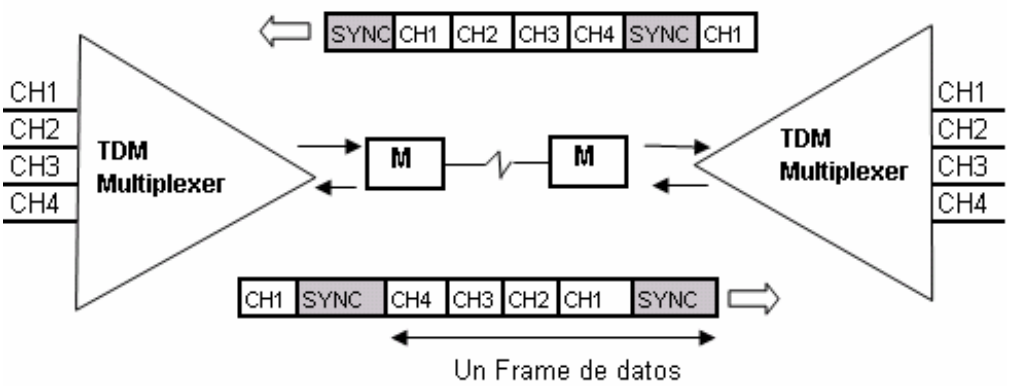

Figura 1.26. Ubicación de Time Slots en Clear Channel.[26]

En los sistemas Clear Channel existen 3 modos de sincronización:

- El primer modo de sincronización provee relojes de transmisión y recepción para el equipo de usuario, conectado al puerto de datos del multiplexer TDM (MUX).
- En el segundo modo de sincronización, el canal de datos envía y recibe información acompañado por el reloj recibido, derivado del reloj del sistema central para el equipo de usuario conectado al MUX TDM, y acepta datos de usuario de acuerdo al reloj del equipo transmisor de usuario.

[26] Fuente: www.internetghana.com/wan.htm

- En el tercer modo de sincronización el canal de datos transmite y recibe datos acorde a la señal de reloj provista por el equipo conectado en el puerto de datos del MUX. Cuando se usa modo de cronómetro, el principal enlace cronometrado debería ser bloqueado para la señal de reloj provista por la interface del puerto de datos de usuario.

Estas múltiples fuentes de selección de reloj aseguran máxima flexibilidad, tanto para el enlace principal como para el puerto de datos.

1.6.2.1.1. Redes Clear Channel Típicas

Dependiendo de las necesidades del cliente la conexión de circuitos privados dedicados permiten establecer de manera permanente la comunicación entre dos sitios, tres o más.

1.6.2.1.1.1. Sucursal Oficina Central

En la figura 1.27, un canal de datos sincrónico nx64 Kbps originado desde la oficina remota (sucursal) en el puerto de datos uno (CH1) es mapeado sobre n timeslots del enlace principal E1. El canal de datos nx64 Kbps está ruteado a través de la red E1 hacia la oficina central, terminando en un puerto de datos en el correspondiente TDM MUX.

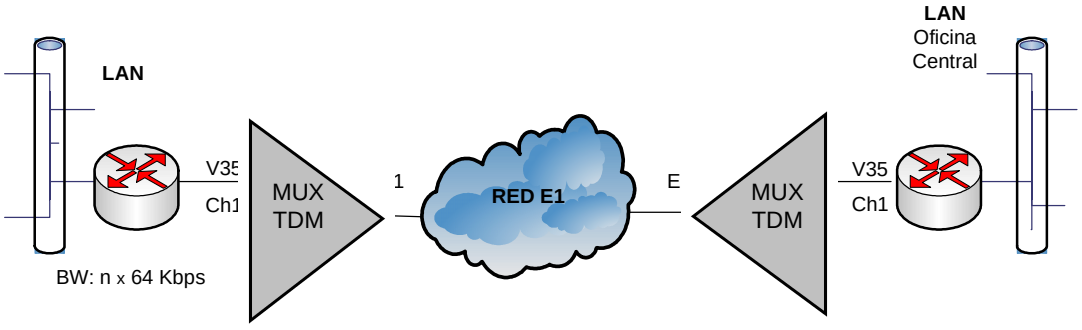

Figura 1.27. Clear Channel Sucursal - Oficina Central.[27]

[27] Fuente: www.internetghana.com/wan.htm

1.6.2.1.1.2. Multiples Agencias hacia la Oficina central

Este tipo de conectividad Clear Channel es utilizada para conectar más de una agencia con la oficina central.

Los canales de datos nx64 Kbps originados desde las agencias remotas son ruteadas sobre la red backbone E1 del proveedor de servicio en time slots dedicados. Los datos agregados (fraccional de E1) terminan dentro del MUX ubicado en la oficina central.

Un canal de datos originado desde una agencia en particular tiene un correspondiente puerto de datos en MUX de la oficina matriz. Los time slots dedicados son mapeados sobre esos puertos de datos para proveer punto a punto, circuitos de datos dedicados arrendados entre la oficina central y cada una de las oficina remotas.

Los puertos disponibles en el MUX TDM pueden ser interfaces V.35, X21, RS530 y G703 balanceada 120.

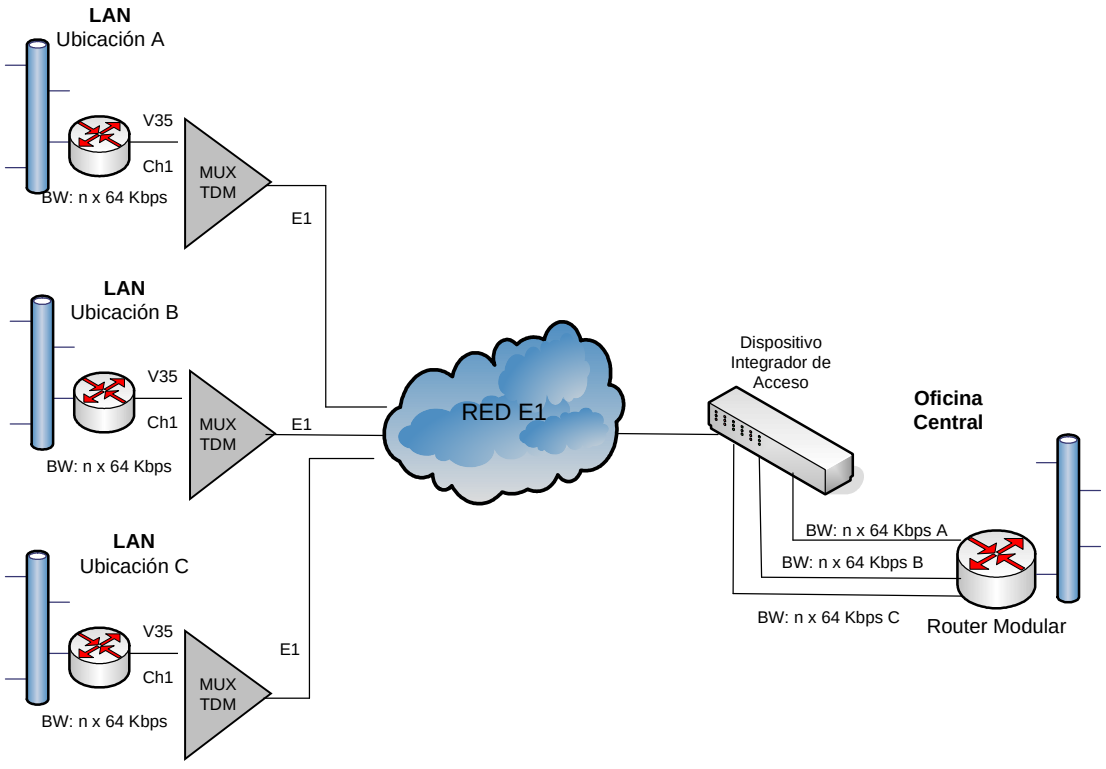

Figura 1.28. Clear Channel Multiagencias - matriz.[28]

[28] Fuente: www.internetghana.com/wan.htm

2. REDES PRIVADAS VIRTUALES

2.1. INTRODUCCIÓN

Una red se extiende sobre un área geográfica amplia, a veces un país o un continente; abarca una colección de máquinas destinadas a ejecutar programas de usuario (aplicaciones).

En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones, sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial.

El alto costo necesario para implementar y mantener enlaces privados, involucra invertir en hardware, software y en servicios de telecomunicaciones para crear redes amplias de servicio (WAN), está llevando a las empresas a una situación insostenible. Las líneas de larga distancia, así como los servicios conmutados, representan una serie de necesidades diarias. El personal de soporte necesario para gestionar las tecnologías complejas conlleva un crecimiento continuo tanto en el número de personas como en su experiencia. Igualmente, la dependencia de aplicaciones de red requiere un aprovisionamiento separado de backup además de una expansión de la infraestructura de la red privada ya existente.

Los ahorros de costos son el poderoso atractivo que ofrecen las Redes Privadas Virtuales ya que se construyen sobre una red pública, sin olvidar la seguridad de los datos transmitidos.

Las VPN están sin duda desplazando a las líneas dedicadas y a Frame Relay, actualmente la penetración es baja, pero poco a poco toma fuerza.

2.2. RED PRIVADA VIRTUAL

Virtual Private Network (VPN) es un grupo de dos o más sistemas de ordenadores, generalmente conectados a una red corporativa privada, que se comunican "con seguridad" sobre una red pública.

Es decir, que para transmitir información a través de una red pública (insegura), en la VPN se aplican métodos de seguridad para garantizar la privacidad de los datos que se intercambian entre ambas, y protocolos de túneles.

A las Redes Privadas Virtuales, se les considera “privadas” porque se establecen exclusivamente entre el emisor y el receptor de la información, y “virtuales”, porque no se necesita un cable o cualquier otro medio físico directo entre los comunicantes.

Las VPN extienden la red corporativa de una empresa a las oficinas distantes, por ejemplo. En lugar de alquilar líneas dedicadas con un costo muy elevado, utilizan los servicios mundiales de IP, incluyendo la Internet.

Usando una VPN, se crea una conexión privada segura a través de una red pública como Internet. Los usuarios remotos pueden hacer una llamada local a Internet, y no usar llamadas de larga distancia.

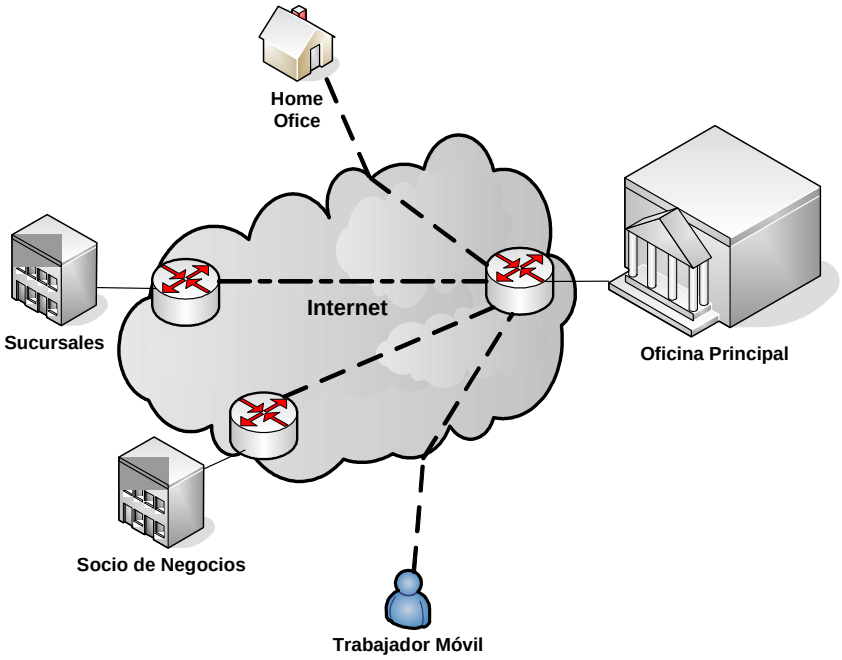

Figura 2.1. Diagrama de una VPN en una Organización.[29]

[29] Fuente: http://computer.howstuffworks.com/vpn.htm

La VPN lo que hace es crear un túnel entre los dos puntos a conectar utilizando infraestructura pública, usa una técnica llamada entunelamiento (tunneling), los paquetes de datos son enrutados por la red pública, tal como Internet o alguna otra red comercial, en un túnel privado que simula una conexión punto a punto. Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura. También hace universales para su transporte los diferentes protocolos LAN entre los que se encuentran IP, IPX, Appletalk y Netbeui, de allí la característica de multiprotocolo que hace sumamente universal la tecnología de las redes virtuales privadas.

2.2.1. REQUERIMIENTOS BÁSICOS DE UNA VPN

Una Red Privada Virtual ha de proveer de los siguientes mecanismos básicos, aunque en ocasiones y situaciones puede obviarse algunos.

- Autentificación de usuarios, verificar la identidad de los usuarios, para poder restringir el acceso a la VPN solo a los usuarios autorizados.
- Administración de direcciones, debe asignar una dirección del cliente sobre la red privada, y asegurar que las direcciones privadas se mantienen privadas.
- Encriptación de datos, los datos que viajan por la red pública, deben ser transformados para que sean ilegibles para los usuarios no autorizados.
- Administración de claves, debe mantener un mantenimiento de claves de encriptación para los clientes y los servidores.
- Soporte multiprotocolo, ha de ser capaz de manejar protocolos comunes, usando las red pública, por ejemplo IPX, IP, etc.

2.3. TIPOS DE VPN

2.3.1. SISTEMAS BASADOS EN HARDWARE

Los sistemas basados en hardware, son routers que encriptan. Son seguros y fáciles de usar, requieren de una configuración correcta y listo. Ofrecen un gran rendimiento, porque no malgastan ciclos de procesador haciendo funcionar un Sistema Operativo. Es hardware dedicado, muy rápido y de fácil instalación.

La implementación entre ruteadores provee la capacidad de asegurar un paquete en una parte de la red, esta seguridad se logra a través del tunneling de paquetes. Las principales ventajas conseguidas con la implementación sobre routers son:

- Capacidad de asegurar el flujo de paquetes entre dos redes, a través de una red pública como Internet.
- Capacidad de auntentificar y autorizar a usuarios el acceso sobre redes privadas.

2.3.2. SISTEMAS BASADOS EN FIREWALL

Estos se implementan con software de cortafuegos (firewall). Tienen las ventajas de los mecanismos de seguridad que utilizan los cortafuegos, incluyendo el acceso restringido a la red interna. También realizan la traducción de direcciones (NAT). Estos satisfacen los requerimientos de autentificación fuerte.

Muchos de los cortafuegos comerciales, aumentan la protección, quitando al núcleo del Sistema Operativo algunos servicios peligrosos que llevan estos por default, y les provee de medidas de seguridad adicionales, que son mucho más útiles para los servicios de VPN.

El rendimiento en este tipo decrece, ya que no se tiene hardware especializado de encriptación.

2.3.3. SISTEMAS BASADOS EN SOFTWARE

Estos sistemas son ideales para las situaciones donde los dos puntos de conexión de la VPN no están controlados por la misma organización, o cuando los diferentes cortafuegos o routers no son implementados por la misma organización. Este tipo de VPN ofrece el método más flexible en cuanto al manejo de tráfico. Con este tipo, el tráfico puede ser enviado a través de un túnel, en función de las direcciones o protocolos, en cambio en los VPN por hardware, todo el tráfico era enrutado por el túnel. Podemos hacer un enrutamiento inteligente de una manera mucho más fácil.

2.4. ARQUITECTURAS VPN

2.4.1. VPN DE ACCESO REMOTO

También denominadas VPDN (Virtual Private Dial-up Network), es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones, etc.) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

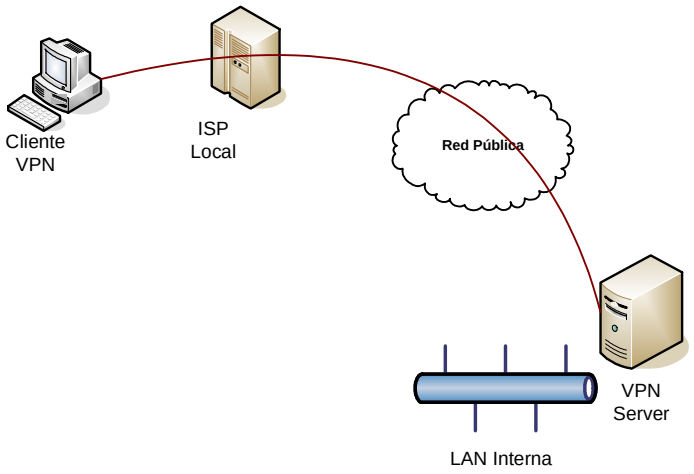

Figura 2.2. Diagrama de VPN por Acceso Remoto.

Muchas empresas han reemplazado con esta tecnología su infraestructura "dial-up" (módems y líneas telefónicas), aunque por razones de contingencia todavía conservan sus viejos modems.

Con el acceso remoto VPN un trabajador que se haya desplazado a otro país, por ejemplo, y que quiere acceder a la base de datos de su compañía, o al correo interno, o a cualquier otro recurso de su red corporativa, solo tiene que conectarse a Internet con una simple llamada local al ISP de la ciudad en la que se encuentre, y ejecutar su cliente de marcación VPN.

A partir de la versión Windows98, Microsoft incluyó un cliente de marcación VPN que funciona con el protocolo de entunelamiento PPTP. Todos los gateways VPN vienen con software VPN clientes para ser instalados en los distintos sistemas operativos presentes en el mercado.

2.4.2. VPN SITIO A SITIO

Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El equipo central VPN, que posee un vínculo a Internet permanente, acepta las conexiones vía Internet provenientes de los sitios y establece el "túnel" vpn. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto, sobre todo en las comunicaciones internacionales.

Esta configuración puede ser de dos tipos:

- Tipo Intranet.
- Tipo Extranet.

2.4.2.1. Tipo Intranet

Si la empresa tiene una o más sucursales remotas que quiere unir en una única red privada, puede hacerlo creando una VPN para conectar ambas redes locales.

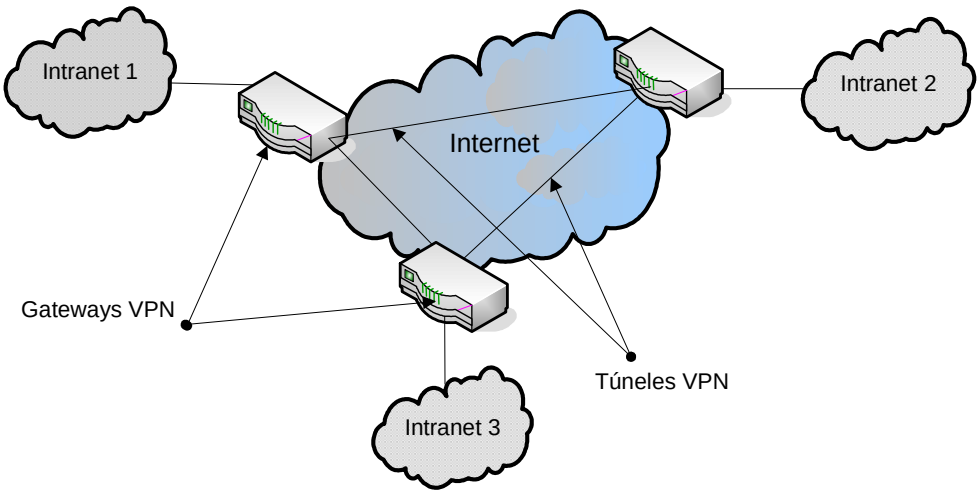

Figura 2.3. Diagrama Intranet VPN.

2.4.2.2. Tipo Extranet

Cuando la empresa tiene una relación cercana con otra compañía (por ejemplo, una empresa asociada, un proveedor o cliente), entonces pueden desarrollar una VPN que conecte sus redes y permita a estas empresas trabajar en un ambiente compartido.

Con una arquitectura de Extranet VPN cada empresa tiene que controlar muy meticulosamente el acceso a los recursos de su red corporativa y a los datos que van a intercambiar con sus socios de negocios. Implementar una topología Extranet VPN implica incrementar la complejidad de los sistemas de control de acceso y de autenticación.

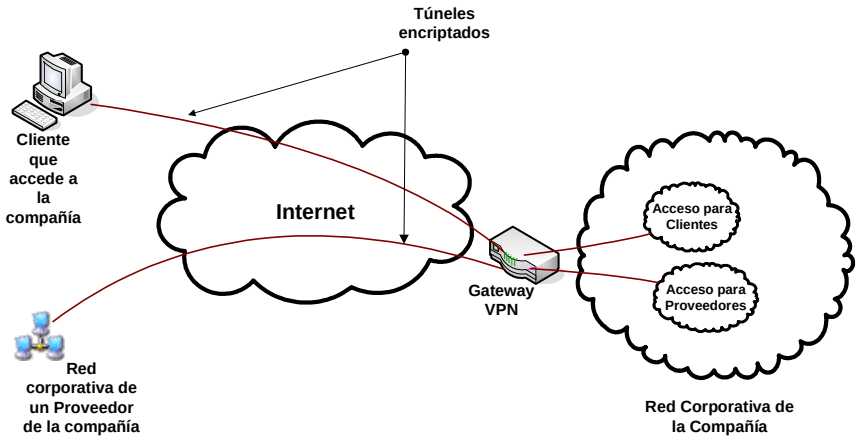

Figura 2.4. Diagrama de Extranet VPN.

2.4.3. VPN INTERNA

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red LAN (Red de área local) de la empresa. Sirve para aislar zonas y servicios de la red LAN interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (Wi-Fi).

La mayoría de incidentes de seguridad está relacionada con abusos dentro de la red de la compañía, por lo tanto a más de los ataques externos no hay que perder de vista los ataques internos. Dependiendo del tipo de negocio o por asuntos legales, cierta información puede ser privada y confidencial a un nivel de departamento.

Una VPN entre departamentos puede ayudar a encontrar esos requerimientos de confidencialidad.

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de RR.HH habilitado pueda acceder a la información.

Otro ejemplo puede ser un requerimiento de e-mail confidencial, como se muestra en la figura 2.5.

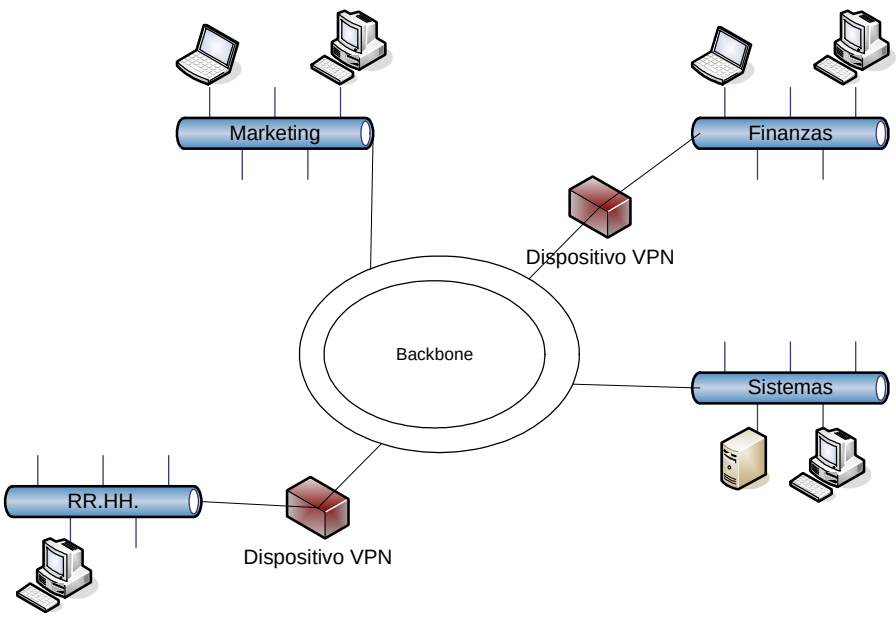

Figura 2.5. Arquitectura VPN Interna.

2.5. TECNOLOGÍAS VPN

Básicamente, y haciendo referencia al modelo OSI, se puede crear una VPN usando tecnologías de Tunneling de capa 2 (enlace de datos) y de capa 3 (red).

2.5.1. TUNNELING

Es una técnica que usa una infraestructura entre redes para transferir datos de una red a otra. Los datos o la carga pueden ser transferidas como tramas de otro protocolo. El protocolo de tunneling encapsula las tramas con una cabecera adicional, en vez de enviarla como la produjo en nodo original. La cabecera adicional proporciona información de routing para hacer capaz a la carga de atravesar la red intermedia. Las tramas encapsuladas son enrutadas a través de un túnel que tiene como puntos finales los dos puntos entre la red intermedia. El túnel es un camino lógico a través del cual se encapsulan paquetes viajando entre la red intermedia. Cuando un trama encapsulada llega a su destino en la red intermedia, se desencapsula y se envía a su destino final dentro de la red. Tunneling incluye todo el proceso de encapsulado, desencapsulado, transmisión de las tramas.

Las tecnologías de Tunneling son:

- DLSW (Data Link Switching).
- IPX for Novell Netware over IP.
- GRE (Generic Routing Encapsulation).
- ATMP (Ascend Tunnel Management Protocol).
- Mobile IP (For mobile users).
- IPSec (Internet Protocol Security Tunnel Mode).
- PPTP (Point-to-Point Tunneling Protocol).
- L2F (Layer 2 Forwarding).
- L2TP (Layer 2 Tunneling Protocol).
- MPLS (Multi Protocol Label Switching).

2.6. EL PROTOCOLO IPSec

2.6.1. DESCRIPCION DEL PROTOCOLO [30]

IPSec en realidad es un conjunto de estándares para integrar en IP, funciones de seguridad basadas en criptografía.

Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y certificados digitales X509v3.

El protocolo IPSec ha sido diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Han sido definidos, sin embargo, ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet.

Dichos algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones de hash. Además es perfectamente posible usar otros algoritmos que se consideren más seguros o más adecuados para un entorno específico: por ejemplo, como algoritmo de cifrado de clave simétrica IDEA, Blowfish o el más reciente AES que se espera sea el más utilizado en un futuro próximo.

Dentro de IPSec se distinguen los siguientes componentes:

- Dos protocolos de seguridad: IP Authentication Header **(AH)** e IP Encapsulating Security Payload **(ESP)** que proporcionan mecanismos de seguridad para proteger tráfico IP.
- Un protocolo de gestión de claves Internet Key Exchange **(IKE)** que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

[30] Fuente: http://www.tid.es/presencia/publicaciones/comsid/esp/23/04.pdf

2.6.2. EL PROTOCOLO AH

El protocolo AH es el procedimiento previsto dentro de IPSec para garantizar la integridad y autenticación de los datagramas IP. Esto es, proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados en tránsito. Sin embargo no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros.

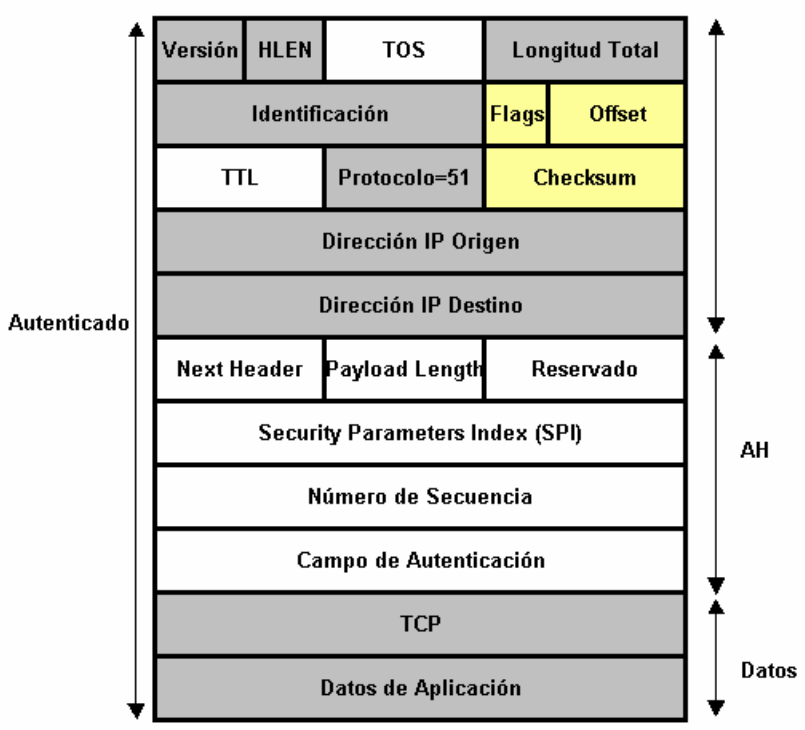

Figura 2.6. Estructura de un Datagrama AH.[31]

Tal como indica su nombre, AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar (tanto IPv4 como IPv6) y los datos transportados, que pueden ser un mensaje TCP, UDP o ICMP, o incluso un datagrama IP completo (ver la Figura 2.6).

AH es realmente un protocolo IP nuevo, y como tal el IANA le ha asignado el número decimal 51. Esto significa que el campo Protocolo de la cabecera IP contiene el valor 51, en lugar de los valores 6 ó 17 que se asocian a TCP y UDP respectivamente. Es dentro de la cabecera AH donde se indica la naturaleza de

[31] Fuente: http://www.tid.es/presencia/publicaciones/comsid/esp/23/04.pdf

los datos de la capa superior. Es importante destacar que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP, excepto los campos variables: TOS, TTL, flags, offset y checksum (ver la Figura 2.6).

El funcionamiento de AH se basa en un algoritmo HMAC, esto es, un código de autenticación de mensajes. Este algoritmo consiste en aplicar una función hash a la combinación de unos datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que denominamos extracto. Dicho extracto tiene la propiedad de que es como una huella personal asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave.

En la Figura 2.7 se muestra el modo en que funciona el protocolo AH. El emisor calcula un extracto del mensaje original, el cual se copia en uno de los campos de la cabecera AH. El paquete así construido se envía a través de la red, repitiéndose en el extremo receptor el cálculo del extracto y comparándolo con el recibido en el paquete.

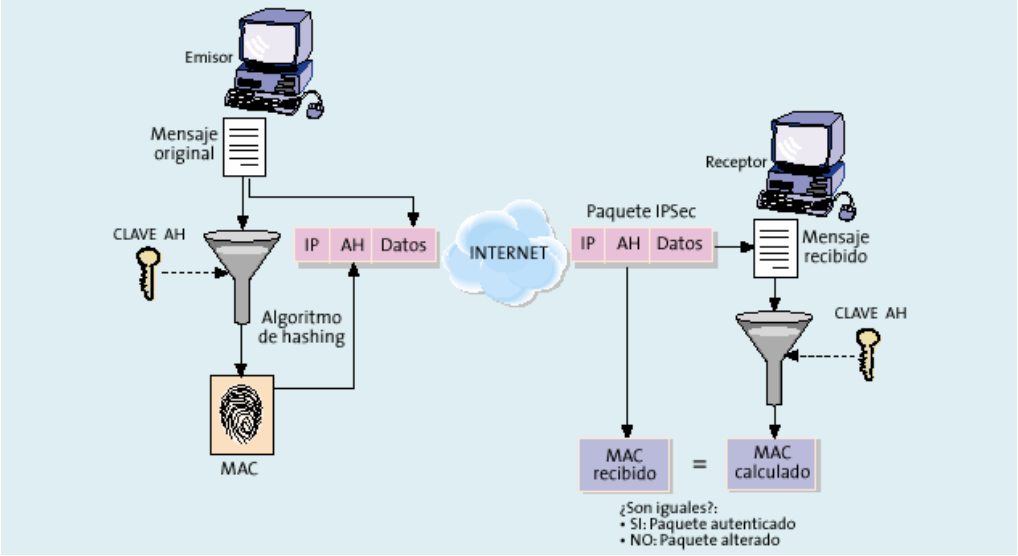

Figura 2.7. Funcionamiento del Protocolo AH.[32]

Si son iguales, el receptor tiene la seguridad de que el paquete IP no ha sido modificado en tránsito y que procede efectivamente del origen esperado.

Si analizamos con detalle el protocolo AH, podemos concluir que su seguridad reside en que el cálculo del extracto (MAC) es imposible sin conocer la clave, y

[32] Fuente: http://www.tid.es/presencia/publicaciones/comsid/esp/23/04.pdf

que dicha clave (en la Figura 2.7, clave AH) sólo la conocen el emisor y el receptor.

2.6.3. EL PROTOCOLO ESP

El objetivo principal del protocolo ESP (Encapsulating Security Payload) es proporcionar confidencialidad, para ello especifica el modo de cifrar los datos que se desean enviar y como este contenido cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH.

Dado que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo; este formato consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo IP (por ejemplo, TCP, UDP o ICMP, o incluso un paquete IP completo). En la Figura 2.8 se muestra la estructura de un datagrama ESP, en la que se observa cómo el contenido o carga útil viaja cifrado.

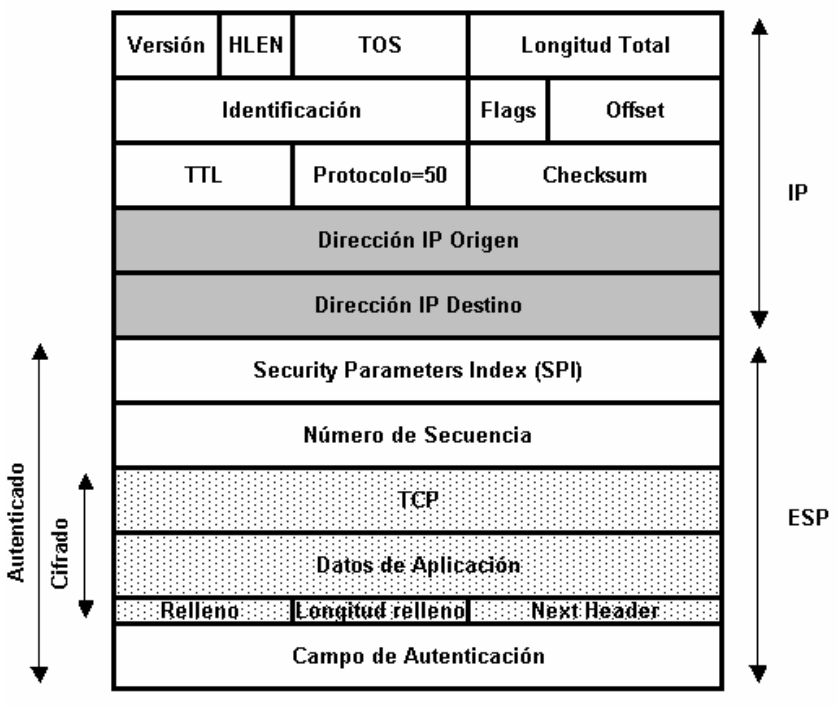

Figura 2.8. Estructura de un datagrama ESP.[33]

[33] Fuente: http://www.tid.es/presencia/publicaciones/comsid/esp/23/04.pdf

El IANA ha asignado al protocolo ESP el número decimal 50. Esto implica que el campo Protocolo de la cabecera IP contendrá el valor 50, mientras que dentro del mensaje ESP se indica la naturaleza de los datos. Puesto que este campo, al igual que la carga útil, está cifrado, un hipotético atacante que intercepte el paquete no podrá saber si el contenido es TCP o UDP; esto es completamente normal ya que el objetivo que se persigue es, precisamente, ocultar la información.

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica. Típicamente se usan algoritmos de cifrado bloque, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque (8 o 16 bytes, en la mayoría de los casos). Por esta razón existe un campo de relleno, tal como se observa en la Figura 2.9, el cual tiene una función adicional: es posible añadir caracteres de relleno al campo de datos para ocultar así su longitud real y, por tanto, las características del tráfico. Un atacante suficientemente hábil podría deducir cierta información a partir del análisis de ciertos parámetros de las comunicaciones, aunque estén cifradas, tales como el retardo entre paquetes y su longitud. La función de relleno está pensada para dificultar este tipo de ataques.

En la Figura 2.9 se representa cómo el protocolo ESP permite enviar datos de forma confidencial. El emisor toma el mensaje original, lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP. Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bits ininteligibles. En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales.

Está claro que la seguridad de este protocolo reside en la robustez del algoritmo de cifrado, es decir, que un atacante no puede descifrar los datos sin conocer la clave, así como en que la clave ESP únicamente la conocen el emisor y el receptor.

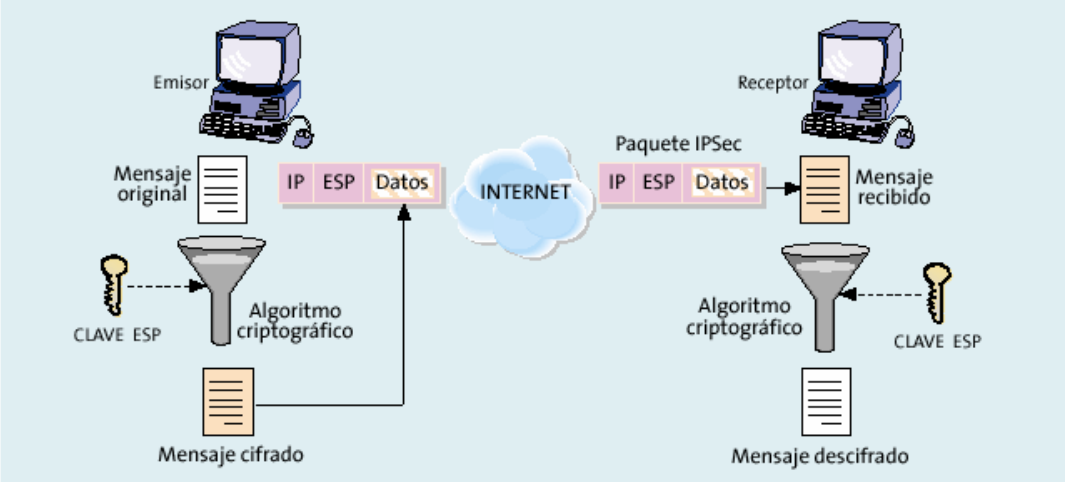

Figura 2.9. Funcionamiento del protocolo ESP.[34]

La distribución de claves de forma segura es, por consiguiente, un requisito esencial para el funcionamiento de ESP y también de AH, como hemos visto anteriormente.

Asimismo, es fundamental que el emisor y el receptor estén de acuerdo tanto en el algoritmo de cifrado o de hash como en el resto de parámetros comunes que utilizan. Esta labor de puesta en contacto y negociación es realizada por un protocolo de control, denominado IKE, que se explicará más adelante.

2.6.4. LOS MODOS TRANSPORTE Y TUNEL

Antes de entrar en los detalles del protocolo IKE es necesario explicar los dos modos de funcionamiento que permite IPSec. Tanto ESP como AH proporcionan dos modos de uso:

2.6.4.1. El Modo Transporte

En este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo

[34] Fuente: http://www.tid.es/presencia/publicaciones/comsid/esp/23/04.pdf

transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.

2.6.4.2. El Modo Túnel

En éste el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

El modo túnel es empleado principalmente por los gateways IPSec, con objeto de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el procesado del tráfico IPSec en un equipo. El modo túnel también es útil, cuando se utiliza junto con ESP, para ocultar la identidad de los nodos que se están comunicando. Otra aplicación del modo túnel, tanto con ESP como con AH, es poder establecer Redes Privadas Virtuales (VPN) a través de redes públicas, es decir, interconectar de forma segura redes de área local, incluso en el caso de que éstas usen direccionamiento privado o no legal en Internet.

IPSec puede ser implementado bien en un host o bien en un equipo dedicado, tal como un router o un firewall, que cuando realiza estas funciones se denomina gateway IPSec. La Figura 2.10 muestra los dos modos de funcionamiento del protocolo IPSec, donde:

- En la Figura 2.10a se representan dos hosts que entienden IPSec y que se comunican de forma segura. Esta comunicación se realiza en modo transporte, por tanto la información que se protege es únicamente el protocolo TCP o UDP, así como los datos de aplicación.
- En la Figura 2.10b se muestran dos redes que utilizan para conectarse dos gateways IPSec y, por tanto, emplean una implementación en modo túnel. Se puede ver que la comunicación se realiza a través de una red de datos pública, entre un PC situado en una red local con otro PC situado en una red local remota, de modo que entre los gateways IPSec se establece un

túnel a través del cual viajan protegidas las comunicaciones entre ambas redes locales.

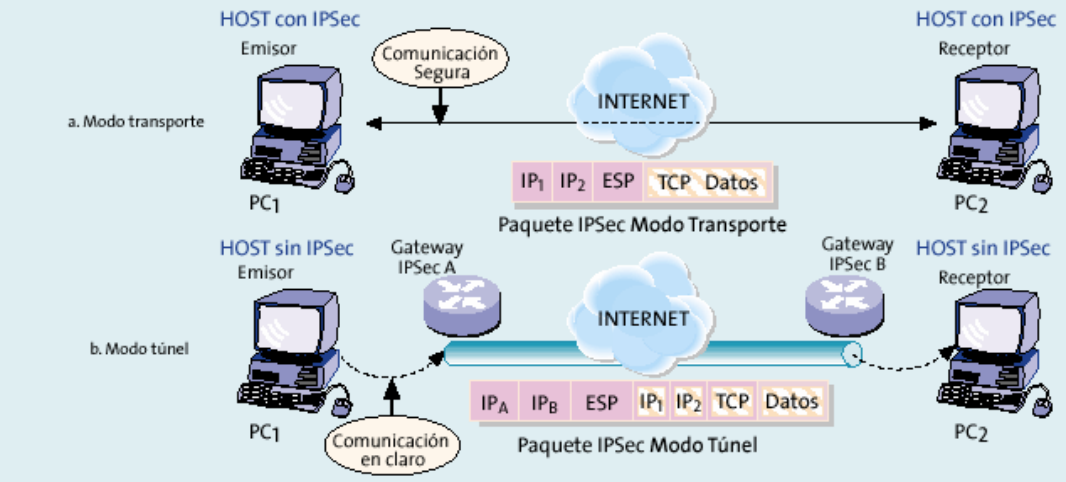

Figura 2.10. Modos de Funcionamiento Transporte y Túnel en IPSec.[35]

Sin embargo ambos PC's envían y reciben el tráfico en claro, como si estuviesen situados en la misma red local. Este esquema tiene la ventaja de que los nodos situados en redes separadas pueden comunicarse de forma segura y transparente, concentrándose, al mismo tiempo, las funciones de seguridad en un único punto, facilitando así las labores de administración.

2.6.5. IKE (INTERNET KEY EXCHANGE)

Un concepto esencial en IPSec es el de asociación de seguridad (SA), es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SA's, una por cada sentido de la comunicación.

Hasta el momento se ha supuesto que ambos extremos de una asociación de seguridad deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos estén de acuerdo

[35] Fuente: http://www.tid.es/presencia/publicaciones/comsid/esp/23/04.pdf

tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios; a esta operación se le llama negociación de SA's.

El IETF ha definido el protocolo IKE para realizar tanto esta función de gestión automática de claves como el establecimiento de las SA's correspondientes.

Una característica importante de IKE es que su utilidad no se limita a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos, como, por ejemplo, OSPF o RIPv2.

IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios: ISAKMP y Oakley.

ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec. Dicha negociación se lleva a cabo en dos fases:

2.6.5.1. Primera Fase IKE

La fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro y autenticado.

Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene mediante el algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de los nodos, para ello es necesario un paso adicional de autenticación.

Existen varios métodos de autenticación, los dos más comunes se describen a continuación:

- El primer método de autenticación se basa en el conocimiento de un secreto compartido que, como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones hash cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentican mutuamente. Para no debilitar la seguridad de este mecanismo de autenticación, debe configurarse un secreto distinto para cada par de nodos, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de nodos. Por esta razón en entornos en los que se desea interconectar muchos nodos IPSec la gestión de claves es muy complicada. En este caso no se recomienda el uso de autenticación mediante secreto compartido, sino autenticación basada en certificados digitales.
- En los estándares IPSec está previsto el uso de un método de autenticación que se basa en utilizar certificados digitales X509v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere de la aparición de un elemento más en la arquitectura IPSec, la PKI (Infraestructura de Clave Pública), cuya integración se tratará con detalle más adelante.

2.6.5.2. Segunda Fase IKE

En la segunda fase el canal seguro IKE es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, en nuestro caso IPSec.

Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga

definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

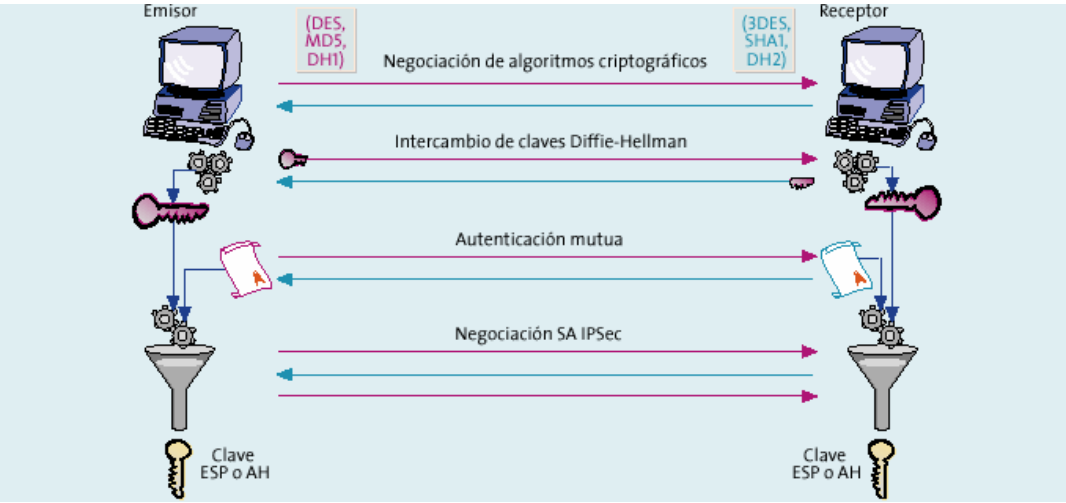

Figura 2.11. Funcionamiento del protocolo IKE.[36]

El funcionamiento del protocolo IKE y el modo en que se obtiene una clave de sesión, que es la que se utiliza para proteger las conexiones ESP o AH. Se muestra en la figura 2.11.

2.6.6. INTEGRACIÓN DE IPSEC CON UNA PKI

El uso de una PKI aparece en IPSec como respuesta a la necesidad de un procedimiento para autenticar de forma fiable a un conjunto de nodos que desean comunicarse mediante IPSec, siendo dicho conjunto de nodos muy numeroso. La existencia de una PKI ofrece otras ventajas, ya que se centraliza el alta y baja de los usuarios, además se posibilita la introducción de tarjetas inteligentes para soportar los certificados, lo cual es muy interesante para la aplicación de IPSec en un entorno de tele-trabajadores o usuarios móviles.

Bajo el nombre de PKI (Infraestructura de Clave Pública) se engloban todos los elementos y procedimientos administrativos que permiten emitir, revocar y, eventualmente, renovar los certificados digitales para una comunidad de usuarios. En el caso de IPSec los sujetos de los certificados son los nodos IPSec, mientras

[36] Fuente: http://www.tid.es/presencia/publicaciones/comsid/esp/23/04.pdf

que la función de los certificados es proporcionar un medio fiable para autenticar la identidad de los dispositivos IPSec. Cada uno de los dispositivos IPSec dispondrá de un certificado digital que contendrá su clave pública y la información suficiente para identificar de forma unívoca al dispositivo (tal como su nombre DNS, su dirección IP o su número de serie). Esta asociación entre clave pública e identidad está avalada por la firma de la Autoridad de Certificación (CA) integrada en la PKI, que da validez al certificado. Se supone que todos los dispositivos IPSec reconocerán como válida la misma CA, para lo cual deberán disponer de una copia del certificado de la propia CA.

Los protocolos para la interacción de los dispositivos IPSec con una PKI no están especificados en ninguno de los protocolos de IPSec. Todos los fabricantes utilizan X.509v3 como formato común de los certificados, así como los estándares de la serie PKCS para la solicitud y descarga de certificados. Sin embargo, el protocolo de comunicaciones, mediante el cual los dispositivos IPSec dialogan con la PKI, no está totalmente estandarizado. Esto hace que existan varias alternativas según el fabricante de que se trate.

En general los nodos IPSec necesitan realizar ciertas operaciones básicas con una PKI: acceder al certificado de la CA, solicitar y descargar un certificado, así como comprobar la validez de un certificado recibido.

En la actualidad, la mayoría de los nodos IPSec realizan la validación de los certificados mediante consultas de la Lista de Certificados Revocados (CRL), que se almacena en el directorio de la PKI. Para ello, cada uno de los nodos mantendrá una copia de la CRL, que actualizará periódicamente mediante una consulta LDAP al directorio de la PKI. Típicamente, los períodos de actualización de la CRL serán del orden de horas, de modo que existirá cierto retardo desde que la PKI revoca un certificado hasta que todos los dispositivos tengan constancia de dicha revocación.

Para la solicitud y descarga de certificados existe un protocolo denominado SCEP, que se ha convertido en un estándar de facto en las operaciones de registro y descarga de certificados para aplicaciones IPSec. SCEP es un protocolo desarrollado originalmente por Cisco y Verisign, que se basa en el intercambio de mensajes PKCS, mediante protocolo HTTP, para automatizar los procesos de solicitud y descarga de certificados.

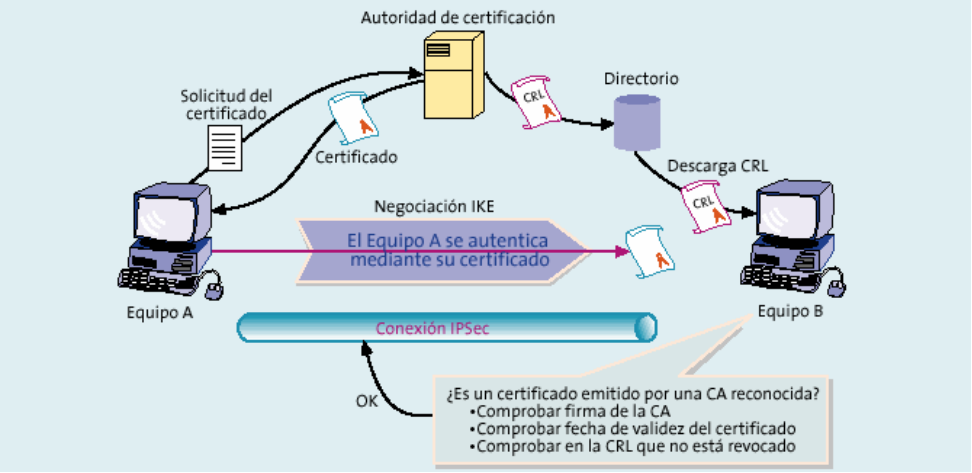

Figura 2.12. Integración de una PKI en IPSec.[37]

En la Figura 2.12 se representan los flujos de comunicación entre una PKI y un nodo IPSec. Inicialmente, cada uno de los nodos genera un par de claves (pública y privada) y envía una petición de certificado a la CA, en la que incluye información de su identidad y su clave pública. Al mismo tiempo, el nodo descarga el certificado raíz de la CA; a continuación, la CA genera un certificado para el dispositivo IPSec y éste lo recibe. A partir de ese momento el nodo IPSec podrá usar su certificado en una negociación IKE para autenticarse frente a otros dispositivos. Periódicamente los dispositivos IPSec accederán al directorio de la PKI para actualizar la CRL.

2.7. SERVICIOS DE SEGURIDAD OFRECIDOS POR IPSEC

2.7.1. INTEGRIDAD Y AUTENTICACIÓN DEL ORIGEN DE LOS DATOS

El protocolo AH es el más adecuado si no se requiere cifrado. La opción de autenticación del protocolo ESP ofrece una funcionalidad similar, aunque esta protección, a diferencia de AH, no incluye la cabecera IP. Como se comentó anteriormente, esta opción es de gran importancia para aquellas aplicaciones en las cuales es importante garantizar la invariabilidad del contenido de los paquetes IP.

[37] Fuente: http://www.tid.es/presencia/publicaciones/comsid/esp/23/04.pdf

2.7.2. CONFIDENCIALIDAD

El servicio de confidencialidad se obtiene mediante la función de cifrado incluida en el protocolo ESP. En este caso es recomendable activar la opción de autenticación, ya que si no se garantiza la integridad de los datos el cifrado es inútil. Esto es debido a que aunque los datos no pudiesen ser interpretados por nadie en tránsito, éstos podrían ser alterados haciendo llegar al receptor del mensaje tráfico sin sentido que sería aceptado como tráfico válido.

Además de ofrecer el cifrado del tráfico, el protocolo ESP también tiene herramientas para ocultar el tipo de comunicación que se está realizando; para ello permite introducir caracteres de relleno en el contenido de los datos del paquete, de modo que se oculta la verdadera longitud del mismo. Esta es una protección útil contra las técnicas de análisis de tráfico, que permiten a un atacante deducir información útil a partir del estudio de las características del tráfico cifrado. El análisis de tráfico es un riesgo que debe considerarse seriamente, recientemente se ha documentado la viabilidad para deducir información a partir del tráfico cifrado de una conexión SSH. Es previsible que este tipo de ataques se hagan más habituales y sofisticados en el futuro, conforme se generalice el cifrado de las comunicaciones.

2.7.3. DETECCIÓN DE REPETICIONES

La autenticación protege contra la suplantación de la identidad IP, sin embargo un atacante todavía podría capturar paquetes válidos y reenviarlos al destino. Para evitar este ataque, tanto ESP como AH incorporan un procedimiento para detectar paquetes repetidos. Dicho procedimiento está basado en un número de secuencia incluido en la cabecera ESP o AH, el emisor incrementa dicho número por cada datagrama que envía y el receptor lo comprueba, de forma que los paquetes repetidos serán ignorados.

Esta secuencia no podrá ser modificada por el atacante, debido a que se encuentra protegida por medio de la opción de integridad para cualquiera de los dos protocolos (AH y ESP) y cualquier modificación en este número provocaría un error en la comprobación de la integridad del paquete.

2.7.4. CONTROL DE ACCESO

Involucra autenticación y autorización, dado que el uso de ESP y AH requiere el conocimiento de claves, y dichas claves son distribuidas de modo seguro mediante una sesión IKE en la que ambos nodos se autentican mutuamente, existe la garantía de que sólo los equipos deseados participan en la comunicación. Es conveniente aclarar que una autenticación válida no implica un acceso total a los recursos, ya que IPSec proporciona también funciones de autorización. Durante la negociación IKE se especifica el flujo de tráfico IP que circulará a través de la conexión IPSec. Esta especificación es similar a un filtro de paquetes, considerándose el protocolo, las direcciones IP de los puertos origen y destino, el byte "TOS" y otros campos.

Por ejemplo, puede utilizarse IPSec para permitir el acceso desde una sucursal a la red local del centro corporativo, pero impidiendo el paso de tráfico hacia máquinas especialmente protegidas.

2.7.5. NO REPUDIO

El servicio de no repudio es técnicamente posible en IPSec, si se usa IKE con autenticación mediante certificados digitales. En este caso, el procedimiento de autenticación se basa en la firma digital de un mensaje que contiene, entre otros datos, la identidad del participante. Dicha firma, gracias al vínculo entre la clave pública y la identidad que garantiza el certificado digital, es una prueba inequívoca de que se ha establecido una conexión IPSec con un equipo determinado, de modo que éste no podrá negarlo. En la práctica, sin embargo, esta prueba es más compleja, ya que requeriría almacenar los mensajes de negociación IKE y, además, no está definido un procedimiento para referenciar este evento a una fecha concreta.

2.8. APLICACIONES CON IPSEC

La tecnología IPSec permite construir soluciones de comunicaciones que ofrecen confidencialidad y autenticación en la capa IP, independientemente de cual sea el medio de transporte (FR, PPP, xDSL o ATM). Además, la inclusión de seguridad en la capa IP tiene la ventaja de que se extiende universalmente, ofreciendo un nivel de seguridad homogéneo de manera independiente del tipo que sean las aplicaciones, siempre que estén basadas en IP.

IPsec tiene muchas implementaciones, a continuación se presentan las más comunes.

2.8.1. IMPLEMENTACIÓN DE IPSEC EN LINUX

FreeS/WAN es una implementación libre distribuida bajo licencia GPL (GNU Public Licence) del protocolo IPsec para sistemas operativos GNU/Linux. El proyecto comprende dos grandes áreas, una es el código que se agrega al núcleo de Linux (actualmente es un parche separado ya que no integra el núcleo) y la otra parte es el código de las herramientas que el usuario utiliza para hacer que se establezcan los túneles (entre otras cosas).

Justamente una de las ventajas de utilizar IPSec es que existen muchos otros sistemas operativos que tienen implementado IPSec (además de que es sumamente seguro) y esto permite que con Linux podamos establecer túneles cifrados contra otras redes que tengan sistemas operativos diferentes.

Otro caso común de uso de IPsec y/o FreeS/WAN es el del denominado “Road Warrior” o Guerrero de Carretera. Bajo este nombre contempla el escenario en el que una persona puede conectar un único equipo (portátil ó PDA) a una red corporativa desde fuera de esta. Sería el caso de un trabajador que quiere conectar con su empresa desde casa, un representante en viaje de negocios que necesita conectarse al servidor desde la habitación de su hotel, etc. FreeS/WAN también contempla este caso, y es capaz de operar tanto en modo cliente (en el ordenador del trabajador remoto) como servidor (en el router de entrada a la red corporativa) para dar conexión a los road warriors.

2.8.2. IMPLEMENTACIÓN DE IPSEC EN UNIX

Una puesta en práctica de IPsec se incluye en NetBSD y FreeBSD, pertenecen a la misma familia Unix, BSD comprende tres variedades y tienen sus propias características que los hacen únicos:

- OpenBSD: Enfocado a la Seguridad.
- FreeBSD: Plataforma i386, primando el rendimiento.
- NetBSD: Sistema UNIX, que se ejecuta en mayor número de plataformas hardware.

OpenBSD, para conseguir su objetivo de máxima seguridad, el proyecto esta ubicado en Canadá, donde se exporta con criptografía integrada, esto les ha permitido ser el primer sistema operativo en incluir IPsec. A partir de su versión 2.2, OpenBSD incorpora IPSec de serie.

La forma en la que se configuran los sistemas IPsec y las pasarelas es, hasta un cierto punto, trabajo del diseñador; sin embargo, el RFC contiene algunas recomendaciones importantes sobre cómo se debería implementar para evitar al máximo la confusión. [38]

Existen dos entidades administrativas que controlan lo que le ocurre a un paquete. Una es la “Base de Datos de Asociación de la Seguridad” (SAD, *Security Association Database*, llamado TDB o tabla TDB en el código fuente de IPsec de OpenBSD), y el otro es la “Base de Datos de Política de la Seguridad” (SPD, *Security Policy Database*).

Una entrada SAD incluye:

- Dirección IP de destino.
- Protocolo IPsec (AH o ESP).
- SPI (cookie).
- Contador de secuencias.
- Indicador de secuencia O/F.
- Ventana de información anti-réplica.
- Tipo de AH e información.
- Tipo de ESP e información.

[38] Fuente: http://tech.zone.ee/openbsd/faq/es/faq13.html

- Información sobre el tiempo de vida.
- Indicadores de modos túnel/transporte.
- Información sobre el camino MTU.

Una entrada SPD contiene:

- Puntero a SAs activas.
- Campos de selector.

Cada SA puede definir una cabecera ESP y una cabecera AH. Una sesión de IPsec debe tener una de las dos o ambas, pero no se puede definir sin ninguna de las dos.

OpenBSD implementa el intercambio automático de claves ISAKMP en el dæmon isakmpd.

FreeBSD es un avanzado sistema operativo para arquitecturas x86 compatibles (incluyendo Pentium® y Athlon™), amd64 compatibles (incluyendo Opteron™, Athlon 64 y EM64T), Alpha/AXP, IA-64, PC-98 y UltraSPARC®. FreeBSD es un derivado de BSD, la versión de UNIX® desarrollada en la Universidad de California, Berkeley. FreeBSD es desarrollado y mantenido por un numeroso equipo de personas. El soporte para otras arquitecturas está en diferentes fases de desarrollo.

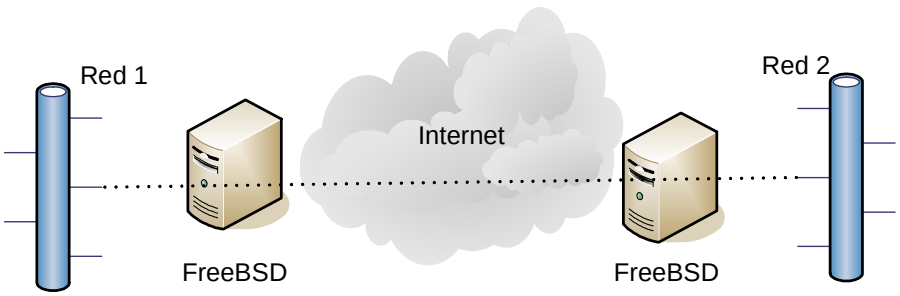

Figura 2.13. VPN que utiliza dos gateways FreeBSD.

FreeBSD está especialmente dedicado a los procesadores Intel y Alpha y "hereda" una parte de la filosofía de seguridad de OpenBSD. Semejante a Linux,

el hecho que funcione con procesadores Intel hace que sea uno de los BSD más ampliamente conocido.

Ofrece altas prestaciones en comunicaciones de red, rendimiento, seguridad y compatibilidad, todavía inexistentes en otros sistemas operativos, incluyendo los comerciales de mayor renombre, es el servidor ideal para servicios de Internet o Intranet. Proporciona servicios de red robustos, incluso en situaciones de alta carga, haciendo un uso eficaz de la memoria para mantener buenos tiempos de respuesta con cientos o miles de procesos simultáneos de usuarios.

FreeBSD 5.X contiene una pila IPsec “acelerada por hardware”, conocida como “Fast IPsec”, que fue obtenida de OpenBSD. Emplea hardware criptográfico (cuando es posible) a través del subsistema crypto para optimizar el desempeño de IPsec. Este subsistema es nuevo, y no soporta todas las opciones que están disponibles en la versión KAME de IPsec.

2.8.3. IMPLEMENTACIÓN DE IPSEC EN WINDOWS

IPSec está soportado en Windows Server™ 2003, Windows XP, y Windows 2000, y está integrado con el servicio de Directorio Activo. Las políticas IPSec se pueden asignar mediante Políticas de Grupo, lo que permite que los parámetros de IPSec se configuren a nivel de dominio, sitio o unidad organizativa.

Comprende la configuración de directivas IPSec y el protocolo Intercambio de claves de Internet (IKE, Internet Key Exchange), existe una interfaz gráfica de usuario y varias herramientas de la línea de comandos para ello.

Microsoft L2TP/IPSec es un cliente VPN que se puede descargar gratis y permite a computadores con Windows 98, Windows Millennium Edition (Me) o Windows NT® Workstation 4.0, usar conexiones L2TP (Layer Two Tunneling Protocol) con IPSec, la combinación de L2TP e IPSec, se conoce como L2TP/IPSec. Es una tecnología altamente segura para realizar conexiones de acceso VPN a través de la red pública como Internet. Microsoft L2TP/IPSec VPN Client también provee soporte para travesía Network Address Translation (NAT).

IPSec es transparente para las aplicaciones de usuario final y los servicios del sistema operativo, excepto por un breve retardo necesario para negociar una relación de seguridad entre ambos equipos.

2.8.4. IMPLEMENTACIÓN DE IPSEC EN CISCO

Los siguientes productos de Cisco pueden implementar una VPN con IPSec:

- Cisco VPN routers: Usa el software Cisco IOS soporta Ipsec para habilitar una VPN segura, la VPN optimizada por routers es perfecto para una WAN híbrida.
- Cisco Secure PIX Firewall: Ofrece un gateway VPN, alternativa cuando la seguridad de grupo posee la VPN.
- Cisco VPN Concentrator series: Ofrece la capacidad de acceso remoto poderoso y VPN sitio a sitio, interface de administración fácil para usar y un VPN client.
- Cisco Secure VPN Client: Habilita acceso remoto seguro hacia un router Cisco o PIX Firewalls y corre en el sistema operativo Windows, entre otros sistemas operativos.
- Cisco Secure Intrusion Detection System (CSIDS) y Cisco Secure Scanner: Puede ser usado para monitorear y auditar la seguridad de la VPN.
- Cisco Secure Policy Manager y Cisco Works 2000: Provee sistema de administración amplia VPN.

En la tabla 2.3 se muestra los productos Cisco y sus características y beneficios para VPN's sitio a sitio y acceso remoto.

	VPN Sitio-a-Sitio	**VPN de Acceso Remoto IPSec**
Cisco PIX Security Appliances	SI	SI
Cisco VPN 3000 Series	SI	La característica más rica
Cisco IOS Software or Cisco Catalyst Switches	La característica más rica	SI
Cisco ASA 5500 Series	SI	La característica más rica

Tabla 2.1. Productos Cisco para VPN Sitio-a-Sitio y Acceso Remoto.[39]

[39] Fuente: http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns142/netbr09186a00801f0a72.html

El siguiente gráfico muestra una integración de productos Cisco Systems en las VPN.

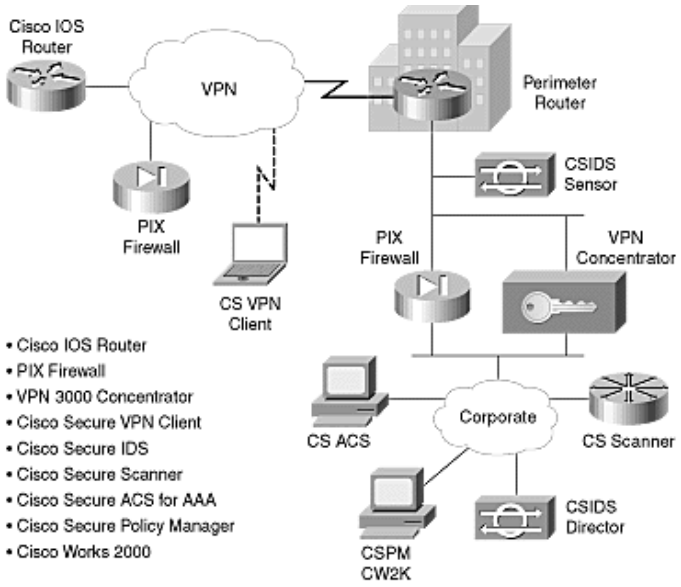

Figura 2.14. Integración de tecnología Cisco.[40]

2.8.5. OTRAS IMPLEMENTACIONES

La mayoría de los cortafuegos y routers disponen de capacidades VPN, en muchos casos se trata de soluciones propietarias, aunque la mayoría han migrado o lo están haciendo a IPSec.

Algunos de los fabricantes que también utilizan IPSec como protocolo de tunneling para VPN son:

- FW-1.
- Macintosh.
- Solaris.
- Sonicwall.
- Motorola (Vanguard).

[40] Fuente: http://www.cisco.com

3. SITUACIÓN ACTUAL DE LA EMPRESA

3.1. DESCRIPCIÓN DE LA EMPRESA

3.1.1. ANTECEDENTES

La empresa comercializadora tomada como caso de estudio para este proyecto de titulación es “CONFITECA” Confites Ecuatorianos C.A, la misma que nace en 1965 con el objetivo de elaborar chicles para el consumidor ecuatoriano, en 1969 comienza a producir chicle bola, después incorpora en su portafolio de productos caramelos duros y suaves.

Por los años ochenta sus ventas crecían a un ritmo reducido del 3% anual, la compañía inicia la fase de desarrollo comercial, toma la decisión de crear su fuerza de ventas, surgen las empresas de distribución de marcas propias y de terceras líneas. Durante la etapa inicial Confiteca centró su distribución en Quito para continuar haciéndolo en Guayaquil.

Desde el año 1993 hasta el año 2003 se hacen inversiones muy grandes en maquinaria e infraestructura en Ecuador, Perú y Colombia. Incursiona su presencia en los mercados vecinos de la región andina, creando un grupo corporativo formado por Confiteca en Ecuador, Confiperú en Perú y Confitecol en Colombia, poco a poco consolida su estrategia exportadora haciéndola mucho más agresiva. Actualmente los productos de CONFITECA se exportan a más de 35 países alrededor del mundo.

Ecuador además de ser la matriz, en porcentaje es el mercado principal del grupo regional. El catálogo de productos de Confiteca se compone básicamente de chicles (con sus productos A go go, Kataboom, Tumix, Boogie), Lolipop’s (con sus marcas Plop y American Paleta) y caramelos (Jaazz, Mint, Zoom, American Toffee).

En chupetería la compañía supera el 60% de las ventas nacionales, mientras que en goma de mascar su liderazgo alcanza un 62% del mercado. Las cifras alcanzadas en la línea de caramelos a pesar de ser reducidas, no dejan de ser importantes: 20% en caramelos duros y 12% en caramelos suaves.

Confiteca cuenta con una compleja infraestructura de distribución compuesta por una flota de camiones capaces de atender a 38,000 puntos de venta en Ecuador,

lo que equivale al 92% de los puntos de venta existentes en el país para productos de confitería.

Esta empresa familiar 100% ecuatoriana incursiona en el mercado de los chocolates en el 2005 con su propia fábrica, bajo el nombre de Ecuatoriana de Chocolates.

La compañía cuenta con un importante laboratorio de control de calidad, Confiteca fue la primera empresa de Ecuador reconocida por el gobierno como capaz de realizar análisis de laboratorio a cualquier otra empresa.

Confiteca es una empresa multinacional regional con un tamaño capaz de hacer frente a las grandes multinacionales y un equipo de trabajo muy bien consolidado.

Actualmente es una de las 14 empresas de mayor éxito en el país, tanto por su presencia en el mercado como por el volumen de exportación de sus productos y lidera el mercado confitero del área andina.

3.1.2. VISIÓN

Satisfacer con liderazgo las necesidades de productos de consumo masivo en el Área Andina.

3.1.3. MISIÓN

“Desarrollar y fortalecer el liderazgo de distribución de productos de confitería, con especialización tienda a tienda, y convertirlo en un servicio legendario para productos de consumo masivo, directamente o a través de alianzas estratégicas.

Optimizar constantemente nuestros procesos de desarrollo y producción de confitería, manteniéndolos altamente competitivos, flexibles y adaptables a las cambiantes necesidades de los consumidores y socios comerciales.

Desarrollar y fortalecer un eficiente trabajo de marcas para lograr su reconocimiento como factor crítico de éxito.

Actuar de manera ética, eficiente y rentable para garantizar el bienestar de nuestros clientes, colaboradores, accionistas y de la comunidad.”

3.1.4. ORGANIGRAMA CORPORATIVO

La empresa está conformada por las siguientes áreas y su respectiva jerarquía, en la figura 3.1, podemos apreciar que el nivel más alto es la junta directiva que representa a los accionistas de la empresa, luego tenemos el comité corporativo que la representan el presidente ejecutivo y los directores.

La presidencia ejecutiva corporativa consta del representante legal, quien coordina todas sus actividades con los directores de áreas y los gerentes de las empresas aliadas de Perú y Colombia.

Las gerencias generales de Confiperú y Confitecol pertenecen a empresas ubicadas en Perú y Colombia respectivamente, cuya dependencia directa la tienen con la Presidencia Ejecutiva Corporativa de Confiteca.

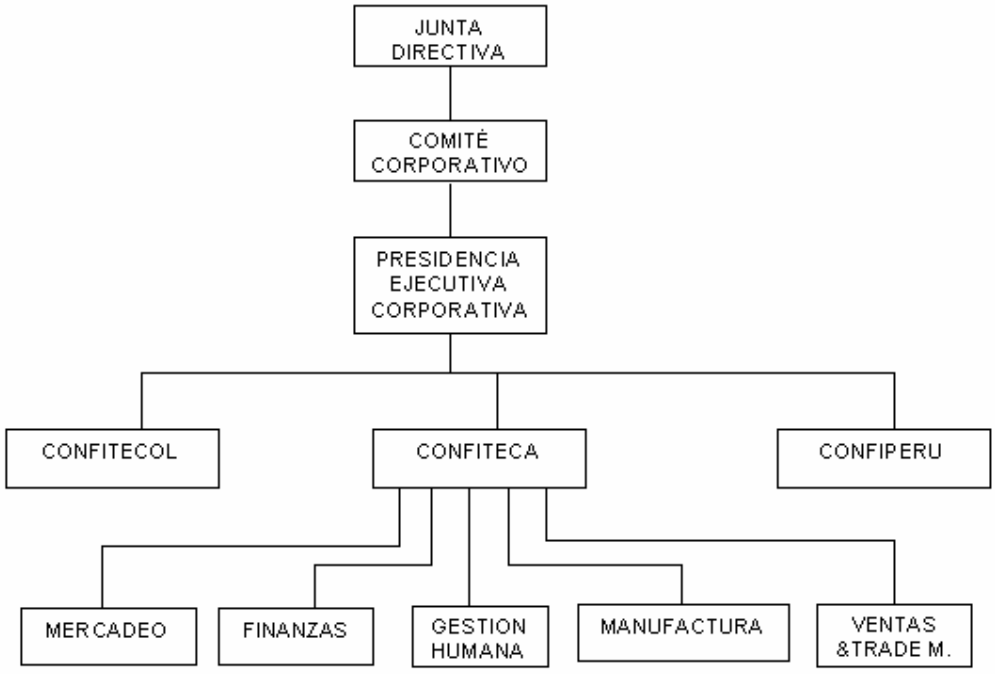

Figura 3.1. Diagrama organizacional corporativo de Confiteca.[41]

[41] Fuente: Confiteca

3.1.5. PRESENCIA EN EL PAIS

Su organización empresaria es de tipo piramidal, con su cima en la sede central ubicada en la ciudad de Quito y sus 9 sucursales en las ciudades de Ibarra, Quito (Carcelén), Santo Domingo de los Colorados, Ambato, Cuenca, Machala, Guayaquil, Quito (Av. Colón) y Portoviejo.

El representante legal y autoridad de la matriz es el Presidente Ejecutivo Corporativo, mientras que en cada ciudad existe un gerente regional.

3.1.5.1. Sede Central

Está ubicada al sur de la capital de la república en una extensión de unos 1000 metros cuadrados, consta de dos edificios, bodegas y la planta industrial.

En los edificios funcionan los diferentes departamentos que conforman el área administrativa de la empresa, las bodegas son de materia prima y producto terminado. La planta industrial esta distribuida en caramelería, grageas, chupetería y la nueva que es de chocolates.

Da cabida a mas de 700 empleos entre personal de planta, fuerza de ventas y personal administrativo. La sede central es la parte medular de Confiteca, donde parte la planificación de la producción, la logística, el sistema de información.

Desde aquí se traza toda la estrategia y las políticas a utilizar en todo el país para poder lograr los objetivos de la compañía.

3.1.5.2. Sucursales

Las sucursales están distribuidas estratégicamente en todo el país, en las principales ciudades. La función de estas agencias es brindar el soporte y apoyo a los vendedores de la zona circundante, en cuanto a abastecimiento de productos y recopilación de documentos para sustentos legales.

También recopila la información de ventas diariamente y a su vez la envía hacia la matriz donde se centralizan los datos de todas las regionales.

Consta administrativamente de un jefe regional, una asistente, supervisores de zona y la fuerza de ventas.

3.1.6. SISTEMA DE DISTRIBUCIÓN

Confiteca tiene dos modalidades de distribución claramente definidas y son:

3.1.6.1. Preventa

Es una forma de distribución en la cual el agente de ventas toma pedidos ya sea de manera manual o con un equipo móvil (palm o hand held) en el punto de venta. Estos pedidos recopilados en el día son entregados al área administrativa de logística, para ser procesados y facturados de acuerdo a la disponibilidad de inventario del producto. Al siguiente día hábil, son despachados hacia el cliente.

3.1.6.2. Autoventa

Es la otra modalidad de distribución que consiste en que cada agente de ventas se moviliza en un pequeño furgón cargado de productos, constituyéndose en una bodega móvil. Visita a cada cliente previamente asignado, para tomar el pedido, entregar el producto y facturar en ese mismo momento lo despachado.
Cada vendedor maneja 15 itinerarios que constituyen una ruta, existen 111 rutas en todo el país que son cubiertas por la fuerza de ventas.

3.2. SISTEMAS DE INFORMACIÓN

3.2.1. SISTEMA ERP.

El sistema ERP (Enterprise Resource Planning), integra los procesos relevantes de la empresa, el departamento de Sistemas en los años 1999-2000 desarrolla e implementa un nuevo sistema que cumpla con las necesidades y requerimientos de la compañía. Este sistema se denomina Sistema de Información Administrativa y de Gestión – SIAG XXI cuyos objetivos principales son:

- Ser un sistema eficiente para la organización, y adaptado a las necesidades del cliente externo como interno.

- Apoyar a la Administración y comunicación Inter-departamental e inter-empresarial, mediante la implementación de tecnología capaz de estructurar con eficiencia una organización cero papeles.

3.2.1.1. Características del Sistema ERP.

Las características más relevantes de este sistema transaccional se describen a continuación:

- Arquitectura Cliente – Servidor.
- Desarrollado en un ambiente Windows con herramientas gráficas que facilitan su operación.

Figura 3.2. Menú principal del sistema ERP.[42]

- Sistema totalmente modular.
- Maneja un concepto básico de "multimoneda" cuyo principio es transformar cualquier transacción, a cualquier tipo de moneda en el cual sea utilizado, de manera que su adaptación sea completa.
- Integrar las operaciones propias de la empresa tanto desde el área de producción como la de comercialización.
- Posibilita la centralización de la información.
- Un sistema con ayudas en línea en cada módulo que lo conforma, de manera que el usuario final, pueda acudir al mismo y le posibilite solucionar cualquier inquietud que tenga en cuanto a la operación del mismo.

[42] Fuente: Confiteca.

- Control de acceso a los módulos, mediante un sistema de administración de perfiles de usuario que permita o niegue el acceso a información autorizada.
- Permite emitir reportes de auditoria de acceso de ingreso o modificación de la información.

3.2.1.2. Módulos del Sistema ERP

- **Subsistema de Consistencia de datos**

Presentar a través de reportes las novedades o inconsistencias que hayan ocurrido en las diferentes operaciones entre los módulos; ayudan por tanto en la auditoria de información del sistema.

- **Subsistema de Devoluciones**

Administrar y controlar la gestión de devoluciones de la bodega de cuarentena tanto de producto terminado, de mercadeo y de insumos.

- **Subsistema de Ingresos a Producción**

Automatizar la gestión de ingresos de la bodega de producción tanto de producto terminado como productos reempacados.

- **Subsistema de Lista de Materiales**

Administrar y controlar los componentes (materia prima, materiales, semielaborados e insumos) que conforman un producto.

- **Subsistema de Operaciones Hand Held**

Recibir y enviar la información de los vendedores, en su labor de venta cuando utilizan los equipos móviles o de mano (hand held) en la captura de datos. Básicamente este módulo se lo conoce como una INTERFAZ entre el sistema central y el equipo de mano.

- **Subsistema de Cuentas por Pagar**

Administrar y controlar las obligaciones de la empresa hacia sus proveedores mediante procesos automatizados.

- **Subsistema de Cartera**

Administrar y controlar las obligaciones de los clientes con la empresa mediante procesos automatizados.

- **Subsistema de Compras**

Realizar el ingreso y control de órdenes de compras locales o importadas, a fin de realizar un seguimiento de los requerimientos de las diferentes áreas de la compañía.

- **Subsistema de Contabilidad**

Registrar y controlar las transacciones contables definidas en el plan de cuentas, el mismo que permitirá la emisión de informes contables que conlleven a determinar la situación financiera-contable de la empresa.

- **Subsistema de Estadísticas**

Recopilar y organizar la información cuantitativa de módulos de inventarios y ventas, de manera que permita realizar cálculos estadísticos de los datos interrelacionados entre sí, para su análisis y apoyo a las decisiones gerenciales.

- **Subsistema de Facturación**

Permitir el ingreso y control de facturas y devoluciones de mercancía dentro del proceso de ventas. Mantiene una relación estrecha con el módulo de inventarios.

- **Subsistema de Inventarios**

Realizar un control de los inventarios, logrando un efectivo monitoreo del flujo de existencias de los diferentes tipos de productos que tiene la empresa como productos terminados, materias primas, materiales, repuestos, semielaborados y misceláneos.

- **Subsistema de Ruteros**

Administrar la información básica de los clientes como su código, nombre, dirección, tipo de cliente, tipo de negocio, etc; de una forma sencilla y efectiva.

- **Subsistema de Tesorería**

Registrar y controlar los pagos y cobros en efectivo o cheque de las obligaciones hacia los proveedores y de los clientes.

- **Subsistema de ventas**

Registrar y controlar los pedidos tanto de mercado local como de exportación, para que luego de un proceso de logística de abastecimiento poder despachar todos y cada uno de ellos.

3.2.2. SISTEMA DE RECURSOS HUMANOS

Existen básicamente dos módulos que conforman el sistema de RRHH en la empresa siendo:

- El sistema de control de personal – SISPER
- El subsistema de nómina

3.2.2.1. Sistema de control de personal – SISPER

Permitir al Jefe de Recursos Humanos de la organización, llevar un control diario de las horas: de entrada, salida, almuerzo, al 25%, al 50% y al 100% que ha laborado un empleado.

3.2.2.2. Sistema de Nómina

Administrar y controlar de forma automatizada los pagos de haberes y prestaciones de todos los empleados de la compañía.

3.2.3. SISTEMA DE APOYO A DECISIONES

Confiteca tiene instalado Power Play, que es un software utilizado por personas de niveles estratégicos y tácticos, en el análisis de la información y toma de decisiones. Se caracteriza por ser una poderosa herramienta OLAP (Online Analytical Processing) que permite a los usuarios explorar grandes volúmenes de datos sumarizados con un tiempo de respuesta muy veloz. Tanto usuarios de nivel táctico como usuarios de áreas de negocios, pueden hacer sus propios análisis multidimensionales, crear reportes y compartirlos para facilitar la toma de decisiones.

Power Play genera sus propios cubos multidimensionales utilizando para ello una opción propia denominada Transformer como herramienta de modelado. Estos cubos (archivos) son sets de datos que contienen decenas de millones de registros consolidados y cientos de miles de categorías (miembros), incluyendo también reglas de negocio y cálculos.

Las principales características de esta herramienta son:

- Modelar datos multidimensionales es muy sencillo para el personal técnico del área de sistemas.
- Permite combinar varias fuentes de datos, como por ejemplo información de ventas y de saldos.
- Tiene dos formas de analizar la información:
  a) Visualizador únicamente de los datos.
  b) Reporteador, que permite al usuario final crear sus propios informes.
- Permite combinar sus características con Excel, de manera que el usuario pueda potencializar las funciones que dicha hoja de cálculo le ofrece.
- La información es revisada de manera remota desde la red WAN que posee Confiteca Quito con sus sucursales y tiene la posibilidad de acceso desde Internet con el uso de un navegador (Explorer, Netscape, etc.)

3.2.3.1. Descripción básica de los cubos de información en Power Play

Desde la adquisición e implementación de Cognos – Power Play en Confiteca, el área de Sistemas ha ido incorporando nuevos cubos de información, de acuerdo a las necesidades de los usuarios finales. Básicamente, la tendencia de entregar información gerencial a través de esta herramienta, se lo realiza por áreas (inventarios, ventas y cartera).

A continuación se describen los cubos que se tienen habilitados para el análisis gerencial de información de apoyo a decisiones.

- **Cubo de inventarios mensuales**

Almacenar la información de los saldos de todos los productos a fin de que puedan ser analizados, comparados y evaluados para servir de apoyo en la toma de decisiones en materia de abastecimiento a nivel nacional.

- **Cubo de ventas**

Registrar la información de ventas del día a día por vendedor y ciudades donde se distribuyen los productos, de forma que se pueda analizar y evaluar el desempeño de las ventas y facilitar la toma de decisiones gerenciales.

- **Cubo de cartera**

Registrar los saldos de las cuentas por cobrar por cliente, permitiendo realizar un control de las obligaciones pendientes y realizar el seguimiento que determine el monto de cada deuda hacia la empresa.

3.3. INFRAESTRUCTURA DE RED

3.3.1. RED LAN

Local Area Network (LAN), es la red de comunicaciones de Confiteca instalada dentro de su campus, la cual permite a los usuarios compartir información y recursos como: espacio en disco duro, impresoras, CD-ROM, acceder al correo electrónico, acceso al sistema integrado y al Internet. Para tener un mejor panorama se describe a continuación los elementos de la red LAN.

3.3.1.1.Arquitectura

La arquitectura de la red LAN de Confiteca es Ethernet o también conocida como IEEE 802.3, en este caso la computadora escucha el cable de la red y espera hasta un periodo de silencio para poder mandar un mensaje que choca en el tránsito con otros mensajes. Si se pasa del 1% de colisiones o 15% de utilización de cable, se dice que la red está saturada.

Existen dos tipos de ethernet 802.3 y que están vigentes en Confiteca:

- La ethernet 802.3 a 10Mbps.
- La ethernet 802.3 a 100Mbps.

3.3.1.2. Topología de red

La topología de la red LAN de Confiteca es de tipo estrella, en este caso todos los mensajes deben pasar a través de un dispositivo central de conexiones conocido como concentrador de cableado, que puede ser un HUB o SWITCH, el cual controla el flujo de datos. Tanto la matriz como las regionales tienen la misma topología de red.

3.3.1.3.Diagrama de red LAN en la Matriz

En la figura 3.3 se muestra la red LAN en la Matriz, donde se puede apreciar las conexiones entre los switch's de los pisos y el switch central del centro de cómputo. Para enlazar estos dispositivos se utiliza fibra óptica.

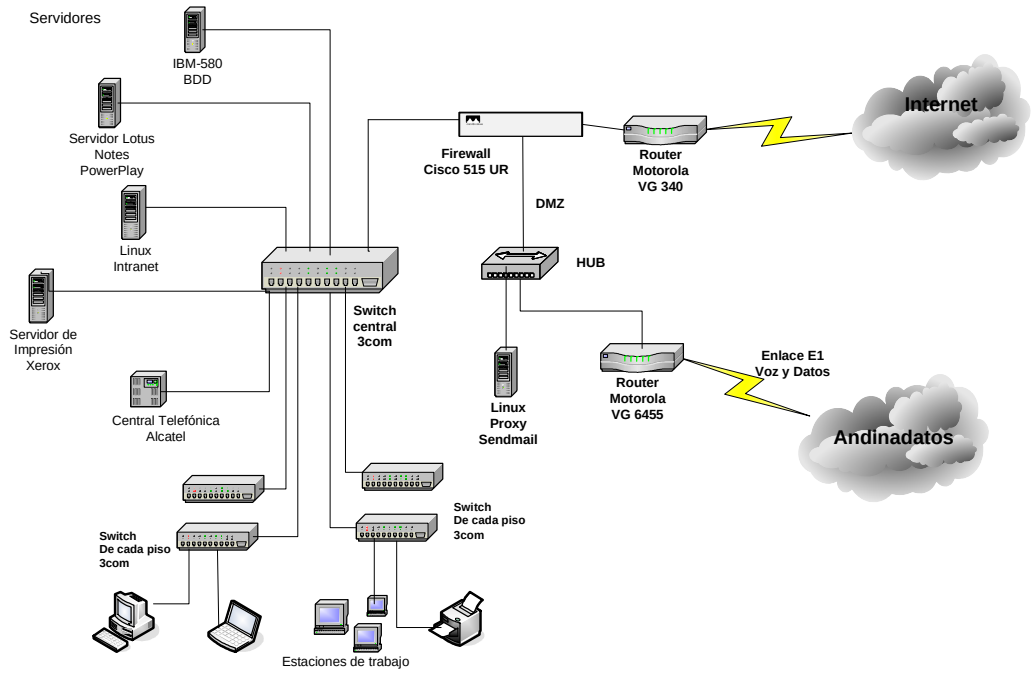

Figura 3.3. Red LAN Confiteca.[43]

[43] Fuente: Confiteca.

3.3.1.4. Diagrama de red LAN en las Regionales

En las regionales la red de Area Local en realidad es pequeña, constan de un número reducido de computadores y un servidor de base de datos.

Guayaquil es la regional más grande donde existe mayor cantidad de estaciones de trabajo, pero se mantiene un solo servidor de bases de datos.

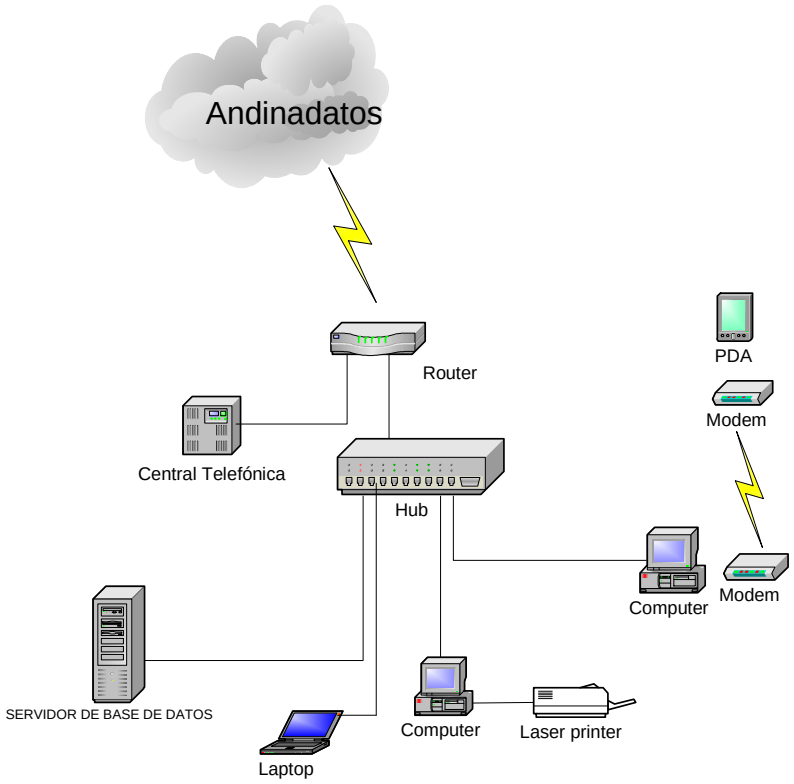

Figura 3.4. Red LAN en Regionales de Confiteca.[44]

3.3.1.5. Estaciones de trabajo

Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos.

[44] Fuente: Confiteca.

Cada usuario dispone de una PC que cumple con las necesidades, generalmente utilizadas para acceder al Sistema ERP, al correo electrónico, Internet e impresiones a través de la red.

Se tienen 183 estaciones de trabajo en la matriz y 40 distribuidas en todas las sucursales.

3.3.1.6. Servidores

Los servidores dentro de la red de Confiteca sirven para compartir sus recursos a todos los usuarios, son parte fundamental en la composición de la red, en ellos se guarda la información de la compañía. Existe 1 servidor en cada regional y 10 en la matriz sumando un total de 18 en todo el país.

Se tienen servidores de: correo corporativo, para los dominios, bases de datos, Internet, Power Play, entre otros. Más adelante se muestra las características y la aplicación de cada servidor.

De acuerdo a las necesidades, los usuarios utilizan el respectivo servidor, pero los que tienen la mayor afluencia de usuarios son los de correo electrónico, base de datos y el Proxy.

3.3.2. RED WAN

La red WAN (Wide Area Network) enlaza computadoras que se encuentran geográficamente dispersas con la sede central, en Confiteca la conexión entre las oficinas remotas se realiza a través de la red pública de teléfonos (dial-up) y también mediante enlaces con líneas dedicadas.

3.3.2.1. Topología

La red WAN de Confiteca presenta una topología centralizada en donde las operaciones de cómputo primarias se realizan en un solo lugar, las estaciones distantes alimentan de información a la central.

A menudo un sistema de este tipo es concebido como una red en estrella donde cada sitio remoto ingresa al sistema central vía una línea de comunicación.

3.3.2.2. Diagrama de Red WAN

En la figura 3.5 se aprecia la red WAN de Confiteca formada por las sucursales y la matriz a través de los enlaces de Andinadatos y dial-up, también consta la conexión a Internet con la empresa Impsat.

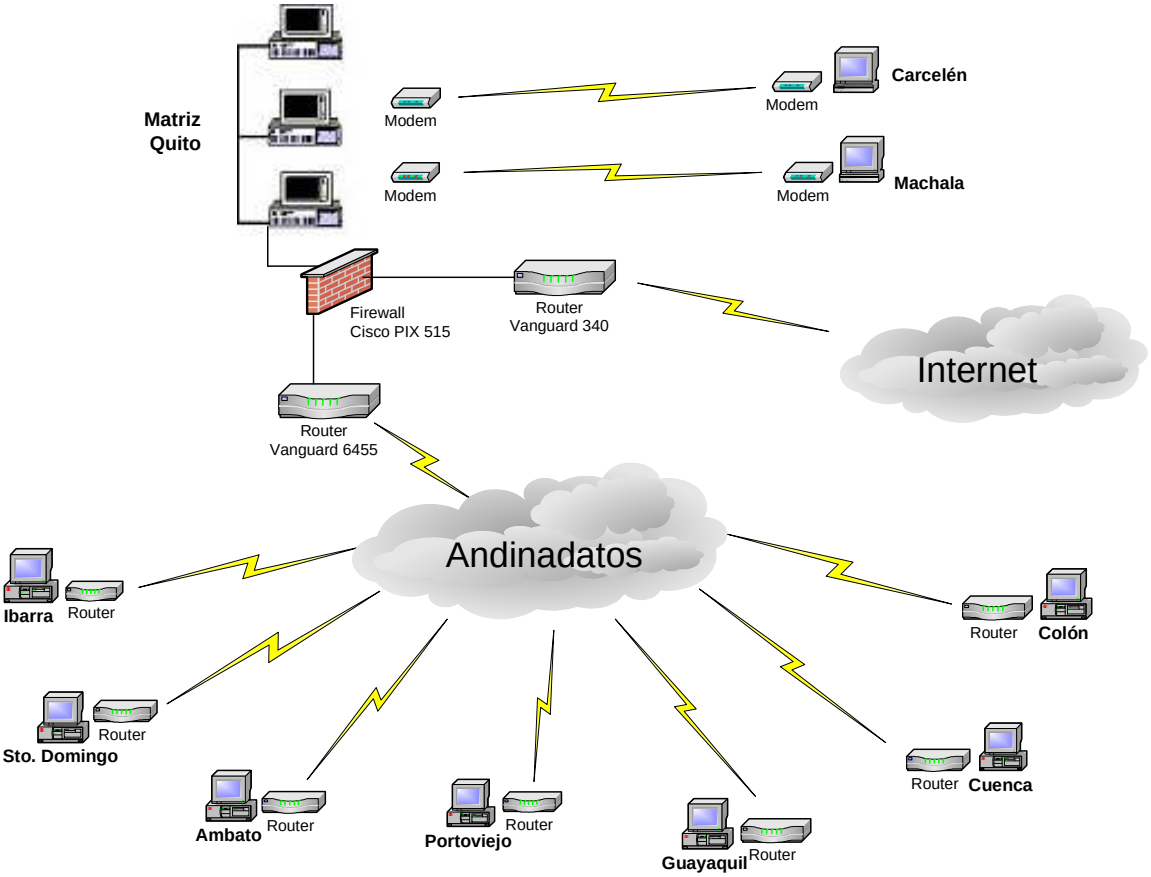

Figura 3.5. Red WAN de Confiteca. [45]

[45] Fuente: Confiteca.

3.4. INFRAESTRUCTURA DE TELECOMUNICACIONES

Para poder interconectar sus agencias con la oficina matriz ubicada en Quito, y éstas a su vez hacia el mundo entero, Confiteca cuenta con medios de transmisión en cada uno de estos puntos remotos. Dos sucursales usan la red telefónica pública y las demás agencias los sistemas privados de comunicaciones como son líneas dedicadas.

A continuación las tecnologías que utiliza la empresa para tener una comunicación global y oportuna.

3.4.1. LÍNEAS DEDICADAS

Se utilizan en la mayoría de las regionales, es una manera efectiva de conexión de redes, proporcionan conexiones dedicadas a tiempo completo y no utilizan una serie de conmutadores para completar la conexión. La calidad de esta línea es, a menudo, superior a la calidad de la línea telefónica.

Los enlaces dedicados los provee Andinadatos, son Clear Channel – Punto a Punto y utilizan la red TDM.

Como última milla, a cada agencia llega un par de cobre que se conecta a un modem de alta velocidad marca RAD de propiedad de Andinadatos.

Los routers le pertenecen a Confiteca así como también es responsable de la configuración y mantenimiento.

En la Matriz, como nodo central la velocidad es de 1 E1 canalizado (2.048 Mbps), donde cada time slot de 64 Kbps es asignado a la respectiva agencia de acuerdo a la velocidad de conexión contratada, como se muestra en la tabla 3.1.

SUCURSAL	TIME SLOT En E1 Matriz	Velocidad (Kbps)
SANTO DOMINGO	8	64
IBARRA	4	64
COLON UIO	5	64
GUAYAQUIL	2,3	128
CUENCA	7	64
PORTOVIEJO	9	64
AMBATO	10	64

Tabla 3.1. Distribución de líneas dedicadas en Confiteca.[46]

[46] Fuente: Andinadatos.

3.4.2. DIAL-UP ENTRE AGENCIAS

Se utiliza este tipo de conexión en agencias en las cuales no amerita tener una conexión dedicada, debido al volumen de información y número de usuarios de la red.

En este caso para conectarse a la sede central se utiliza SLIP (Serial Line Internet Protocol), es un protocolo muy simple diseñado hace mucho tiempo y es meramente un protocolo de entramado de paquetes. Define una secuencia de caracteres que sirven de trama a los paquetes IP en una línea serie.

SLIP es un protocolo que permite utilizar el TCP/IP en una línea telefónica por medio de un módem. Ambos ordenadores en un enlace SLIP necesitan conocer la dirección del otro para el encaminamiento.

Se requieren dos modem's, el emisor y el receptor con sus respectivas líneas telefónicas y configurar la conexión SLIP en los servidores tanto de la matriz como de la sucursal.

3.4.3. DIAL-UP PARA HAND HELD

Es utilizado para transmitir la información de las ventas diarias efectuadas por un vendedor de la empresa, esta persona generalmente trabaja en una ciudad distante, por lo tanto no puede acercarse con regularidad a la oficina de la regional a la que pertenece.

Para solucionar este problema de movilización de los vendedores, se optó por programar al hand held con comandos AT de un modem externo que será el emisor, en la sucursal respectiva existe un modem receptor destinado a atender las conexiones remotas.

De esta forma al terminar el día, uno o más agentes pueden utilizar esta opción para transmitir información de todas sus transacciones hacia la regional y también puede recibir actualización de precios, inventario, cartera, etc.

Se consiguen velocidades de 9600 bps como promedio dependiendo de la distancia y calidad de las líneas telefónicas.

Esta modalidad de conexión se tiene implementada en todas las agencias del país, permitiendo tener información de las ventas en forma oportuna para tomar decisiones por parte de los directivos de la empresa.

3.4.4. CONEXIÓN A INTERNET

Para acceder al servicio de Internet, la corporación mantiene una conexión permanente de banda ancha de 128/256 Kbps con la empresa Impsat.
Esta conexión es aprovechada por casi todas las agencias del país, en el caso de las regionales, utilizan las líneas dedicadas para conectarse al servidor Proxy que está en la matriz, de esta manera, usuarios de distintas ciudades se conectan al Internet sin tener que pagar un costo adicional por este servicio.

3.4.5. VOZ SOBRE IP Y FRAME RELAY

Voz sobre IP (VoIP) es una tecnología que permite hacer llamadas de voz utilizando una red de datos como Internet o las redes internas de las empresas. Las ventajas de esta tecnología son evidentes, además este sistema posibilita comunicarse con cualquier lugar del mundo.
Confiteca utiliza VoIP con sus filiales de Perú y Colombia a través de Internet mediante un Gateway en cada país, los equipos utilizan una IP pública y se conectan a la central telefónica para que la persona que llama pueda marcar la extensión deseada.
Las sucursales dentro del país que tienen líneas dedicadas también transmiten voz dentro de la red de datos sin cargo adicional mediante las tarjetas FX de los ruteadores, propiamente esta tecnología es conocida como Voz sobre Frame Relay (VoFR).
Las centrales telefónicas se conectan directamente a la tarjeta FX que disponen de dos puertos, se tiene por lo tanto dos líneas internas para comunicarse entre agencias.
Una desventaja de este tipo de transmisión de voz, es que la calidad suele ser un poco inferior a la telefonía tradicional, porque la voz viaja en paquetes y eso puede causar la demora o pérdida de algún paquete.

La calidad en la voz también está limitada por el ancho de banda que dispongan las agencias y mucho tiene que ver también la forma de conexión a Internet.

3.5. PLATAFORMA DE SOFTWARE Y HARDWARE

3.5.1. SISTEMA OPERATIVO DE RED

Es el sistema (Software) que se encarga de administrar y controlar en forma general la red, para esto tiene que ser un sistema operativo multiusuario.
El Sistema operativo de red que se utiliza en Confiteca es Microsoft Windows, el esquema de la red Microsoft trabaja en modo de dominio, soporta el protocolo TCP/IP y proporciona una interfaz amigable al administrador de la red.

3.5.2. ESTACIONES DE TRABAJO

Para las estaciones de trabajo se emplea sistemas operativos como Windows 2000, Windows XP, Windows NT, Windows ME, Windows 95, Windows 98, además de presentar una interfaz de fácil manejo a los usuarios, proporciona a éstos el soporte para ejecutar el conjunto de aplicaciones que cumplen con los requerimientos de información y trabajos que se manejan en Confiteca.
En la tabla 3.2, se aprecia la distribución de cada uno de los sistemas operativos que se utilizan, mientras que en la tabla 3.3 la distribución del hardware.

SISTEMA OPERATIVO	CANTIDAD
Windows 95	38
Windows 98	46
Windows ME	13
Windows NT	2
Windows 2000	67
Windows XP	57
TOTAL	223

Tabla 3.2. Sistema operativo de estaciones de trabajo.[47]

[47] Fuente: Confiteca.

Modelo	Número de máquinas
Pentium I	2
Pentium II	72
Pentium III	80
Pentium IV	69
Total :	223

Tabla 3.3. Hardware de Estaciones de Trabajo.[48]

3.5.3. APLICACIONES DE USUARIO

El software de aplicaciones está formado por programas informáticos que se comunican con los usuarios de la red y permiten compartir información y recursos.

Para que los usuarios puedan realizar su trabajo de la mejor manera y de acuerdo al rango o las funciones que desempeña, se le instala todo o parte del software listado a continuación: Microsoft Office 97/2000/XP, Internet Explorer, Lotus Notes 5.0, Unify Vision 8.0 (Sistema ERP), Norton Antivirus, Winzip, Adobe Acrobat.

3.5.4. HARDWARE DE RED

Son aquellos dispositivos que se utilizan para interconectar a los componentes de la red, serían básicamente las tarjetas de red y el cableado entre servidores y estaciones de trabajo, así como los cables para conectar los periféricos.

3.5.4.1.Tarjeta de Interfaz de Red

Para pertenecer a la red ethernet, cada computadora tiene instalada una tarjeta de interfaz de red (Network Interface Card, NIC) y el software adecuado para que la tarjeta funcione. Normalmente las tarjetas deben enviar y recibir las tramas.

Los controladores son de distintos fabricantes y existen en velocidades de transmisión de 10 Mbps en poca cantidad y de 100 Mbps en su gran mayoría.

[48] Fuente: Confiteca.

3.5.4.2.Cableado

La empresa dispone de cableado estructurado, capaz de interconectar los equipos que forman la red, por ejemplo las estaciones de trabajo con los servidores, entre las estaciones de trabajo y el switch central se tiene cable de par trenzado UTP categoría 5e, mientras que entre los switch de cada piso y el switch central se utiliza fibra óptica.

3.5.5. HARDWARE Y SOFTWARE DE SERVIDORES

Ciudad	Marca	Modelo	Sistema Operativo	Uso
Quito	IBM	RS/6000 F80	AIX 4,3,3	Bases de datos principales
Quito	IBM	RS/6000 39H	AIX 3,2,5	Bases de datos especiales
Quito	IBM	RS/6000 580	AIX 4,3,3	Bases de datos de desarrollo
Quito	IBM	Netfinity 3000	Windows 2000 SERVER	Antispam
Quito	Intel	SBT2 – PIII	Windows 2000 SERVER	Control de accesos
Quito	Intel	SGB2 – PIV	Windows 2003 SERVER	Sistema de información gerencial
Quito	Intel	SBT2 – PIII	Linux Red Hat 9,0	Correo electrónico
Quito	Intel	Pentium III	Windows XP Professional	Licencias de aplicaciones
Quito	Clone	Pentium IV	Windows 2000 SERVER	Servidor de impresiones
Quito	Clone	Pentium III	Linux Red Hat 9,0	Proxy
Guayaquil	Intel	SBT2 – PIII	SCO UNIX 5,0,5	Base de datos
Machala	Compaq	Pentium	SCO UNIX 5,0,5	Base de datos
Portoviejo	Intel	SBT2 – PIII	SCO UNIX 5,0,5	Base de datos
Ibarra	Intel	SBT2 – PIII	SCO UNIX 5,0,5	Base de datos
Ambato	Intel	SBT2 – PIII	SCO UNIX 5,0,5	Base de datos
Sto. Domingo	Intel	SBT2 – PIII	SCO UNIX 5,0,5	Base de datos
Quito – Norte	Intel	SBT2 – PIII	SCO UNIX 5,0,5	Base de datos
Cuenca	Intel	SBT2 – PIII	SCO UNIX 5,0,5	Base de datos

Tabla 3.4. Hardware y Software de servidores.[49]

[49] Fuente: Confiteca.

3.5.6. DISPOSITIVOS INTERCONECTANTES

Constan los equipos utilizados para la interconexión en las redes LAN y WAN, como son ruteadores, modems, firewall, gateway VoIP y switchs.

Ubicación	Marca	Modelo	Aplicación
Quito	AT&T	paradine	SLIP
Quito	UsRobotics		SLIP
Carcelén	Motorota	V3600	SLIP
Machala	Motorota	3266	SLIP
Quito	Motorola	V3600	receptor Hand Held remoto
Quito	Motorola	3266	receptor Hand Held remoto
Guayaquil	Motorola	3266	receptor Hand Held remoto
Cuenca	Motorola	3266	receptor Hand Held remoto
Ambato	Motorola	3266	receptor Hand Held remoto
Ibarra	Motorola	3266	receptor Hand Held remoto
Sto. Domingo	Motorola	3266	receptor Hand Held remoto
Portoviejo	Motorola	3266	receptor Hand Held remoto
Esmeraldas	Motorola	V3600	emisor Hand Held remoto
Quevedo	Motorola	3266	emisor Hand Held remoto
Riobamba	Racal		emisor Hand Held remoto
Puyo	Motorola	3266	emisor Hand Held remoto
Guaranda	Motorola	V3600	emisor Hand Held remoto
Salinas	Motorola	V3600	emisor Hand Held remoto
Babahoyo	Motorola	3266	emisor Hand Held remoto
Milagro	Motorola	3266	emisor Hand Held remoto
Macas	Motorola	V3600	emisor Hand Held remoto
Piñas	Motorola	V3600	emisor Hand Held remoto
Tulcán	Motorola	3266	emisor Hand Held remoto
San Gabriel	Motorola	3266	emisor Hand Held remoto
Otavalo	Motorola	V3600	emisor Hand Held remoto
Latacunga	Motorola	3266	emisor Hand Held remoto
Chone	Motorola	V3600	emisor Hand Held remoto
Manta	Motorola	V3600	emisor Hand Held remoto
Jipijapa	Motorola	V3600	emisor Hand Held remoto
Ventanas	Motorola	3266	emisor Hand Held remoto

Tabla 3.5. Listado de Modem's instalados en todo el país.[50]

[50] Fuente: Confiteca.

Ubicación	Marca	Modelo	Utilidad
Quito	Vanguard	6455	WAN
Quito	Vanguard	340	Internet
Ibarra	Vanguard	300	WAN
Sto. Domingo	Vanguard	320	WAN
Colón UIO	Vanguard	300	WAN
Ambato	Vanguard	320	WAN
Portoviejo	Vanguard	320	WAN
Cuenca	Vanguard	320	WAN
Guayaquil	Vanguard	320	WAN
Quito	Cisco	515	Firewall
Quito	AddPac	AP200	VoIP

Tabla 3.6. Dispositivos Interconectantes de la red WAN.[51]

Ciudad	Marca	No. Puertos	Ubicación
Quito	3COM	24(10/100Mbps)	Centro de Cómputo
Quito	3COM	24(10/100Mbps)	Centro de Cómputo
Quito	3COM	24(10/100Mbps)	Centro de Cómputo
Quito	3COM	24(10/100Mbps)	Centro de Cómputo
Quito	3COM	24(10/100Mbps)	Segundo piso
Quito	3COM	24(10/100Mbps)	Segundo piso
Quito	3COM	24(10/100Mbps)	Planta Industrial
Quito	3COM	24(10/100Mbps)	Planta Industrial
Quito	3COM	24(10/100Mbps)	Edificio Ventas
Quito	GENIUS	16(10/100Mbps)	Edificio Ventas
Quito	3COM	24(10/100Mbps)	Edificio Ventas
Cuenca	GENIUS	16(10/100Mbps)	Rack de comunicaciones
Ibarra	ENCORE	8(10/100Mbps)	Rack de comunicaciones
Guayaquil	3COM	8(10/100Mbps)	Rack de comunicaciones
Guayaquil	3COM	24(10/100Mbps)	Rack de comunicaciones
Guayaquil	3COM	24(10/100Mbps)	Rack de comunicaciones
Portoviejo	CNET	8(10/100Mbps)	Rack de comunicaciones
Ambato	3COM	12(10/100Mbps)	Rack de comunicaciones
Machala	CNET	8(10/100Mbps)	Rack de comunicaciones
Carcelén	ENCORE	8(10/100Mbps)	Rack de comunicaciones
Sto. Domingo	ENCORE	8(10/100Mbps)	Rack de comunicaciones
Colón UIO	3COM	24(10/100Mbps)	Rack de comunicaciones

Tabla 3.7. Listado de equipo de conectividad LAN.

[51] Fuente: Confiteca.

3.6. REQUERIMIENTOS Y NECESIDADES DE LA EMPRESA

A continuación las principales necesidades de Confiteca que actualmente presenta y que deberán ser atendidas oportunamente.

3.6.1. RENOVACIÓN TECNOLÓGICA

La evolución de la tecnología, particularmente de la electrónica, los sistemas informáticos y las telecomunicaciones ha obligado a las empresas a estar actualizadas constantemente, en Confiteca se podría tomar en cuenta lo siguiente:

- Es necesario actualizar las estaciones de trabajo que cuentan con procesadores Pentium I y Pentium II, por la escasez de repuestos no resulta conveniente mantenerlos, además sus características han perdido terreno frente al avance de los sistemas operativos y aplicaciones.
- Existen todavía regionales que utilizan un HUB como concentrador de red, lo que hace que el rendimiento de la red LAN no sea ideal. Por lo tanto se deberá cambiarlos por Switch's.
- Actualización de Routers, ya que existen modelos que ya no tienen repuestos como por ejemplo el Vanguard 300. Se está incorporando el modelo Vanguard 340 que incluso soporta IPSec y se lo podría utilizar para una VPN en caso de implementarla con ruteadores.
- Incremento de Firewalls en las sucursales para brindar mayor seguridad a la información, debido a que tienen datos igual de importantes y además pueden ser utilizados como pasarela hacia la matriz en caso de un ataque informático.
- Nuevos servidores de bases de datos, algunas sucursales e incluso la matriz disponen de equipos muy antiguos como Compaq Presario (Pentium I) y el IBM RS/6000 39H. Se corre el riesgo de que se dañen definitivamente y se pierda información muy importante.
- Incrementar la capacidad de los UPS, el número de servidores del centro de cómputo aumentó y el sistema in-interrumpido de energía está llegando al 100 % de su capacidad.

- La tecnología de PDA's también necesita de una renovación, se ha utilizado desde 1996 hand held marca Telxon, pero como esta marca desapareció, se está reemplazándolos por PALM con mejores características de memoria, video, procesador, aplicaciones.

3.6.2. REDUCCIÓN DE COSTOS EN TELECOMUNICACIONES

En nuestro país el costo de las telecomunicaciones y en particular para las empresas sigue siendo elevado.

En Confiteca se ha establecido una reducción máxima (o minimización) de sus costes de funcionamiento, de forma que ello no pueda afectar de manera alguna al negocio.

La administración efectiva de los gastos de telecomunicaciones e informática ayuda a determinar el servicio que deberá ser reducido y que pueda generar ahorro de divisas.

Para la minimizar el rubro que representa este servicio a la compañía se puede destacar los siguientes puntos:

- El costo que representa el pago de líneas dedicadas es sin duda el mayor, de ahí la necesidad de buscar proveedores mas competitivos.
- Reducir el consumo de las líneas telefónicas convencionales para la comunicación entre agencias de la corporación, se está logrando con la utilización de VoIP.
- Buscar alternativas para la conexión de Internet, por ejemplo nuevas formas de conexión u otros proveedores que ofrezcan un buen servicio pero menor costo, manteniendo las mismas características del enlace.
- Estudiar nuevas tecnologías de conectividad como por ejemplo VPN, satélites, microondas. Que signifiquen un ahorro significativo para la empresa.

3.6.3. INCREMENTAR SEGURIDADES DE LA INFORMACIÓN

Al utilizar el sistema en una red estará a un nivel más alto de riesgo que si no estuviese conectado a una. Además de atentados brutales a los ficheros de contraseñas y usuarios sin acceso apropiado, la presencia de un sistema en una red más grande aumenta la oportunidad de que ocurra un problema de seguridad y la forma posible en que pueda ocurrir.

La red LAN de Confiteca presenta el esquema de dominios que aporta grandes ventajas en la seguridad de la red gracias al control de usuarios y privilegios de accesos a recursos del dominio, también se dispone de un Firewall para aislar la red de ataques externos.

Pero se necesita implementar más seguridades, que puede ser un sistema de detección de intrusos (IDS) y fundamentalmente políticas que ayuden a contrarrestar ataques internos o externos.

3.6.3.1.Políticas de Seguridad

La verdadera seguridad de un sistema va más allá de la instalación de un Firewall o una actualización más reciente, la configuración de un cierto fichero, o la cuidadosa administración del acceso de los usuarios a los recursos de sistema. Es una manera de ver las diferentes amenazas que acechan al sistema y lo que se está dispuesto a hacer para evitarlas.

“Ningún sistema es totalmente seguro a menos que esté apagado (y aun así, es posible que se lo roben)”[52].

Cada vez que el sistema esté encendido puede ser atacado, desde una broma hasta un virus capaz de destruir el hardware, a la posibilidad que los datos sean borrados.

Pero con una actitud apropiada además de algunas buenas herramientas, se puede gozar de un sistema sano sin problemas de seguridad.

Por lo tanto es muy importante implementar en Confiteca un conjunto de políticas de seguridad, que sea una guía para todo el personal de la corporación, de como utilizar la información de la compañía y los cuidados que se deben tener con ella.

[52] Fuente: http://universalvision.galeon.com/soporte.htm

3.6.3.2.Políticas de Uso del Internet

En la actualidad no existen políticas de uso del servicio de Internet, esto implica que los usuarios pueden visitar sitios web pornográficos, páginas web no confiables, bajarse algún programa que contenga un virus que se propague por la red o sufrir ataques de algún software espía.

Por lo tanto se deberá elaborar un conjunto de políticas para que el usuario utilice este servicio de manera ética y correcta, de tal forma que la empresa no corra ningún riesgo.

A continuación una lista de los posibles usos no-permitidos del Internet dentro de la empresa.

- Acceder a cualquier tipo de material con fines particulares, por ejemplo un empleado que usa la computadora para bajar un programa para uso personal, para enviar o recibir correspondencia privada o para pedir información sobre productos comerciales.
- Acceder a cualquier tipo de material ofensivo, discriminatorio o ilegal, la más grave de las ofensas si es voluntaria y consciente, porque implica desconocer no sólo las reglas de uso de la Internet, sino las la empresa misma.
- Poner a disposición de otros empleados material no permitido.

3.6.3.3. Políticas de Uso de Correo Electrónico

De igual forma el intercambio de correo electrónico desde y hacia la empresa, no fluye bajo ninguna regla que limite algún parámetro, al no tener políticas establecidas el usuario puede enviar correos de cualquier índole.

El único control que se tiene es el tamaño de los adjuntos, el límite es de 2 Mbytes, pero se dan casos de usuarios que no toman en cuenta este limitante y lógicamente colapsa el servidor de correo electrónico.

Todos los usuarios del servicio de correo electrónico de Confiteca deberían conocer y respetar las condiciones generales, de no hacerlo se debería plantear sanciones.

Dentro de las políticas de correo electrónico se podría tomar en cuenta:

- Protección de claves asociadas a los buzones de correo electrónico.
- Responsabilidad del mal uso de sus cuentas de correo, ya sea por negligencia o por una utilización abusiva del servicio.
- Las personas que violen los sistemas de seguridad del correo electrónico.
- Envío de contenidos ilegales, como apología del terrorismo, programas piratas, pornografía infantil, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general, etc.
- Difusión masiva de mensajes, en especial de publicidad no solicitada. Cualquier tipo de ataque encaminado a entorpecer o dificultar el servicio de correo u otros servicios. Se incluyen los conocidos ataques a través del envío de un número alto de mensajes por segundo.

3.6.4. INTRANET Y EXTRANET

Confiteca es una compañía que ha crecido, y surge la necesidad de recopilar en una plataforma todos aquellos datos que puedan tener interés para directivos y empleados.

Esto se lograría con la implementación de una Intranet, donde se podrá centralizar todas las aplicaciones que utiliza el personal de la empresa.

En la Intranet serían factibles los siguientes módulos:

- Workflow.
- Acceso al sistema ERP.
- Correo electrónico (Webmail).
- Noticias y comunicados.
- Contactos.
- Tareas.
- Foros.
- Archivos.

Si se habla de la importancia de una Intranet, también hace falta una Extranet para realizar gestiones con organizaciones o personas externas como clientes importantes, proveedores y empresas aliadas.

Sería ideal tener una Extranet que permita a estos clientes preferenciales hacer sus pedidos directamente a través de una página web y en Confiteca procesar dicho pedido para su entrega inmediata.

De igual forma se podría tratar con ciertos proveedores, de modo que las órdenes de compra sean confirmadas y publicadas en un portal, así se eliminarían trámites burocráticos que demoran la compra de repuestos o materia prima.

Se podría pensar en los siguientes módulos para la Extranet:

- Catálogo de Productos.
- Tienda Virtual asociada con instituciones bancarias.
- Gestión de pedidos.
- CRM.
- Buscadores.

3.6.5. PLAN DE CONTINGENCIAS

En cualquier momento, la instalación informática de la empresa puede quedar total o parcialmente inoperativa como consecuencia de un siniestro fortuito.

Esta suspensión de las operaciones afecta directamente al negocio de la misma, así como su imagen, su base de clientes, etc.

Nunca se ha tomado en cuenta un desastre que pudiera generar la perdida total de información, hoy en día prácticamente todas las personas tienen acceso al Sistema Integrado de Confiteca por lo que un colapso o desaparición de éste, podría generar una paralización total o parcial de la empresa y consecuentemente pérdidas económicas que podrían ser cuantiosas.

En los últimos años han ocurrido daños de mediana gravedad que gracias a los respaldos sacados periódicamente se devolvió la funcionalidad del sistema en poco tiempo.

Confiteca siendo una empresa grande y que crece día a día, no debe quedarse de brazos cruzados ante un posible desastre informático que provocaría más de un problema.

Es así que es necesario empezar a crear un plan de contingencias, el cual será un documento guía para prevenir desastres y actuar con eficacia cuando ocurran.

3.7. DISEÑO DE POSIBLES IMPLEMENTACIONES VPN PARA LA EMPRESA COMERCIALIZADORA

Partiendo de la infraestructura tecnológica y física de Confiteca, se sugiere que los posibles escenarios de implementación de una Red Privada Virtual (VPN), sean los siguientes:

VPN Sitio a Sitio:

- Firewall (PIX) – Firewall (PIX).
- Router – Router.
- Servidor (Linux)–Servidor(Linux).

VPN de Acceso Remoto:

- Host – Firewall.
- Host – Servidor.

A continuación el detalle de cada escenario con algunas instrucciones básicas de instalación, requerimientos y configuración:

3.7.1. PIX TO PIX

Este escenario permitiría integrar las sucursales con la matriz utilizando Firewalls Cisco PIX como dispositivos esenciales para montar la VPN entre los distintos sitios de la empresa. En la matriz se dispone de un Cisco PIX 515 y sería necesario adquirir otro para cada agencia, en este caso particular se analiza la conexión entre 2 PIX, todo el tráfico entre los sitios es encriptada utilizando IPSec.

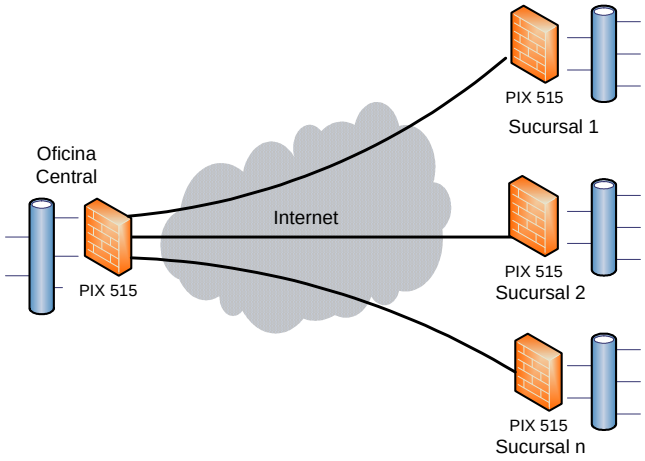

Figura 3.6. Escenario VPN PIX to PIX.

La tabla 3.8 resume el cripto rendimiento de cada modelo Cisco PIX security (utilizando 3DES y AES-128 con paquetes de 1400-bytes).

Modelo	Máximo de Túneles Sitio-a-Sitio y Usuarios Remotos	3DES Performance	AES-128 Performance
Cisco PIX 501	10	3 Mbps	4.5 Mbps
Cisco PIX 506E	25	15 Mbps	30 Mbps
Cisco PIX 515E with VAC+	2000	130 Mbps	130 Mbps
Cisco PIX 525 with VAC+	2000	145 Mbps	135 Mbps
Cisco PIX 535 with VAC+	2000	425 Mbps	495 Mbps

Tabla 3.8. Rendimiento de dispositivos Cisco PIX Security IPSec.[53]

Los aparatos Cisco PIX proveen hasta 16 niveles de roles administrativos customizables así que las empresas pueden conceder a los administradores y personal de operación el nivel apropiado de acceso para cada dispositivo (por ejemplo solo monitoreo, acceso solo lectura para la configuración, solo configuración VPN, o solo configuración Firewall).

3.7.1.1.Requerimientos

- Un Firewall Cisco PIX 515 en cada sucursal.
- Acceso a Internet en cada agencia.
- IP públicas para cada Firewall.
- Tarjeta aceleradora VPN (VAC).

[53] http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns142/netbr09186a00801f0a72.html

3.7.1.2.Configuración [54]

La configuración de IPSec en cada PIX debe variar solamente al poner la información del par y la convención de nombramiento elegidas para los crypto maps y transform sets. La configuración se puede verificar con los comandos **write terminal** o usando el **show**. Los comandos relevantes son **show isakmp**, **show isakmp policy**, **show access-list**, **show crypto ipsec transform-set**, y **show crypto map**. La información sobre estos y otros comandos del Firewall Cisco PIX se puede encontrar en la sección de Anexos.

IPSec puede ser configurado mediante los siguientes pasos:

- Configurar IKE para claves Precompartidas.
- Configurar IPSec.
- Configurar Network Address Translation (NAT).
- Configurar opciones del sistema PIX.

3.7.1.2.1. Configurar IKE para llaves Preshared

Habilitar IKE en las interfaces de terminación IPSec usa el comando **isakmp enable**. En este panorama, el interfaz exterior (outside) es el IPSec que termina el interfaz en ambos PIX. IKE sería configurado en ambos PIX, estos comandos demuestran solamente un PIX.

isakmp enable outside

También se debe definir las políticas de IKE que son utilizadas durante las negociaciones de IKE usando el comando **isakmp policy**. Al usar este comando, se debe asignar un nivel de la prioridad para identificar las políticas únicamente. En este caso, la prioridad más alta (valor 1) se asigna a la política, la política también se fija para utilizar una llave precompartida, el algoritmo de cálculo del uso MD5 para la autentificación de los datos, utiliza DES para Encapsulating

---

54 http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a0080094761.shtml#conf

Security Payload (ESP), usa Diffie-Hellman group 1, y fija el lifetime de la Asociación de seguridad (SA).

isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000

La configuración IKE puede ser verificada con el comando **show isakmp policy**.

Finalmente, hay que configurar la llave precompartida y asignar una dirección del par usando el comando **isakmp key**. La misma llave debería corresponder en los pares de IPSec cuando se usa llaves preshared. La dirección difiere, dependiendo de la dirección IP del par alejado, ejemplo:

*isakmp key ********** address 172.22.112.12 netmask 255.255.255.255*

3.7.1.2.2. Configurar IPSec

Se inicia IPSec cuando uno de los PIX recibe el tráfico que es destinado para el otro PIX dentro de la red. Este tráfico es denominado “tráfico interesante” y que necesita ser protegido por IPSec. Una lista de acceso se utiliza para determinar qué tráfico inicia las negociaciones de IKE e IPSec. La lista de acceso mostrada abajo de permite el tráfico para ser enviado de la red 10.1.1.x, vía el túnel de IPSec, a la red 172.16.1.x. La lista de acceso en la configuración del PIX opuesto refleja la misma.

access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0

El IPSec transform set, define la política de seguridad que usan los pares para proteger el flujo de datos. El IPSec transform es definido usando el comando **crypto ipsec transform-set.** Un nombre único se debe elegir para el transform fijado y hasta tres transforms se pueden seleccionar para definir los protocolos de seguridad de IPSec. Esta configuración utiliza solamente dos transforms: **esp-hmac-md5** y **esp-des**.

crypto ipsec transform-set chevelle esp-des esp-md5-hmac

Los crypto map instalan los IPSec SA's para el tráfico cifrado, para crear un crypto map, se debe asignar un nombre del mapa y un número de secuencia, y define los parámetros del crypto map. El crypto map "transam" mostrado debajo usa IKE para establecer IPSec SAs, cifra cualquier cosa que la acces-list 101, tiene un par del sistema, y utiliza el "chevelle transform-set" para decretar su política de la seguridad para el tráfico.

crypto map transam 1 ipsec-isakmp
crypto map transam 1 match address 101
crypto map transam 1 set peer 172.22.112.12
crypto map transam 1 set transform-set chevelle

Después de definir el crypto map, aplica el crypto map a la interface, la interface escogida podría ser la interfaz que termina IPSec.

crypto map transam interface outside

3.7.1.2.3. Configurar Network Address Translation (NAT)

Este comando dice al PIX no haga NAT a cualquier tráfico juzgado como interesante para IPSec. Así, todo el tráfico que empareja las declaraciones del comando de la lista de acceso es exento de los servicios NAT.

nat (inside) 0 access-list 101

3.7.1.2.4. Configurar Opciones de Sistema PIX

Porque todas las sesiones de entrada se deben permitir explícitamente por una lista de acceso o un conducto, el comando **sysopt connection permit-ipsec** se utiliza para permitir todas las sesiones IPSec autenticadas. Con IPSec el tráfico es protegido, el secundario del conducto chequea si podía ser redundante y pueda hacer fallida la creación del túnel. El comando **sysopt** contempla varias características de la seguridad y de la configuración del cortafuego PIX.

sysopt connection permit-ipsec

3.7.2. CISCO VPN CLIENT

El ejemplo en esta sección demuestra el uso de autenticación extendida, llave pre-compartida de la autentificación (Xauth), del modo de IKE para la autentificación de IKE entre un Firewall de PIX y un cliente seguro del Cisco VPN.

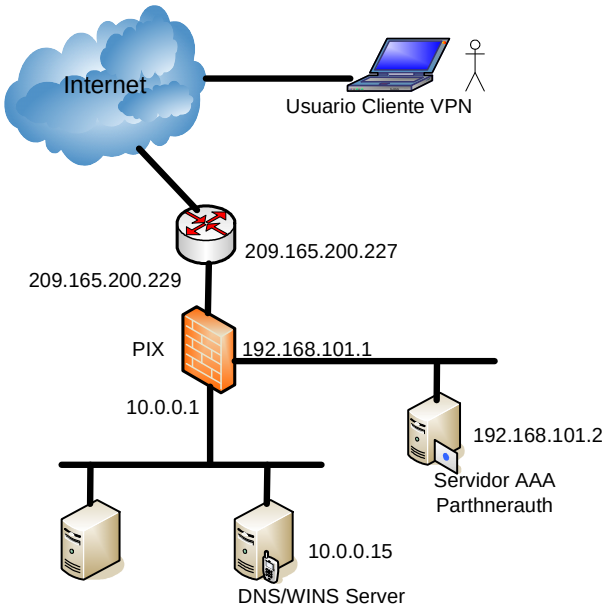

Figura 3.7. Acceso VPN Client.

3.7.2.1. Requisitos

- Un Firewall Cisco PIX 515.
- Software VPN Client.
- Un servidor AAA.
- Conexiones a Internet.

3.7.2.2.Configuración del PIX Firewall

Se debe seguir estos pasos para configurar el Firewall PIX para interoperar con el Cisco Secure VPN Client:

Paso 1. Definir parámetros relacionados AAA:

aaa-server TACACS+ protocol tacacs+

aaa-server partnerauth protocol tacacs+

aaa-server partnerauth (dmz) host 192.168.101.2 abcdef timeout 5

Paso 2. Configurar la política IKE:

isakmp enable outside

isakmp policy 8 encr 3des

isakmp policy 8 hash md5

isakmp policy 8 authentication pre-share

Paso 3. Configurar un comodín (wildcard), llave pre-shared:

isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0

Paso 4. Crear una lista de acceso que define las direcciones virtuales de los clientes VPN:

access-list 80 permit ip host 10.0.0.14 host 192.168.15.1

access-list 80 permit ip host 10.0.0.14 host 192.168.15.2

access-list 80 permit ip host 10.0.0.14 host 192.168.15.3

access-list 80 permit ip host 10.0.0.14 host 192.168.15.4

access-list 80 permit ip host 10.0.0.14 host 192.168.15.5

Paso 5. Configurar NAT 0:

nat 0 access-list 80

Paso 6. Configurar una transform set que define como será porotegido:

crypto ipsec transform-set strong-des esp-3des esp-sha-hmac

Paso 7 Crear un cripto map dinámico. Especifica cuales transform sets serán permitidos para esta entrada cripto map dinámico:

crypto dynamic-map cisco 4 set transform-set strong-des

Paso 8. Agregar el crypto map dinámico dentro de un crypto map estático:

crypto map partner-map 20 ipsec-isakmp dynamic cisco

Paso 9. Aplicar el crypto map a la interface outside:

crypto map partner-map interface outside

Paso 10. Habilitar Xauth:

crypto map partner-map client authentication partnerauth

Paso 11. Configurar IKE en modo config parámetros relacionados:
ip local pool dealer 192.168.15.1-192.168.15.5
isakmp client configuration address-pool local dealer outside
crypto map partner-map client configuration address initiate

Paso 12. Decirle al PIX para permitir implícitamente el tráfico:
sysopt connection permit-ipsec

3.7.2.3.Configurando Acceso Remoto VPN Client V1.1

Paso 1. Click en **Inicio>Programas>Cisco Secure VPN Client>Security Policy Editor**.

Paso 2. Click en Options>Secure>Specified Connections.

Paso 3. En la ventana **Network Security Policy**, click en **Other Connection** y entonces click en **Non-Secure**.

Paso 4. Click en **File**>**New Connection**. Renombrar New Connection. Por el ejemplo, **ToSanJose**.

Paso 5. Dentro de **Connection Security**, click en **Secure.**

Paso 6. Dentro de **Remote Party Identity and Addressing**, fijar en el panel de la derecha lo siguiente:
a. ID Type—Click en **IP address**.
b. Ingresar la IP del host interno dentro del PIX, son unidades internas que el VPN cliente tendrá acceso. Ingresar **10.0.0.14**.
c. Click en **Connect using Secure Gateway Tunnel**.
d. ID Type—Click en **IP address**.
e. Ingresar la IP de la interface outside del PIX Firewall. Ingresar **209.165.200.229**.

Paso 7. En la ventana **Network Security Policy**, click en **My Identity**. Fijar en el panel lo siguiente:

a. Select Certificate—Click **None**.

b. ID Type—Click **IP address**.

c. Port—Click **All**.

d. Local Network Interface—Click **Any**.

e. Click en **Pre-Shared Key**. Cuando aparezca el diálogo Pre-Shared Key, click en **Enter Key**. Ingresar **cisco1234** y click en **OK**.

Paso 8. En la ventana Network Security Policy, expander Security Policy y fijar lo siguiente:

a. Dentro de **Select Phase 1 Negotiation Mode,** click en **Main Mode**.

b. Selecccionar el **Enable Replay Detection**.

Tomar cualquier valor.

Paso 9. Click en **Security Policy**>**Authentication (Phase 1)**>**Proposal 1** y fijar:

a. Authentication Method—Click en **Pre-shared Key**.

b. Encrypt Alg—Click en **Triple DES**.

c. Hash Alg—Click en **MD5**.

d. SA Life—Click en **Unspecified** para aceptar el valor default.

e. Key Group—Click **Diffie-Hellman Group 1**.

Paso 10. Click en **Security Policy**>**Key Exchange (Phase 2)**>**Proposal 1** fijar:

a. Select the **Encapsulation Protocol (ESP)**.

b. Encryption Alg—Click en **Triple DES**.

c. Hash Alg—Click en **SHA-1**.

d. Encapsulation—Click en **Tunnel**.

Paso 11. Click en **File**>**Save Changes**.

El VPN client está activado ahora.

3.7.3. ROUTER TO ROUTER

Este escenario utiliza específicamente routers de marca Vanguard, ideal porque la empresa comercializadora cuenta con estos dispositivos en la mayoría de sus agencias, y le serviría para VPN Sitio a Sitio.

Esta solución ofrece una atractiva conectividad segura end-to-end en los ambientes donde prevalece el comercio electrónico, la transferencia de fondos electrónica o el tratamiento transaccional es crítico.

Los routers Vanguard 340, 340 Enhanced, 342, 6435 y 6455 soportan IPSec, son capaces de construir VPN's dentro del sistema operativo.

La implementación IPSec en esta línea permite tener soporte IPSec, a todos los productos Vanguard que tienen un zócalo de encryption (SIMM) en la placa base.

Utiliza encripción DES, Triple DES o Triple DES y AES, el Hashing es utilizado para calcular el resumen del mensaje para la autenticación AH o ESP.

La autentificación del par alejado se puede lograr con una clave Pre-compartida, en este caso el valor de la clave solo la conocen los dos equipos IPSec. La llave no se utiliza directamente como llave de cifrado, mejor actúa como origen para crear otros materiales claves para el cifrado y la autentificación.

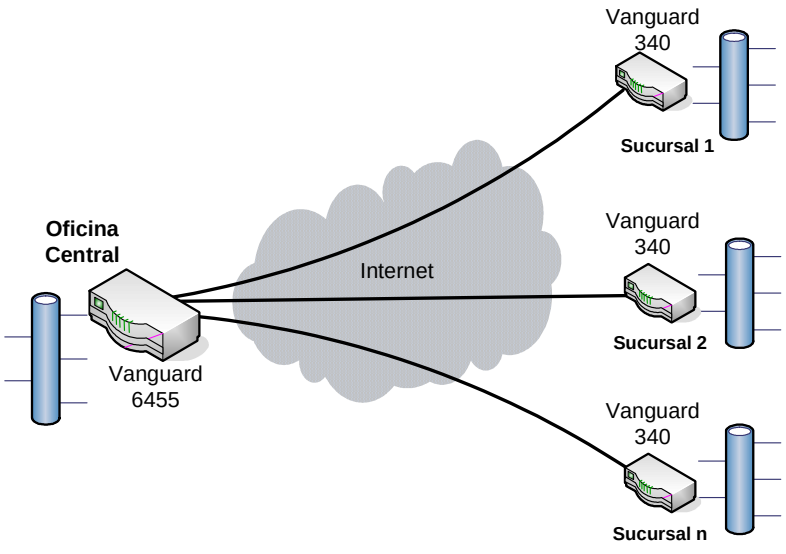

Figura 3.8. Implementación IPSec con routers Vanguard.

3.7.3.1.Características de la Implementación

- Para cada sitio remoto que el nodo es requerido para comunicarse, una interface túnel IPSec es creada permanentemente. Los recursos para la interface son paralizados, sin embargo allí no puede estar pasando cualquier tráfico, entre el sitio remoto y el nodo local. Otras características incluyen:
    - Un túnel requiere otra interface IP para conectar hacia un LCON para acceder a un enlace WAN particular.
    - Múltiples túneles para distintos sitios remotos pueden fluir a través de la misma LCON.
    - Cada interface túnel debería tener su propia dirección IP numerada.
    - Los túneles pueden ser configurados sobre interfaces LAN.
- Una negociación de conexión IPSec entrante es procesada solo si la interface para el nodo que llama está configurada en el nodo local.
- Rutas estáticas pueden ser configuradas para el túnel entre dos sitios.

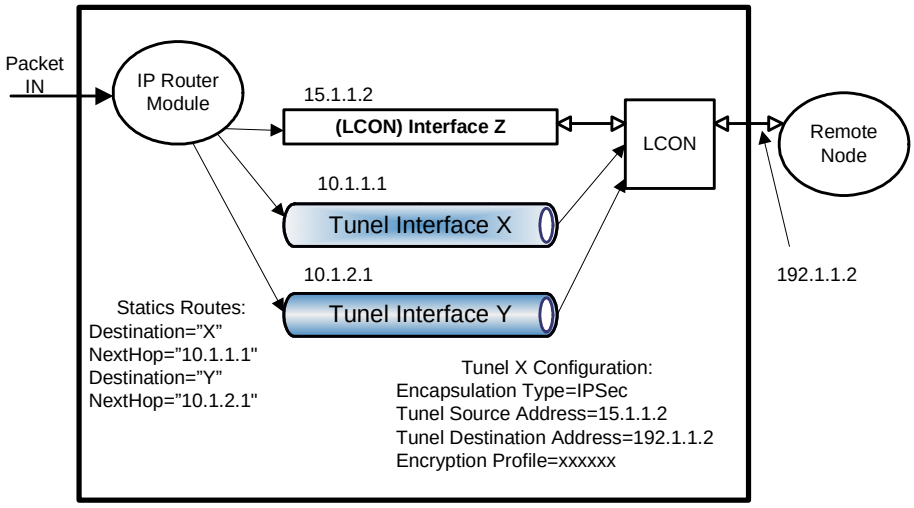

Figura 3.9. Diagrama de encaminamiento en el router.

3.7.3.2. Requerimientos

- Un ruteador Vanguand 340E en cada agencia.
- Conexiones a Internet.
- Tarjeta SIMM encription si el dispositivo no lo tiene.

3.7.3.3.Configuración

La configuración de routers Vanguard es mediante menú de pantalla, hay que seguir estos pasos para acceder a IPSec desde el menú Network Security:

Paso 1: Seleccionar **Configure**, desde el Menú principal CTP, aparecerá el menú Configure.
Paso 2: Seleccionar **Configure Network Security**, se muestra el menú The Configure Network Security.
Paso 3: Seleccionar **Configure IPSec**.

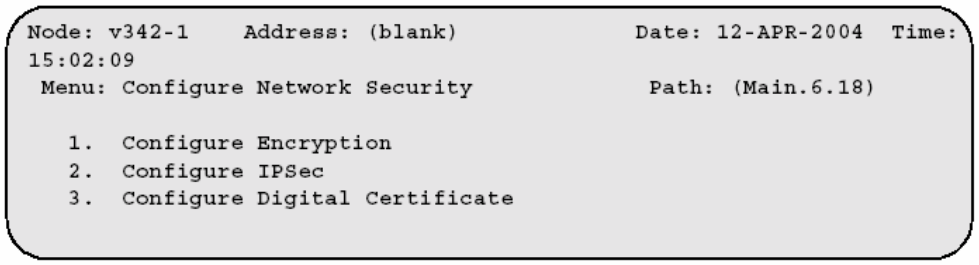

Figura 3.10. Menú de configuración de seguridad en el router.

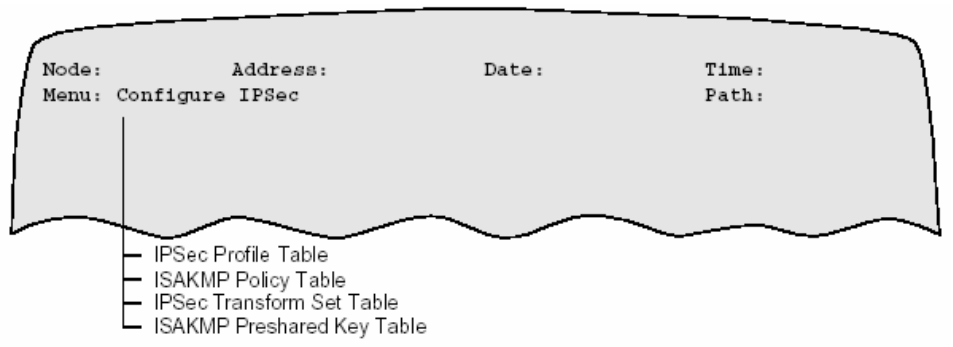

Figura 3.11. Menú de tablas de Configuración IPSec del router.[55]

[55] Fuente: http://www.vanguardnetworks.com

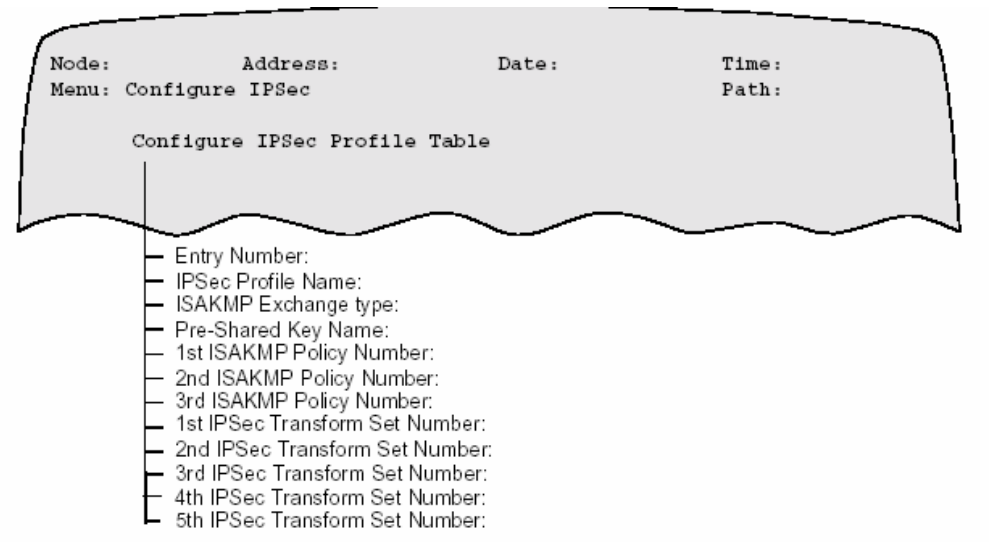

Figura 3.12. Perfil de parámetros IPSec en Vanguard.

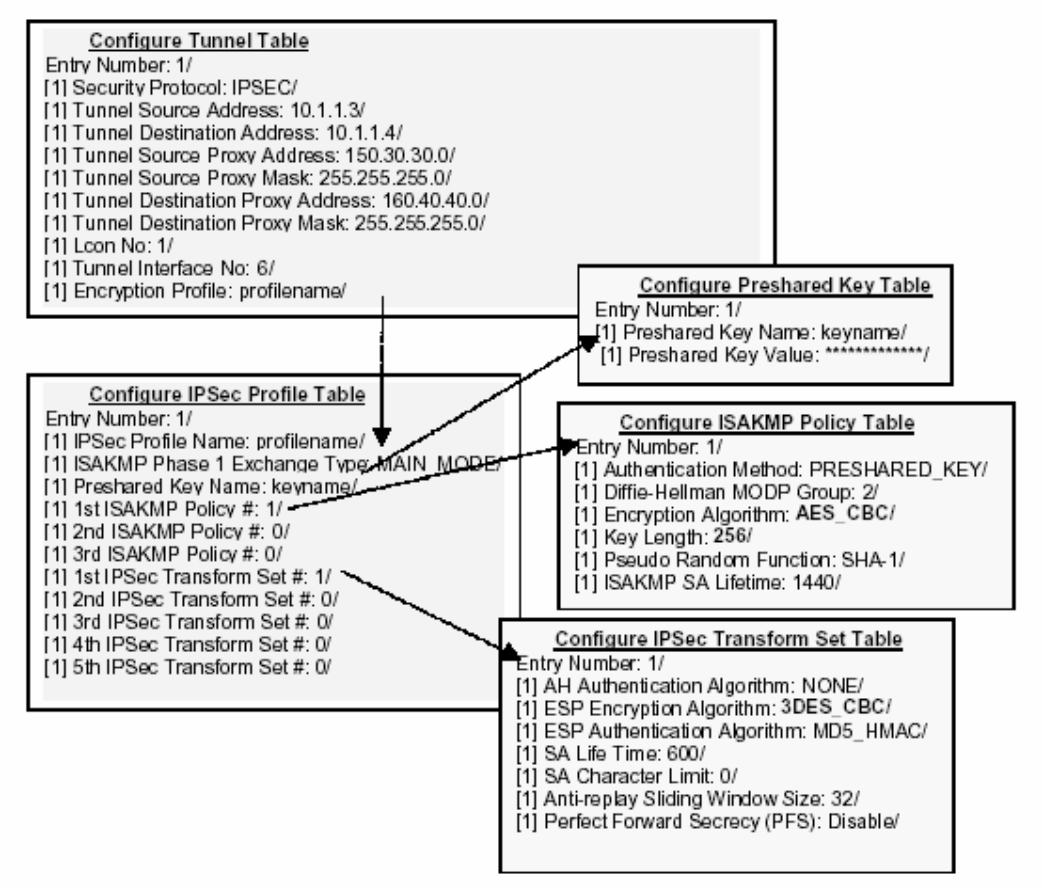

Figura 3.13. Configuración Ejemplo Vanguard IPSec.[56]

[56] Fuente: http://www.vanguardnetworks.com/solutions/tmp/BGP-MPLS_App_Note.pdf

3.7.4. CLIENTE L2TP/IPSEC MICROSOFT

Este escenario sirve para conectar usuarios móviles a la red corporativa de Confiteca, utilizando productos Microsoft.

3.7.4.1.Requerimientos

- Un Servidor con Windows 2003 Server.
- Computador personal con software L2TP/IPSec instalado.
- Conexiones a Internet.

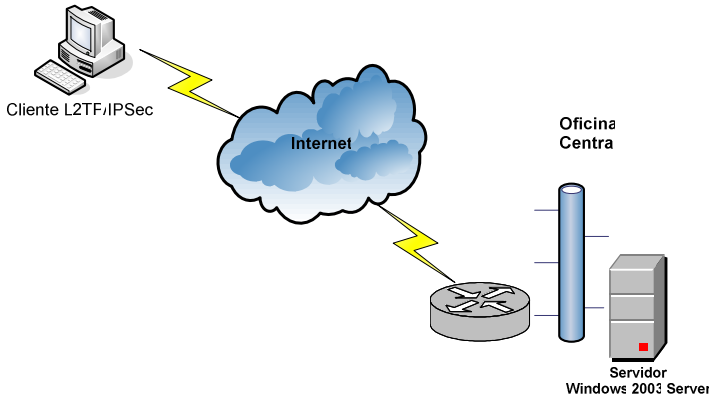

Figura 3.14. Escenario de Cliente Microsoft L2TP/IPSec.

3.7.4.2.Configuración del Servidor

Para este ejemplo el servidor será “HQ-CON-DC-01”, para habilitar y configurar el servicio de Enrutamiento y acceso remoto se tienen los siguientes pasos:

1) Hacer click en el botón **Inicio**, seleccionar **Todos los programas**, **Herramientas administrativas** y, a continuación, click en **Enrutamiento y acceso remoto**.
2) En la consola de **Enrutamiento y acceso remoto**, click con el botón secundario del mouse (ratón) y, a continuación, dar click en **Configurar y habilitar Enrutamiento y acceso remoto**.
3) En el **Asistente para la instalación del servidor de enrutamiento y acceso remoto** dar click en **Siguiente**.
4) Hacer click en el botón de opción **Acceso remoto (acceso remoto o red privada virtual)** (predeterminado) y, a continuación, en **Siguiente**.

5) Activar la casilla de verificación **VPN** y, a continuación, dar click en **Siguiente**.
6) En **Interfaces de red**, dar click para resaltar el adaptador que representa la conexión de Internet en la que funcionará esta VPN. Mantener la selección predeterminada de **Habilitar seguridad** y, a continuación, click en **Siguiente**.
7) En la pantalla **Asignación de direcciones IP**, mantener la opción predeterminada **Automáticamente** dar click en **Siguiente** para continuar.
8) En la pantalla **Administrar servidores de acceso remoto múltiples**, mantener la opción predeterminada para utilizar RRAS para autenticar las solicitudes de autenticación y, a continuación, click en **Siguiente**.
9) En el **Asistente para la instalación del servidor de enrutamiento y acceso remoto** dar click en **Finalizar**.
10) En el cuadro de diálogo **Enrutamiento y acceso remoto**, dar click en **Aceptar** para confirmar los requisitos de **Retransmisión DHCP**.

3.7.4.2.1. Configurar la clave compartida de IPSec

De manera predeterminada, el cliente L2TP y el servidor L2TP de Windows Server 2003 están preconfigurados para la autenticación de IPSec basada en certificados. Al establecer una conexión de L2TP sobre IPSec, se crea automáticamente una directiva de IPSec para especificar que Intercambio de claves de Internet (IKE) utilizará la autenticación basada en certificados durante la negociación de la configuración de seguridad para L2TP. Esto significa que el cliente L2TP y el servidor L2TP deben tener instalado un certificado de equipo para que se pueda establecer correctamente una conexión L2TP sobre IPSec. Ambos certificados de equipo deben proceder de la misma autoridad emisora de certificados (CA).

En algunos casos, no se desea tener un método de autenticación enrutador a enrutador basadas en L2TP. En este caso, la directiva IPSec se puede configurar manualmente para que use claves previamente compartidas al crear conexiones VPN de enrutador a enrutador. Esta clave de autenticación compartida previamente actúa como una contraseña sencilla en la negociación de IKE. Si

ambos extremos pueden probar que conocen la misma contraseña, pueden confiar uno en otro y continuarán con la negociación de claves de cifrado simétricas y privadas y la configuración específica de seguridad para el tráfico L2TP.

Normalmente, se considera que el uso de una clave compartida previamente de IKE no es tan seguro como el uso de certificados, porque la autenticación de IKE (y la confianza implícita) depende sólo del valor de la clave, que se almacena como texto sin formato en la directiva de IPSec. Sin embargo, un usuario malintencionado tendría que conocer la clave compartida previamente y las credenciales de usuario correctas para poder establecer la conexión L2TP sobre IPSec.

Para configurar una clave compartida de IPSec en el servidor se tiene que:

- En la consola de **Enrutamiento y acceso remoto**, click con el botón secundario del mouse en **HQ-CON-DC-01 (local)** y, a continuación, hacer click en **Propiedades**.
- En la página Propiedades de **HQ-CON-DC-01 (local)**, dar click en la ficha Seguridad. Activar Permitir la directiva personalizada IPSEC para la conexión L2TP, escribir 12345 en Clave compartida previamente y, a continuación, click en Aceptar.

3.7.4.3.Configuración del Cliente L2TP/IPSEC

Para crear una conexión L2TP/IPSec se crea una nueva conexión Dial-up manualmente o siguiendo el wizard para una nueva conexión, simplemente se escoge Microsoft L2TP/IPSec VPN Adapter, se provee la dirección IP o nombre del servidor VPN antes que un número de teléfono para esta conexión.

Cuando es usada en una red que soporta una infraestructura public key infrastructure (PKI) se sugiere certificados digitales, Microsoft L2TP/IPSec VPN Client conectará sin requerir cualquier configuración adicional.

Si el servidor VPN requiere usar de claves precompartidas (pre-shared) en lugar de un certificado para autenticación del computador cliente hacia el servidor VPN, se puede configurar autenticación por claves precompartidas utilizando el Microsoft IPSec VPN Configuration Utility.

3.7.5. FREES/WAN TO FREES/WAN [57]

En este ejemplo se describe la implementación de Freeswan en la empresa comercializadora, para escenarios Sitio a Sitio que serviría para conectar las agencias con la matriz. A continuación algunas instrucciones de instalación y configuración.

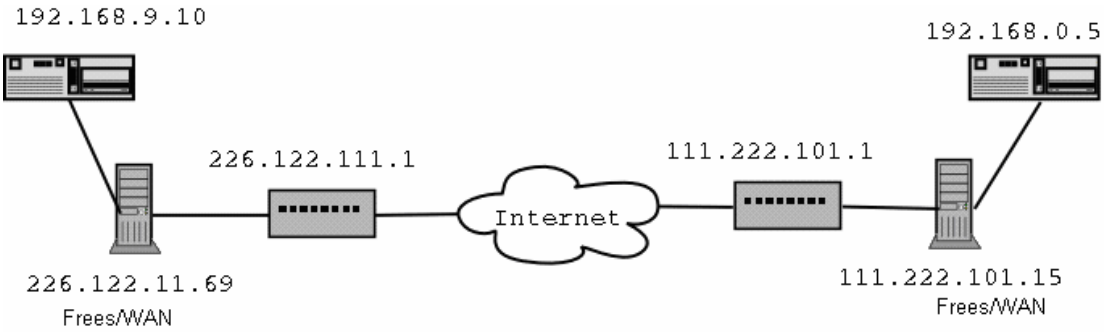

Figura 3.15. Diagrama básico dispuesto para ejemplo con Freeswan.

3.7.5.1.Requerimientos

- Paquete Freeswan tarball/rpm de http://www.freeswan.org.
- Librería gmp desde gnu (http://www.swox.com/gmp/).
- Fuentes Linux Kernel (2.4+ o 2.2).
- Dos servidores.
- Conexiones a Internet.

3.7.5.2.Instalación

3.7.5.2.1. Pasos Generales

- GMP - Descargar, desempacar y construir la librería gmp (./configure, make install, etc.)
- Freeswan - Descargar, desempacar y construir usando el comando 'make menugo'.
- Kernel – Retornar a la configuración del Kernel y chequear la configuración de IPSec dentro de 'Network Options'.

[57] http://www.bozemanlug.org/talks/freeswan_presentation.html

3.7.5.2.2. Pasos Específicos

- Ejecutar el programa de configuración del Kernel (make menuconfig) y guardar la configuración corriente del Kernel.
- Descargar y desempaquetar freeswan (usando **tar -xfzf freeswan.1.98.tar.gz**).
- Tipear **make menugo** (esto iniciará el kernel config y construirá el programa Ipsec).
- Construir un nuevo Kernel que incluye Ipsec.
- Incluir el nuevo Kernel en lilo.conf.
- Correr lilo.conf para invocar los cambios para lilo.conf
- Reiniciar el sistema.
- Generar nuevas llaves rsa (si es necesario) con el comando **ipsec rsasigkey 2048.**
- Actualizar ipsec.secrets con la clave actualizada.
- Actualizar ipsec.conf.

3.7.5.3.Configuración

Freeswan implementa IPSec con KLIPS (Kernel IPSec) y Pluto (demonio IKE), y para configurar utiliza los dos siguientes archivos:

- ipsec.conf - Opciones de configuración de communicación.
- ipsec.secrets - Claves Pre-shared y firmas RSA.

El primero (ipsec.conf) establece la comunicación entre las dos máquinas gateway de Freeswan. Es muy importante que los parámetros de la comunicación entre los dos gateway emparejen exactamente puesto que se utilizan éstos como la primera parte de un proceso de autentificación de dos pasos.

El segundo archivo (ipsec.secrets) lleva a cabo llaves de la firma de RSA utilizadas para cada entrada para identificarse al otro, cada gateway tendrá un archivo de ipsec.secrets distinto.

El **ipsec.conf** tiene dos tipos de secciones, la sección de “config” (configuración) y la sección de “conn” (conexiones). En este momento la única sección de configuración que se acepta en FreeS/WAN es la sección de config “setup”.

- La sección “config setup” tiene toda la información que el software necesita al inicializarse. Este es un ejemplo de esta sección:

config setup

interfaces=%defaultroute
klipsdebug=none
plutodebug=none
plutoload=%search
plutostart=%search
uniqueids=yes

El valor más importante en este ejemplo es el del parámetro interfaces, el valor especial %defaultroute significa que la interface de red que pluto va a utilizar para establecer túneles cifrados, es la que utiliza la ruta por defecto (la que sale a Internet generalmente).

- Las secciones “conn" en cambio se utilizan para decirle a pluto qué tipo de túneles se van a establecer o aceptar. La sección “conn %default”, va a tener los valores por defecto de todas las secciones “conn". Luego en cada sección “conn" se podrán sobrescribir los valores, pero en caso que se omitan se tomaran los escritos en esta sección. Este es un ejemplo de sección conn.

conn %default
    keyingtries=0
    authby=rsasig

El parámetro “keyingtries” determina cuantas veces pluto va a intentar para establecer un túnel, el valor cero indica que siga intentando eternamente.
El parámetro “authby” determina la forma en que se va a estar haciendo la autentificación. El valor “secret” es cuando se utiliza pre-shared-keys (claves compartidas pre-acordadas) y se utiliza el valor rsasig cuando se va a autenticar con una firma digital RSA (cuando se utilizan certificados X509 también se usa este tipo de valor).
Dependiendo el tipo de autenticación y los tipos de túneles que se vayan a utilizar van a existir una sección “conn" por nodo de VPN. En este ejemplo solo permite un túnel por sección “conn" (que de hecho es lo más usual).

```
conn  “hacia right”
   left=%defaultroute
   leftsubnet=192.168.9.0 /24
   leftrsasigkey=0sAQO1wwYJq.........
   right=%any
   rightid=@amigo.xtech
   rightsubnet=192.168.0.0/24
   rightrsasigkey=0sAQNt1jXTSQ.........
   auto=add
```

Dado que el gateway (left) esta conectado directamente al Internet, se utiliza el valor %defaultroute que le indica a pluto que tome el número de IP asignado a la interface que tiene la ruta por defecto (por ejemplo la interface ppp0, si es que nos conectamos a Internet con un modem o línea ADSL). Si este número fuera un IP estático y fijo, entonces podríamos poner directamente el número como valor del campo.

El campo “leftsubnet” indica qué número de IP tiene la red local que esta del lado izquierdo del túnel, o sea, el número de IP de la red LAN del gateway izquierdo. Con respecto al lado derecho (right), vemos que el parámetro right, que indica el número de IP que tiene el lado derecho del túnel, tiene un valor especial: “%any”, esto le indica a pluto que el lado derecho de este túnel va a poder ser cualquier número de IP (o sea un IP dinámico).

Nota: Cuando se utiliza este valor (%any) y la autenticación es por firmas digitales, es necesario agregar el campo rightid=@<alguna_cadena> (en el concentrador y en el nodo), al igual que el lado izquierdo, el derecho también tiene un subnet y una clave pública de RSA.

Por último el parámetro “auto=add” indica que este túnel deberá agregarse a los túneles disponibles, pero pluto no hará nada con él al momento de inicializar todo el servicio (el valor de este campo puede contener start que indica que al inicializar el servicio, pluto intente establecer el túnel), y otros valores que no viene al caso explicarlos.

Este es un ejemplo de túnel “LAN to LAN", si no estuvieran los parámetros de [right|left]subnet= entonces sería un túnel “host to host" (por supuesto las combinaciones son también válidas: “host to LAN" y “LAN to host", sacando y poniendo el parámetro ....subnet= que corresponda).

```
conn “hacia left”
   left=226.122.11.69
   leftsubnet=192.168.9.0/24
   leftrsasigkey=0sAQO1wwYJq.....
   right=%defaultroute
   rightid=@amigo.xtech
   rightsubnet=192.168.0.0/24
   rightrsasigkey=0sAQNt1jXTSQ.....
   auto=start
```

Esta sección “conn" es la que se utilizaría en el nodo right (la otra punta del túnel que acabamos de ejemplificar). Los campos que cambiaron su valor son left=, right= y auto=, left sigue siendo el concentrador y right el nodo, pero los valores son diferentes. En left= se colocó el valor 226.122.11.69 que es justamente el número de IP del nodo left.
Para el caso de right= se utiliza el valor especial %defaultroute que indica exactamente lo mismo que se explicó más arriba para el caso de left. En el caso del parámetro auto=, el valor start indica que al momento de inicializar el servicio, pluto intentará establecer el túnel.

3.7.5.3.1. Configurando las Workstations

Añadir una entrada en la tabla de ruteo para que la máquina local pueda encontrar las máquinas remotas por medio del freeswan gateway.

```
route add -net 192.168.0.0 netmask 255.255.255.0 gw 192.168.9.5
```

Crear un permiso en el Firewall que permita los protocolos IPSec admitir la comunicación entre las dos redes.

3.7.6. INTEGRACION DE VoIP Y LA VPN

Al prescindir de las líneas dedicadas, la comunicación de VoIP que se mantienen con las sucursales de la empresa, también tendría que cambiar de escenario.
En este caso se utilizaría un Gateway de VoIP en cada regional, o ruteadores que dispongan de tarjetas FXS (Routers Vanguard).
De esta manera se lograría integrar voz, datos y hasta video utilizando la misma estructura de la VPN.

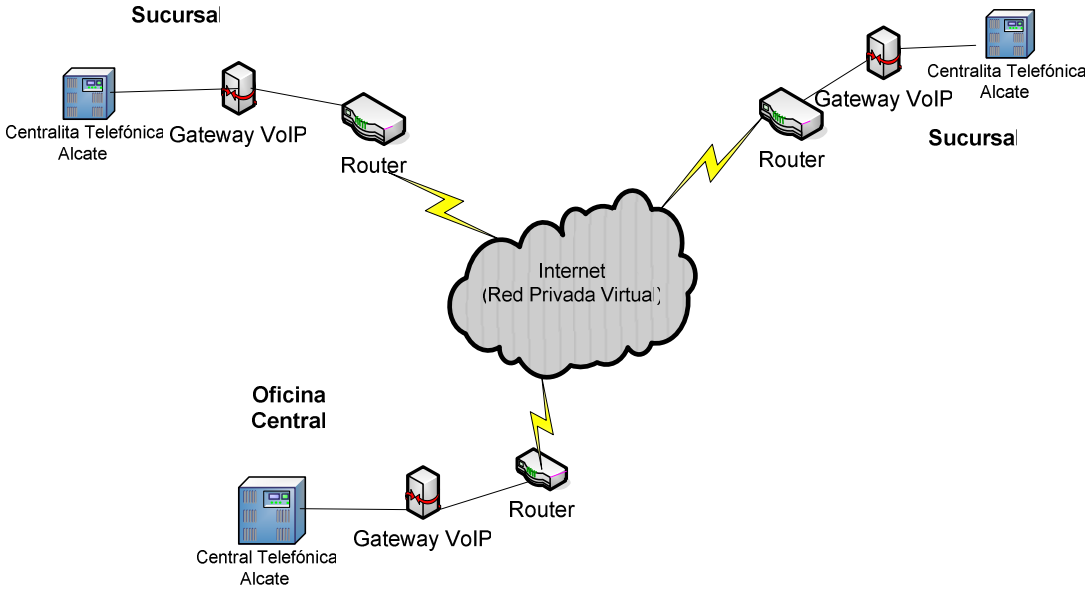

Figura 3.16. Integración de VoIP en la VPN.

4. IMPLEMENTACION DE UN PROTOTIPO VPN

Para implementar el prototipo de la Red Privada Virtual (VPN) en la empresa comercializadora, se tomaron en cuenta las alternativas sugeridas en el capítulo anterior, los recursos económicos para invertir en el proyecto y porque Cisco es uno de los líderes en tecnología de conectividad.

4.1. ESCENARIO DE LA IMPLEMENTACION

4.1.1. DESCRIPCION DEL ESCENARIO

El escenario implementado es "**VPN de acceso remoto"**, se utilizan productos de la línea Cisco Systems**,** en la figura 4.1 se muestra la VPN desarrollada, en este caso se tienen dos componentes principales:

- El servidor o gateway VPN, que es un Firewall Cisco PIX.
- El cliente VPN, que es el software VPN Client Versión 4.6.

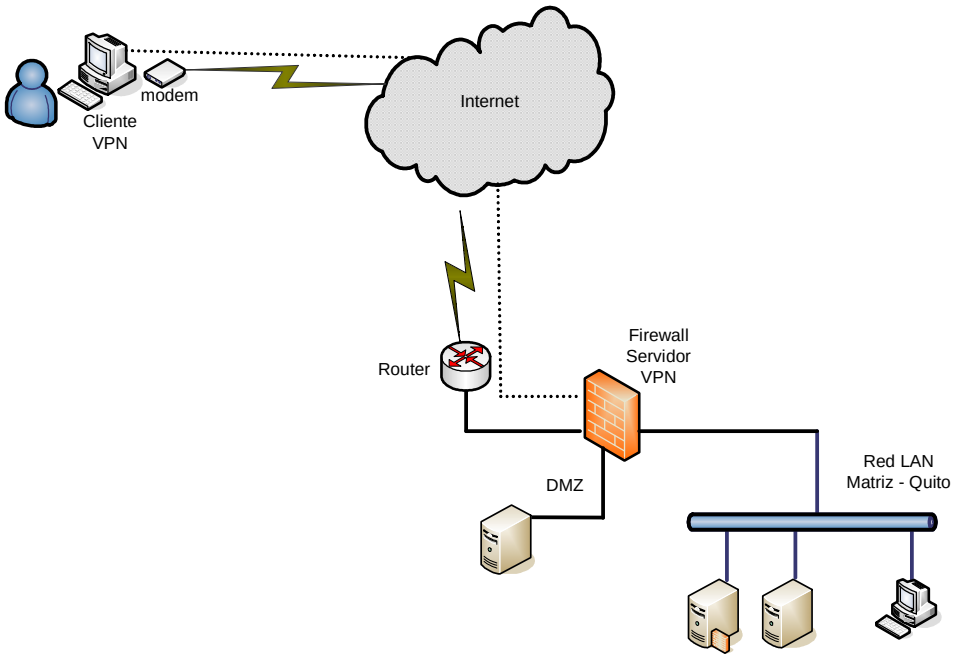

Figura 4.1. Escenario de Acceso Remoto del prototipo VPN.

Este escenario VPN permite a los usuarios móviles acceder de manera segura a los recursos de la red centralizada. El usuario puede tener una conexión dial-up o cualquier otra para acceder al Internet.

En el computador que utilice el usuario será llamado “Cliente VPN” y es donde se instala el software VPN Client versión 4.6, VPN Client en un PC remoto lo comunica con un dispositivo VPN Cisco de la empresa y crea una conexión segura sobre el Internet. Esta conexión segura es una Virtual Private Network (VPN).

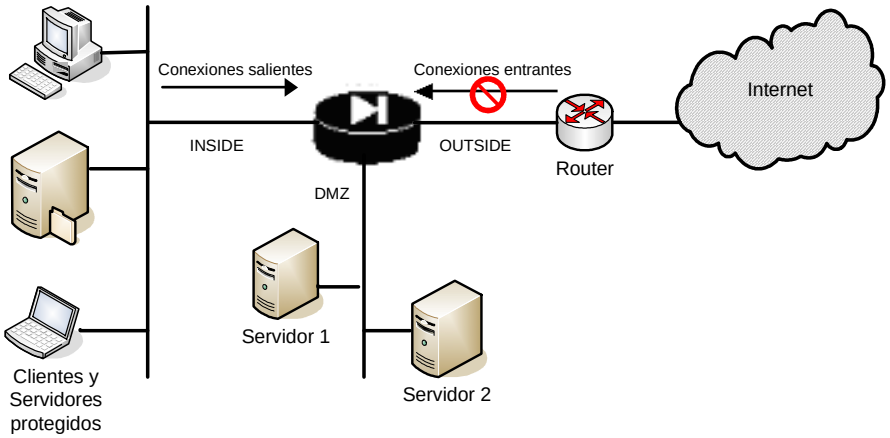

Figura 4.2. Interfaces del Servidor VPN (Firewall).

Mientras que el Firewall será llamado “Servidor VPN”, al disponer que el servidor VPN esté en un Firewall tenemos un solo punto de entrada a la red corporativa, este entorno sirve para:

- Permitir el acceso saliente a Internet.
- Evitar el acceso entrante desde Internet
- Cifrar el tráfico a redes o clientes remotos de la VPN.

4.1.2. CONEXIONES A INTERNET

- **Servidor VPN**

Ancho de Banda Matriz: 128 kbps.
Proveedor: Impsat.
Tecnología Utilizada: Frame Relay
Última milla: Fibra Óptica.

- **Cliente VPN**

Ancho de Banda Cliente: 56 kbps.
Proveedor: Onnet.
Tecnología Utilizada: Dial-up
Última milla: Par telefónico.

4.1.3. FUNCIONAMIENTO

El prototipo VPN implementado en la red de Confiteca funciona de la siguiente manera:

- El cliente VPN se conecta al Internet, desde cualquier sistema operativo soportado por el software VPN Client.
- Ejecuta su conexión privada mediante el software VPN Client, para ello se debe conocer la dirección IP o nombre del servidor VPN.
- El servidor VPN recibe la petición de conexión del cliente, reconoce que desea establecer una VPN, entonces inicia una conexión a través del Internet.
- En este momento se ha de negociar un proceso de confianza mutua que se consigue al verificar el método de autenticación, usuario, password, el algoritmo de encriptación.
- Cuando ambas máquinas confían una en la otra se establece un túnel, esto quiere decir que existe una comunicación constante entre ellas.
- El gateway VPN asigna dinámicamente una dirección IP disponible del pool de direcciones destinadas para este propósito.
- Compara la lista de acceso de la VPN y establece el intercambio de información solo en los hosts permitidos.
- Ahora la red LAN de la empresa ya posee un brazo más que se extiende hasta el lugar donde está el cliente VPN.

4.2. CARACTERÍSTICAS DE HARDWARE Y SOFTWARE DE LOS DISPOSITIVOS

4.2.1. SERVIDOR VPN

La serie Cisco PIX (Private Internet Exchange) Firewall proporciona un alto grado de seguridad en un dispositivo hardware y software fácil de instalar y con un rendimiento sobresaliente. Este dispositivo permite proteger rigurosamente la red interna del mundo exterior.

Cisco PIX 515E Firewall, es una versión de la plataforma PIX con capacidades mejoradas, diseñadas para una seguridad óptima y un buen desempeño de VPN.

Se basa en el Algoritmo de Seguridad Adaptable (ASA) que permite al PIX implementar estrictas medidas de seguridad.

Figura 4.3. Cisco PIX Firewall Modelo 515.[58]

4.2.1.1. Hardware

Modelo:	PIX-515.
Procesador:	Pentium 200 MHz.
Memoria RAM:	32 MB RAM.
Memoria Flash:	16MB.
BIOS Flash:	32KB.
Interfaces Ethernet:	3 de 10/100 Mbps (inside, dmz, outside).

4.2.1.1.1. Peso y Dimensiones

Factor de forma: 1 RU, standard 19-plg, montable en Rack.

Dimensiones (H x W x D): 1.72 x 16.82 x 11.8 in. (4.37 x 42.72 x 29.97 cm).

Peso (con fuente de poder): 11 lb (4.11 kg).

[58] Fuente: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps4094/index.html.

4.2.1.1.2. Ranuras de Expansión

Dos slots PCI de 32-bit/33-MHz.

Dos slots DIMM RAM de 168-pines, soporta hasta 64Mb de memoria máximo.

4.2.1.2.3. Interfaces

Puerto de consola: RS-232, 9600 bps, RJ45.

Puerto Failover: RS-232, 115 Kbps, DB-15 (requiere de cable especial Failover).

Dos interfaces integradas Fast Ethernet 10/100, auto (half/full duplex), RJ45.

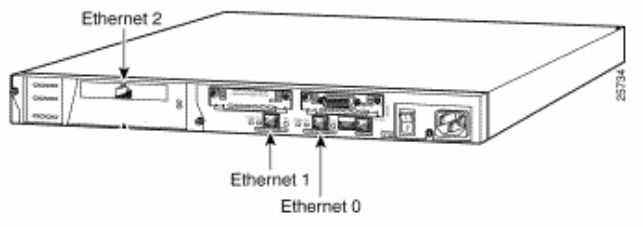

Figura 4.4. Interfaces instaladas en el PIX.

4.2.1.2. Software (Firewall OS)

El Cisco PIX Firewall Release 6.2, es de Licencia Restringida, el modelo Cisco PIX 515 “Restringido” (PIX 515-R) provee un excelente valor para organizaciones que buscan seguridad robusta con Cisco PIX. Incluye 32 MB de RAM, dos interfaces Fast Ethernet 10/100, y soporta una interface adicional Fast Ethernet 10/100Mbps.

4.2.1.2.1. Compatibilidad con Easy VPN server

Los Firewalls PIX pueden actuar como clientes VPN basados en hardware, las siguientes plataformas Easy VPN Server son soportadas para este caso:

Cisco IOS Routers	Release 12.2(8)T y superior
Cisco PIX Firewalls	Release 6.0(1) y superior
Cisco VPN 3000 Concentrators	Release 3.1 y superior

Tabal 4.1. Compatibilidad del PIX con Easy VPN Server.[59]

[59] Fuente:http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080124551.html

4.2.1.2.2. Compatibilidad Cisco para VPN Sitio a Sitio

También los Firewalls pueden interoperar con los siguientes productos VPN Cisco para la conectividad VPN "sitio-a-sitio".

Cisco IOS Routers	Release 12.1(6)T y superior
Cisco PIX Firewalls	Release 5.1(1) y superior
Cisco VPN 3000 Concentrators	Release 2.5.2 y superior

Tabla 4.2. Compatibilidad de dispositivos Cisco para VPN sitio a sitio.[60]

4.2.1.2.3. Compatibilidad VPN Client

El Firewall PIX soporta una amplia variedad de Clientes VPN basados en software y hardware, incluyendo:

Software IPSec VPN clients	Cisco secure VPN Client release 1.1 Cisco VPN concentrator client, release 2.5 y superior Cisco VPN client para Windows, release 3.0 y superior Cisco VPN client para Linux, release 3.5 y superior Cisco VPN client para Solaris, release 3.5 y superior Cisco VPN client para Mac OS X, release 3.5 y superior
Hardware IPSec VPN Clients	Cisco VPN 3002 hardware client, release 3.0 y superior Cisco IOS software Easy VPN remote, release 12.2(3)YJ Cisco PIX Firewall Easy VPN Remote, release 6.2 y superior
Layer 2 Tunneling Protocol (L2TP) IPSec VPN Clients	Microsoft Windows 2000
Poin-to-Point Tunneling Protocol (PPTP) VPN clients	Microsoft Windows 95 Microsoft Windows 98 Microsoft Windows NT 4.0 Microsoft Windows 2000

Tabla 4.3. Compatibilidad con software clientes VPN.[61]

[60] Fuente: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080124551.html
[61] Fuente: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080124551.html

4.2.1.2.4. Criptografía Estándar Soportada

Algoritmos de encripción Asimétrica (public key)	RSA (Rivest, Shamir, Adelman) public/private claves pares 512 bits hasta 2048 bits
Algoritmos de encripción Simétrica	DES: 56 bits 3DES: 128 bits RC4: 40, 56, 64 y 128 bits
Perfect Fordware Secrecy (clave de negociación Diffie-Hellman)	Grupo 1: 768 bits Grupo 2: 160 bits
Algoritmos Hash	MD5: 128 bits SHA-1: 160 bits
Certificados de Autoridad X.509	Baltimore UniCERT Entrust Authority Servicios de certificado Microsoft Windows 2000 VerySign OnSite
Protocolos de enrolamiento de certificado X.509	SCEP

Tabla 4.4. Criptografía que soporta el Cisco PIX.[62]

4.2.2. CLIENTE VPN

El cliente VPN para este escenario es un computador personal (PC) con las siguientes características:

4.2.2.1. Software

Sistema Operativo: Windows 2000 Service Pack 4.
Cisco VPN Client: Versión 4.6.

4.2.2.1.1. Características de VPN Client

VPN Client es una aplicación que corre en un PC Windows, en Sun ultraSPARC workstations, en Linux desktop y en Macintosh (Mac) personal computer.

[62] Fuente: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080124551.html

VPN Client soporta los siguientes dispositivos Cisco VPN:

- Concentradores Cisco VPN 3000, Versión 3.0 y posteriores.
- Cisco PIX Firewall, Versión 6.2.2 (122) o Versión 6.3 (1).
- Cisco IOS Routers, Versión 12.2 (8)T y posteriores.

La siguiente tabla indica los requerimientos del sistema para instalar VPN Client en cada una de las plataformas soportadas.

COMPUTADOR	**SISTEMA OPERATIVO**	**REQUERIMIENTOS**
Computador con un procesador clase Pentium o mayor	Windows 98. Windows ME. Windows NT (service pack 6). Windows 2000 Windows XP	TCP/IP instalado. 50MB disponible en disco. RAM: 32 MB para Windows 98 64 MB para NT y ME 128 MB para Windows 2000 y XP.
Computador con un procesador Intel x86.	Linux Red Hat 6.2 o superiores Linux (Intel), o librerías compatibles con glibe Versión 2.1.1.-6 o superior, usando Kernel versión 2.2.1.2 o posterior. Nota: El VPN Client no soporta SMP (multiprocesador) o kernels de procesador de 6 bits.	32 MB de RAM. 50 MB de espacio en disco
Computador SUN ultra Sparc	Solaris 32 o 64 bits Kernel OS versión 2.6 o posterior	32 MB de RAM. 50 MB de espacio en disco
Computador Macintosh	Mac OS X, Versión 1.0.2.0 o posterior.	50 MB de espacio en disco

Tabla 4.5. Requerimientos del software VPN client V 4.6.[63]

4.2.2.2. Hardware

Procesador: Pentium 4 de 1.8 Ghz.

Memoria RAM: 128 Mbytes.

Disco duro: 40 MBytes.

NIC: 100 Mbps.

Fax MODEM: HR 56Kbps.

[63] Fuente: http://www.cisco.com/en/US/products/sw/secursw/ps2308/prod_release_note09186a00802d398a.html.

4.3. INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS

En las configuraciones de los equipos se utilizan direcciones IP de prueba para proteger la información presente en la red de la empresa comercializadora.

4.3.1. CONFIGURACIÓN DEL FIREWALL

Básicamente cuatro tareas claves están involucradas para configurar VPN con encripción IPSec en un Firewall Cisco PIX:

- Preparar el entorno para la VPN.
- Configurar Internet Key Exchange (IKE).
- Configurar IPSec.
- Permitir el tráfico IPSec.

4.3.1.1. Preparar el entorno para la VPN

Para implementar satisfactoriamente una red con IPSec, requiere de una planificación antes de empezar a configurar el Firewall. Configurar IPSec puede ser complicado, se sugiere considerar los siguientes pasos:

1. Cuales host estarán en la VPN.
2. Cuantos pares estarán.
3. Qué políticas IKE se utilizarán.

En esta implementación, consideramos:

a) Intervendrá el computador remoto y la red LAN de la empresa.
b) En este escenario hay un par de equipos para la VPN.
c) Los parámetros para definir IKE son:
   - Authentication: pre-shared (las llaves se configuran manualmente).
   - Encryption: 3DES.
   - Deffie Helman group: 2.
   - Hash: md5.

4.3.1.2. Configurar Internet Key Exchange (IKE)

En el PIX los comandos de configuración hacen referencia a ISAKMP, la configuración IKE consiste de los siguientes pasos esenciales:

a) Especificar el método de autenticación.
b) Especificar el algoritmo de encripción.
c) Especificando el grupo Diffie-Hellman.
d) Especificando el algoritmo Hash.
e) Habilitar ISAKMP.
f) Especificar el pool de direcciones IP.
g) Crear una lista de acceso (access-list) para definir el tráfico a encriptar.
h) Declarar el grupo.
i) Establecer la clave pre-compartida.

Comandos utilizados:

a) pix(config)# isakmp policy 10 authentication pre-share
b) pix(config)# isakmp policy 10 encryption 3des
c) pix(config)# isakmp policy 10 group 2
d) pix(config)# isakmp policy 10 hash md5
e) pix(config)# isakmp enable outside
f) pix(config)# ip local pool vpn-pool X.Y.200.1-X.Y.200.254
g) pix(config)# access-list acl-no-nat-vpn permit ip V.W.1.0 255.255.255.0 X.Y.200.0 255.255.255.0
pix(config)# access-list acl-no-nat-vpn permit ip P.Q.2.0 255.255.255.0 X.Y.200.0 255.255.255.0
h) pix(config)# vpngroup vpn-grupo address-pool vpn-pool
pix(config)# vpngroup vpn-grupo split-tunnel acl-no-nat-vpn
pix(config)# vpngroup vpn-grupo idle-time 1800
i) pix(config)# vpngroup vpn-grupo password **********

Para verificar la configuración se puede usar los comandos:

pix(config)# show isakmp
pix(config)# show isakmp policy

4.3.1.3. Configurar IPSec

La configuración IPSec será completada en cinco pasos:

a) Configurando transform set (la combinación de algoritmos de encriptación).
b) Configurando el Lifetime de SA (Security Association) IPSec.
c) Creando una entrada cripto map.
d) Aplicar el cripto map set a una interface.
e) Excluir el tráfico VPN de NAT.

Comandos utilizados:

a) pix(config)# crypto ipsec transform-set trans-remota esp-3des esp-md5-hmac
b) pix(config)# crypto ipsec security-association lifetime seconds 600
c) pix(config)# crypto map vpn-out 10 ipsec-isakmp
pix(config)# crypto map vpn-out 10 match address acl-no-nat-vpn (the accesslist)
pix(config)# crypto map vpn-out 10 set transform-set trans-remota (the transform-set)
pix(config)# crypto map vpn-out 10 ipsec-isakmp dynamic vpn-dyn
d) pix(config)# crypto map vpn-out interface outside (applies the crypto map)
e) pix(config)# nat (inside) 0 access-list acl-no-nat-vpn (the access-list)

4.3.1.4. Permitir el tráfico IPSec

Comando:
pix(config)# sysopt connection permit-ipsec

Permite a todos los paquetes que arriban vía el túnel IPSec para pasar entre el Firewall.
Para ver esto se puede utilizar los comandos:
pix(config)# show crypto ipsec sa

Para ver la negociación IPSec, se puede usar el comando “debug”:
pix(config)# debug crypto isakmp
pix(config)# debug crypto ipsec

En el Anexo 2 se muestra el resumen de toda la configuración del PIX para la VPN.

4.3.2. CONFIGURACIÓN DEL CLIENTE VPN

4.3.2.1. Instalación de VPN Client V4.6

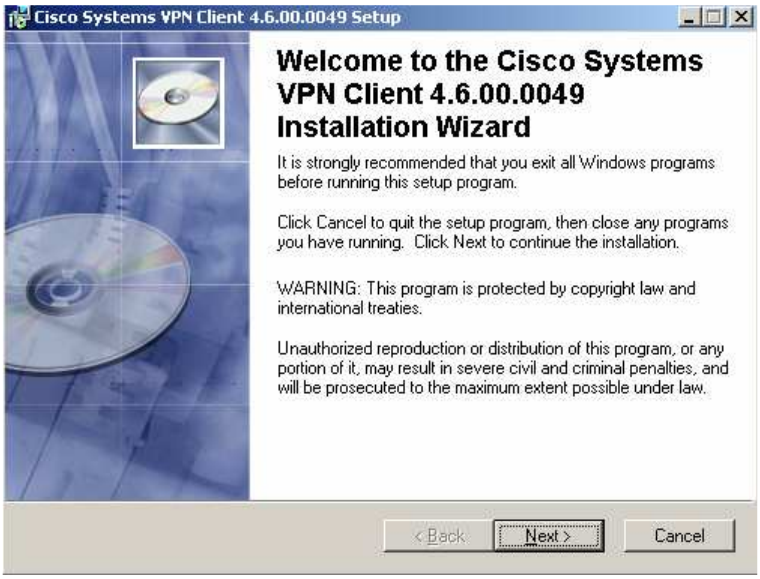

Figura 4.5. Inicio de instalación de VPN client.

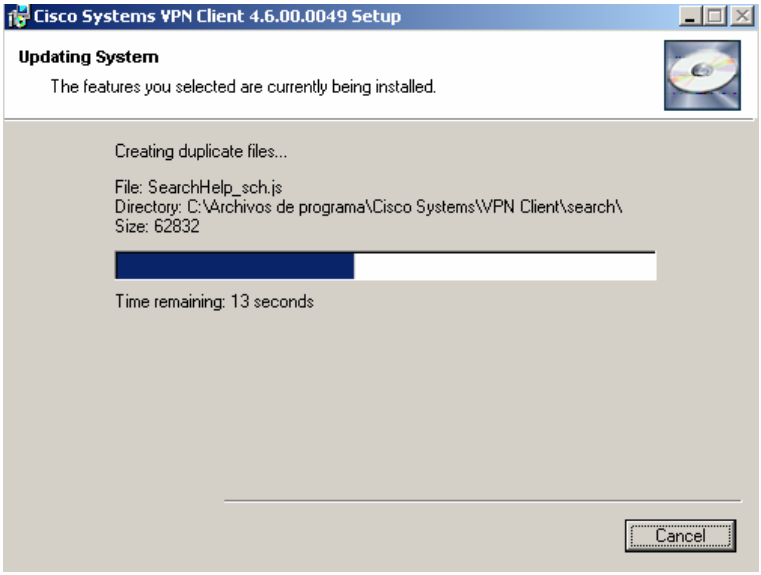

Figura 4.6. Instalación en proceso de VPN client.

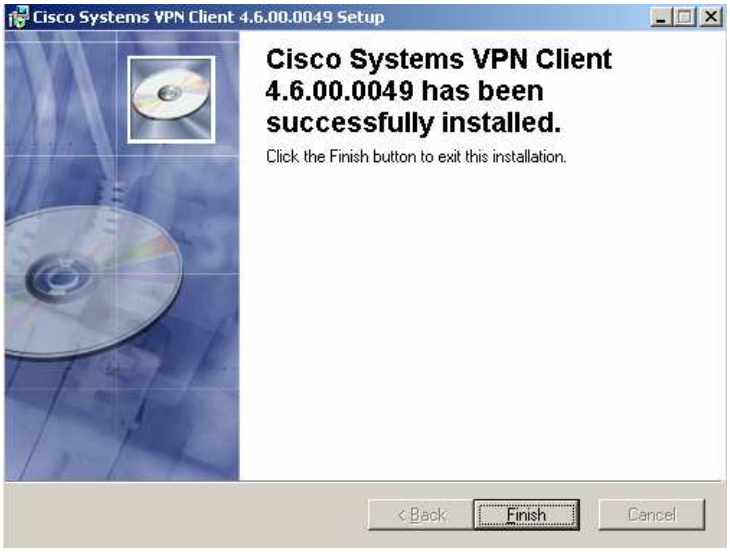

Figura 4.7. Finalización de instalación de VPN client.

4.3.2.2. Configuración de la Conexión VPN

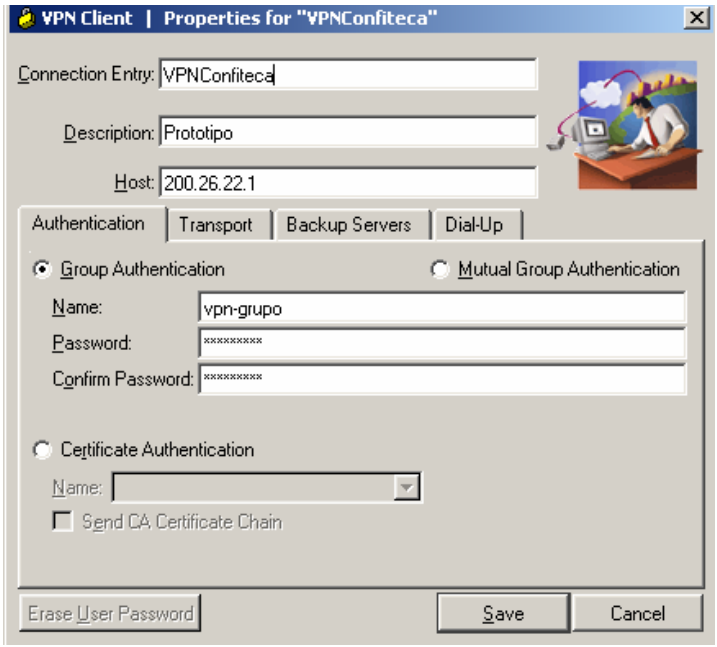

Figura 4.8. Configuración de VPN client.

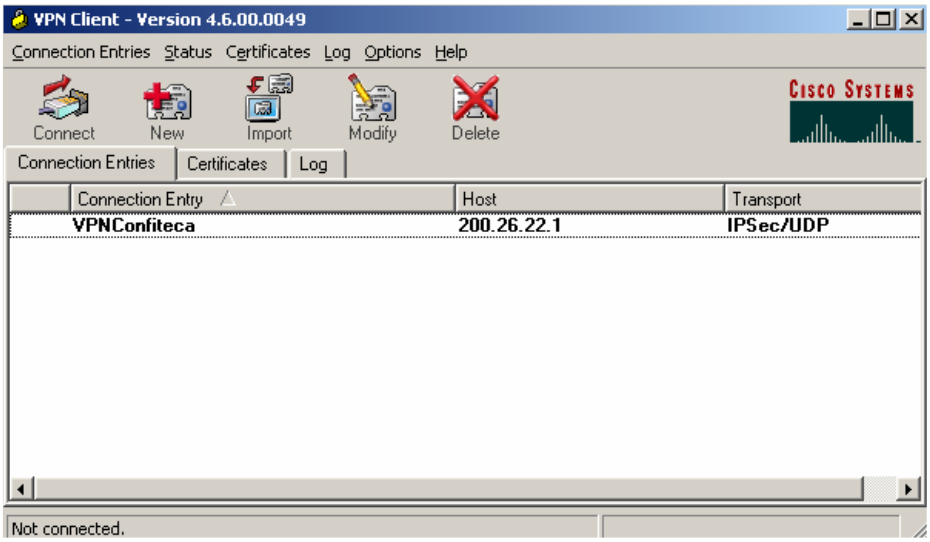

Figura 4.9. Finalización de la configuración de conexión VPN.

4.4. PRUEBAS DE FUNCIONAMIENTO Y RESULTADOS

4.4.1. CONEXIÓN AL INTERNET

El paso inicial para que funcione la VPN es la conexión a Internet, a continuación los pasos respectivos:

Figura 4.10. Iniciando la conexión a Internet.

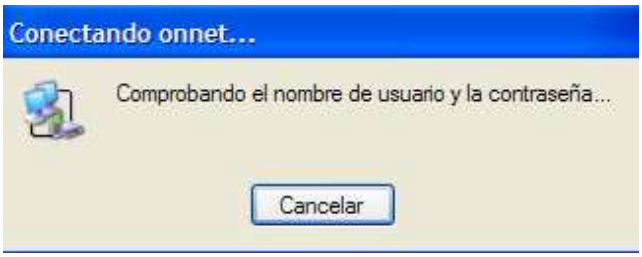

Figura 4.11. Autenticación en el ISP.

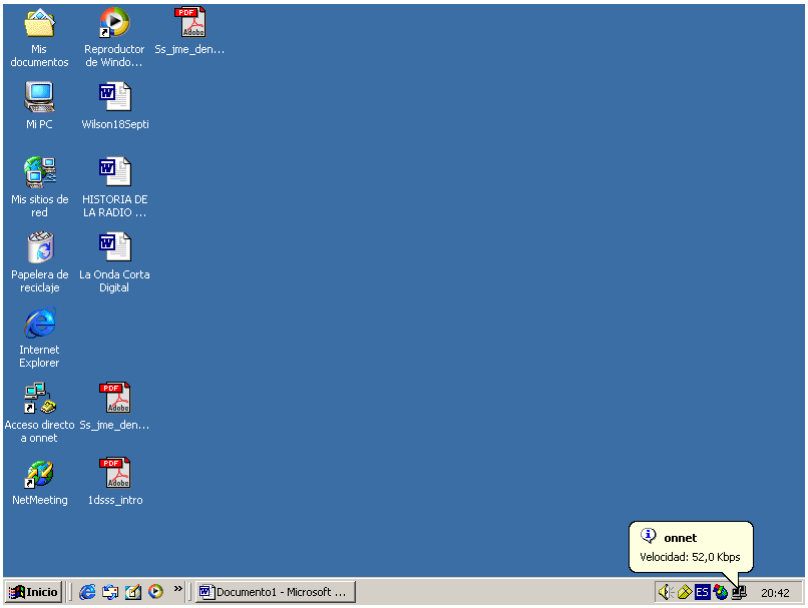

Figura 4.12. Icono de conexión al Internet

Como se puede ver en la figura 4.12 el computador ha establecido conexión con el proveedor de Internet “Onnet”.

4.4.2. CONEXIÓN DE LA VPN

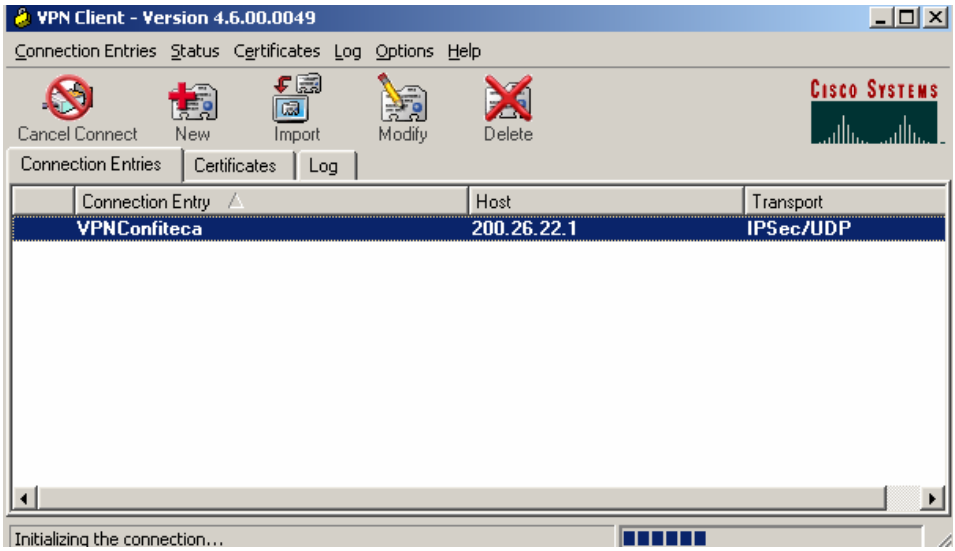

Figura 4.13. Inicio de conexión VPN client.

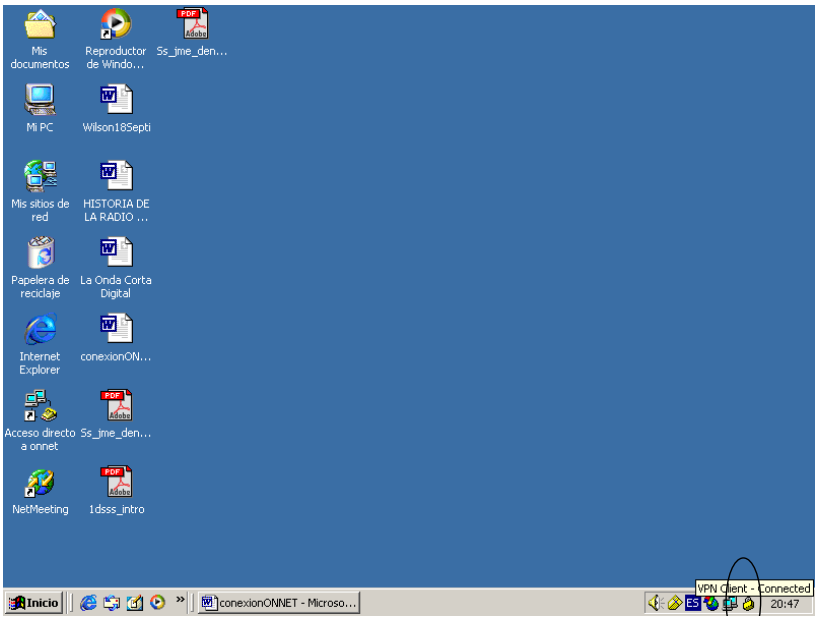

Figura 4.14 VPN conectada.

4.4.3. VERIFICACIÓN DE CONEXIONES Y SERVICIOS

Al establecer la VPN entre el host y el Firewall, prácticamente el PC es uno más de la red y puede acceder a directorios compartidos, revisar el correo electrónico, hacer Telnet a un servidor, impresoras de red, etc.
Para verificar esto, se hicieron las siguientes pruebas:

- **Latencia**

Conocida también como tiempo de respuesta, llamado erróneamente “ping”, es el tiempo que un paquete de datos transmitido a través de una red, tarda en llegar al destino y regresar.
La latencia de una conexión puede ser medida con el comando “ping” y se expresa convencionalmente en milisegundos, en este caso, en la conexión VPN se obtuvo una respuesta satisfactoria de un servidor de la empresa. Hay que tomar en cuenta que la latencia es sensible a la distancia geográfica.
La respuesta obtenida de la conexión es de 365 mseg de promedio, presentada en la figura 4.15.

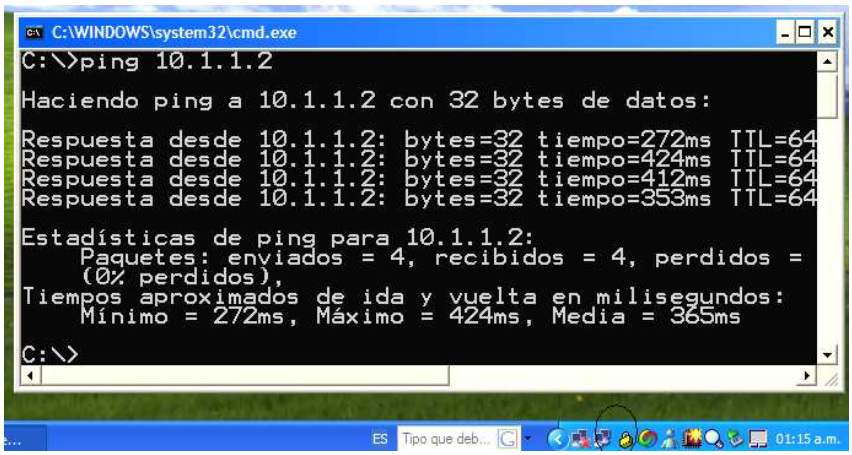

Figura 4.15 Latencia de la conexión VPN.

- **Correo Electrónico**

Otra aplicación útil para cualquier empleado de la empresa es el correo electrónico, en este caso el software de correo Lotus Notes encuentra la conexión con el servidor de la empresa y hace una réplica de las bases de datos para enviar y recibir e-mails.

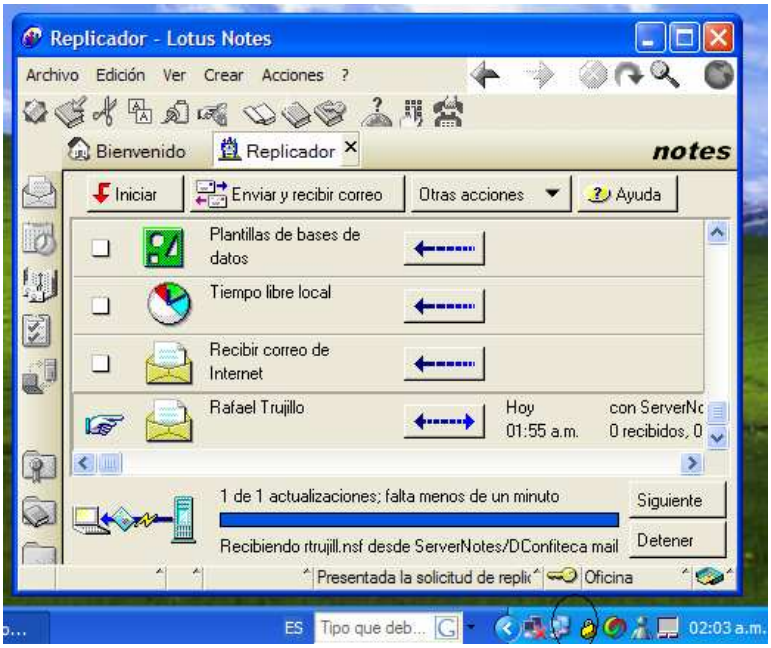

Figura 4.16. Conexión de correo electrónico.

- **Telnet**

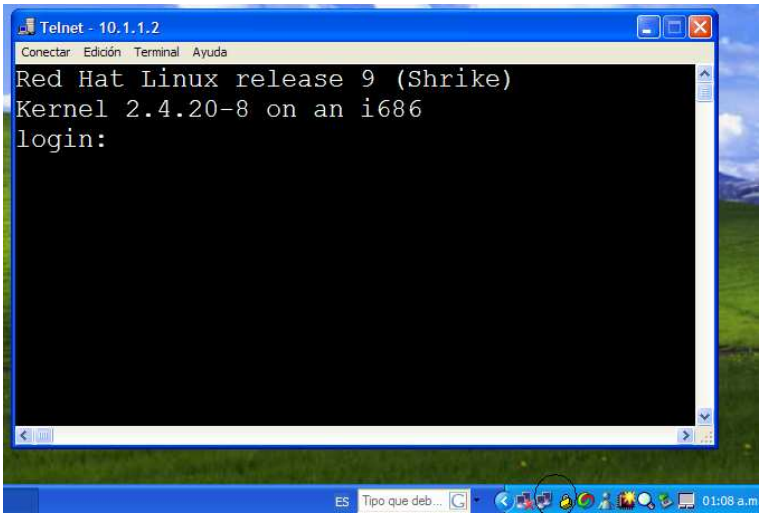

Figura 4.17. Prueba de conexión Telnet.

4.5. ANALISIS DE COSTOS DE LA IMPLEMENTACIÓN VPN

4.5.1. COSTO DEL PROTOTIPO VPN

Para implementar el prototipo VPN dentro de la empresa comercializadora se utilizaron recursos que ya dispone actualmente, por ejemplo la conexión a Internet, el Firewall, la red. Sin embargo es importante mencionar el costo de estos los elementos.

En el lado del cliente se invirtió en la PC y la conexión a Internet para las respectivas pruebas. Resumiendo, se invirtió en lo siguiente:

ITEM	DESCRIPCIÓN	VALOR
1	Firewall Cisco Pix 515 (servidor VPN)	$4.747,50
2	Computador Pentium IV (Cliente VPN)	$650,00
3	Conexión a Internet del Cliente VPN dial-up 20h	$9,00
4	Conexión a Internet corporativo 128/256 Kbps	$1.150,00
	TOTAL	**$6.556,50**

Tabla 4.6. Inversión en el prototipo VPN.

El costo de $6.556,50 representa la inversión que implica construir una VPN utilizando un Firewall como elemento principal. Claro que también hay que agregar las horas/hombre empleadas en la investigación y puesta en marcha, así como el consumo de línea telefónica del lado del cliente.

Si se considera ampliar este tipo de acceso VPN a más usuarios se debería considerar el costo que involucre para cada uno de ellos.

4.5.2. ANALISIS DE COSTOS PARA IMPLEMENTAR VPN EN TODAS LAS AGENCIAS

En este punto se analiza los elementos que intervendrían en la implementación de una VPN global, de tal forma que integre todas las agencias del país con la matriz. De esta forma se tendrá claro el panorama costo beneficio de la VPN en la empresa comercializadora.

4.5.2.1. Gastos Actuales

Por concepto de líneas dedicadas, la empresa comercializadora paga mensualmente a Andinadatos los valores correspondientes que se muestran en la tabla 4.7.

Punto A	Punto B	COSTO	COSTO MAS ICE
Confiteca	Portoviejo	$820,00	**$943,00**
Confiteca	Colón	$147,60	**$169,74**
Confiteca	Ibarra	$620,00	**$713,00**
Confiteca	Sto. Domingo	$360,00	**$414,00**
Confiteca	Guayaquil	$1.140,00	**$1.311,00**
Confiteca	Ambato	$620,00	**$713,00**
Confiteca	Cuenca	$820,00	**$943,00**
Confiteca	*Impsat (Quito)*	$1.150,00	**$1.150,00** *(Internet)*
		$5.677,60	**$6.356,74**

Tabla 4.7. Costos actuales por líneas dedicadas.[64]

Para las agencias que no disponen de líneas dedicadas, la empresa utiliza conexiones dial-up y paga mensualmente a Pacifictel, Andinatel y Ecuanet, los valores por consumo de línea telefónica y cuentas de correo electrónico respectivamente.

	Machala	Carcelén
Pago de Línea Telefónica	$312,02	$147,12
Cuentas de correo “Ecuanet”	$20,00	$10,00
Total	**$332,02**	**$157,12**

Tabla 4.8. Costos por enlaces Dial-up.[65]

Nota: los valores por consumo telefónico varía de acuerdo a su utilización mensual, se ha estimado un promedio diario de 4 horas para transmisión de datos que se agregan a la tarificación por llamadas telefónicas.

Entonces de acuerdo a las cantidades que se muestran en las tablas anteriores, Confiteca paga mensualmente **$6.845,88** entre líneas dedicadas, conexiones dial-up e Internet.

[64] Fuente: Andinadatos, Impsat.
[65] Fuente: Andinatel, Pacifictel y Ecuanet.

4.5.2.2. Posibles Costos con Enlaces VPN

Para implementar una VPN global en la empresa comercializadora, se debe tomar en cuenta la tecnología que se va a utilizar, el hardware o software y las conexiones a Internet. A continuación los costos de los equipos y conexiones a Internet, que se debería invertir de acuerdo al caso que se elija.

CIUDAD	VELOCIDAD	ÚLTIMA MILLA	PROVEEDOR	INSCRIPCIÓN	COSTO
Ibarra	128 Kbps	Cobre	Andinanet	$250,00	$255,00
Sto. Domingo	128 Kbps	Cobre	Andinanet	$250,00	$255,00
Ambato	128 Kbps	Cobre	Andinanet	$250,00	$255,00
Colón	128 Kbps	Cobre	Andinanet	$250,00	$255,00
Carcelén	128 Kbps	Cobre	Andinanet	$250,00	$255,00
Cuenca	128 Kbps	Cobre	Etapaonline	$250,00	$300,00
Guayaquil	128 Kbps	Fibra Optica	Telconet	$350,00	$400,00
Machala	128 Kbps	Radio Enlace	Telconet	$350,00	$400,00
Portoviejo	128 Kbps	Radio Enlace	Telconet	$350,00	$400,00
Quito Matriz	1024 Kbps	Fibra Optica	Impsat	$0,00	$2.000,00
			TOTAL	**$2.550,00**	**$4.775,00**

Tabla 4.9. Costos por acceso a Internet para las agencias.[66]

OPCIÓN	COSTO UNITARIO	CANTIDAD	TOTAL
Router (Vanguard)	$2.100,00	9	**$18.900,00**
Cisco Pix Firewall	$3.500,00	9	**$31.500,00**
Frees/wan (Servidor)	$1.700,00	10	**$17.000,00**
Gateway VoIP	$150,00	9	**$1.350,00**

Tabla 4.10. Opciones de inversión en hardware para VPN.[67]

La inversión inicial para las VPN sería el hardware y las inscripciones a Internet, en las tabla 4.9 y 4.10 constan los valores respectivos.

El costo mensual por Internet (de todas las agencias) le representaría a la empresa **$4.775,00**.

Se puede ver que es menor al valor que se paga por las telecomunicaciones actualmente (que consta en la página anterior).

Por lo tanto según este análisis de costos, al implementar las VPN en Confiteca el ahorro mensual sería de **$2.070,88**.

[66] Fuente: Andinanet, Telconet e Impsat.
[67] Fuente: Uniplex y Compuventas.

4.6. ANALISIS COMPARATIVO CON LINEAS DEDICADAS Y DIAL-UP

CRITERIO	LINEAS DEDICADAS	VPN
Bajo Costo	Los proveedores de estos servicios tienen un costo mucho más elevado por un enlace dedicado.	Reduce el costo de la red y los cargos por accesos al sitio.
Escalabilidad	La escalabilidad es un reto muy grande para las redes TDM ó Frame Relay	Es altamente escalable sobre todo en una red VPN porque no se necesitan conexiones especiales de un lugar a otro lugar. Simplifica las redes WAN.
Despliegue del Servicio Rápido	Regularmente tardan de 1 a 7 semanas en instalar un nuevo enlace	No hay configuración demorada; rápido de implementar
Flexibilidad	Regularmente desarrollada para conexiones de un lugar a otro lugar; de oficinas corporativas a sucursales. No permite el acceso controlado de asociados fuera de la red.	Extiende la red a oficinas remotas, Extranets y trabajadores móviles con una simple conexión. Permite conexiones seguras con asociados, proveedores y distribuidores.
Soporte de aplicaciones IP	Designada para transporte de capa 2. No tienen conocimiento de tráfico de capas más elevadas y ofrece poco valor agregado a capas superiores.	Provee las bases para desplegar servicios mejorados basados en IP tales como comunicaciones unificadas, video multicast, Extranet, acceso remoto y servicios de red seguros.
Cobertura geográfica	Limitada al área de cobertura del proveedor.	Mayor cobertura geográfica y ofrece la estructura para una conectividad mundial.
Acceso Remoto	Regularmente no ofrece acceso remoto	Extiende la seguridad de la red a trabajadores móviles.
Seguridad en la Red	Se basa en la separación de datos para la seguridad del transporte.	Provee una seguridad equivalente o mejor al Frame Relay ya que se utiliza IPSec.

Tabla 4.11. Cuadro VPN vs. Líneas Dedicadas.

CRITERIO	CONEXIONES DIAL-UP	VPN
Métodos de Conexión	El Cliente Dial-up utiliza líneas de teléfono comunes sobre la Red telefónica Conmutada (PSTN) para crear una conexión física hacia un modem en el servidor de acceso remoto en la LAN de la compañía.	El Cliente VPN establece una conexión local hacia el Internet y se conecta a la LAN a través de un VPN Server. Esta conexión provee acceso remoto seguro a través del Internet sobre una conexión TCP.
Costo	Requiere cargos telefónicos expensivos de larga distancia o herramientas de llamada en caso de que exista un número largo de clientes remotos viajando hacia una ubicación distante.	Los clientes remotos requieren solamente un ISP local para conectarse al Internet. Pueden reducir cargos telefónicos de larga distancia.
Requerimientos Hardware/telecomunicación	Requiere muchas líneas telefónicas entrantes y hardware in-house (como Servidor de Acceso remoto, banco de modems, etc).	Requiere una conexión existente hacia el Internet y un Servidor VPN en la LAN.

Tabla 4.12. Conexiones VPN vs. Dial-up.

Luego de ver las comparativas tanto en tecnología como en costos, se puede decir que las VPN tienen muchas ventajas con respecto a las conexiones de líneas dedicadas y dial-up, por lo que siempre serán una alternativa para la conectividad en una organización.

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Luego de finalizar el proyecto, se puede concluir que se cumplieron con los objetivos propuestos para el mismo. Se llegó a diseñar algunas alternativas de implementación VPN en la empresa comercializadora y se construyó un prototipo demostrativo.
- La VPN de Acceso Remoto implementada como prototipo, tiene las funcionalidades de las Redes Privadas Virtuales, y se comprobó que es ideal para las personas que viajan constantemente o que se conectan desde su hogar hacia la oficina central, esta facilidad hace que aumente la productividad de los empleados ya que pueden acceder a la red desde cualquier parte.
- Se analizó que la tecnología VPN es una alternativa totalmente viable, la empresa comercializadora está en la posibilidad de integrar sus sucursales, usuarios móviles y socios estratégicos a un costo efectivo, comparado con las tradicionales líneas dedicadas que arrienda hasta ahora, ya que utilizaría el Internet que está creciendo notoriamente en nuestro país.
- En este proyecto, el protocolo IPSec es el encargado de brindar la seguridad necesaria a la información de la empresa dentro de la VPN, al ser IPSec un estándar difundido ampliamente, permite la interoperatividad de los sistemas de diversos fabricantes.
- Las VPN también tienen vulnerabilidades, entre sus debilidades están los puntos de falla en la ruta y por mínimos que sean pueden desconectar la red entera, el overhead se ve afectado por el proceso de encripción y encapsulación, y la detección de intrusos (IDS) se torna difícil ya que el tráfico va encriptado.
- Definitivamente las VPN seguirán siendo motivo de investigación, en un futuro no muy lejano, muchos estaremos utilizando esta tecnología incluso sin saberlo y el aporte que demos todos los profesionales involucrados en las redes de información será fundamental.

5.2. RECOMENDACIONES

- Es recomendable que a la hora de escoger la opción entre software ó hardware para implementar una VPN, la decisión debe ser analizada en muchos aspectos como son: el número de usuarios, conocimientos del personal de Tecnología y los recursos para la inversión, de ello dependerá la opción correcta.
- Al implementar una VPN basada en un Firewall se recomienda que el número de usuarios no sea elevado, esto reduce el rendimiento del dispositivo e incluso se podría necesitar de una tarjeta aceleradora adicional para poder mantener el equipo operable.
- Se recomienda evaluar muy cuidadosamente el proveedor de Internet, la calidad del servicio prestado es fundamental en el rendimiento de las Redes Privadas Virtuales, se deberá tomar en cuenta la tecnología de conexión, la disponibilidad del servicio, nivel de compartición y soporte técnico todos los días del año.
- También se recomienda cuantificar muy bien el ancho de banda de los accesos a Internet, esta vez además de la navegación, downloads, juegos online, video; van a viajar datos incluso más importantes por el mismo canal. Entonces es importante contratar un ancho de banda que pueda soportar ese tráfico y administrarlo de la mejor manera.
- Es recomendable considerar que nuestro país es uno de los más caros del mundo en cuanto a las telecomunicaciones (Internet y líneas dedicadas), esto puede influir en la estimación del ahorro que se pretenda con las VPN, incluso en algún caso podría salir más costoso que las líneas dedicadas.
- Se debe evitar utilizar el algoritmo DES para el cifrado de datos porque al ser de 64 bits es más fácil descifrarlo y actualmente es considerado inseguro, se recomienda utilizar 3DES u otro más difícil de descifrar.

BIBLIOGRAFÍA

LIBROS:

[1] Redes Privadas Virtuales con Linux.
Oleg Kolesnikov & Brian Hatch, Primera Edición, Editorial: Prentice Hall, año 2003.

[2] Internet Architecture: An Introduction to IP Protocols.
Uyless Black, Primera Edición, Editorial: Prentice Hall, año 2000.

[3] Redes de Computadoras
Andrew Tanenbaum, Tercera Edición, Editorial: Prentice Hall, año 1997.

[4] Internetworking: A Guide to Network Communications LAN to LAN; LAN to WAN.
MILLER A. MARK, Primera Edición, Editorial: M&T Books, año 1991.

[5] Security in Computing
Pfeeger P. Charles, Second Edition, Editorial: Prentice Hall PTR, año 1997

SITIOS DE INTERNET:

[1] http://www.cisco.com

[2]
http://www.tid.es/presencia/publicaciones/comsid/esp/articulos/vol72/internet/internet.html.

[3] http://www.tid.es/presencia/publicaciones/comsid/esp/23/04.pdf.

[4] http://foundation.verizon.com/spanish/06007_service.shtml.

[5] http://www.internetghana.com/wan.htm#clear.

[6] http://www.geocities.com/v.iniestra/apuntes/telefonia/.

[7] http://www.internetghana.com/wan.htm#clear.

[8] http://www.microsoft.com/technet/itsolutions/network/security/ipsecimp.mspx.

[9] http://www.freeswan.ca.

[10] http://es.wikipedia.org/wiki/ATM.

[11] http://www.mundotutoriales.com/tutoriales_frame_relay-mdpal14447.htm.

[12] http://www.sunrisetelecom.com/espanol/frame_relay.pdf.

[13] www.lucent.com/minds/techjournal/pdf/jan-mar1998/paper04.pdf.

[14] http://www.cisco.com/en/US/products/sw/secursw/ps2308/prod_release_note09186a00802d398a.html.

[15] http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080124551.html.

[16] http://www.vanguardnetworks.com/products/whitepaper_Vanguard_IP_VPN.pdf.

ANEXOS

ANEXO 1: GLOSARIO DE TÉRMINOS

Active Directory.- directorio activo. Servicio de directorio desarrollado por Microsoft, que se encuentra integrado en la arquitectura de Windows 2000 Server. Es un sistema centralizado que automatiza la gestión de los datos de usuarios, la seguridad, y los recursos distribuidos en la red.

AES.- Advanced Encryption Standard.

AH.- Autentication Header.

Aplicación.- Software que realiza una función útil. Los programas que se utilizan para realizar alguna función (como correo electrónico, FTP, etc.) son las aplicaciones cliente.

ARPANet.- Siglas de la expresión inglesa Advanced Research Projects Agency Network (Red de la Agencia de Proyectos Avanzados de Investigación), red precursora a la Internet.

Autoridad de Certificación.- En inglés "Certificate Authority". Un emisor de Certificados de Seguridad para las conexiones SSL.

Baud.- Unidad que representa la velocidad de transferencia de la información. Es equivalente a bytes por segundo.

bit.- Unidad elemental de la información. El nombre proviene del inglés, "binary digit" o dígito binario. Originalmente explicada por Sócrates en los Diálogos de Platón, habiéndole llamado "diada" que sería su denominación óptima.

byte.- Conjunto de 8 bits. Puesto que 8 bits es la mínima cantidad requerida para representar los símbolos alfanuméricos.

bps.- Iniciales de bits por segundo.

Cableado.- Columna vertebral de una red que utiliza un medio físico de cable, casi siempre del tipo de red de área local (LAN), que lleva la información de un nodo a otro. La reciente aparición de las redes inalámbricas ha roto el esquema tradicional al no utilizar ningún tipo de cableado.

Certificado de Seguridad.- Archivo de texto usado por el protocolo SSL para establecer una conexión segura. La información en los certificados de seguridad incluye a quien pertenecen, al emisor, un número único de identificación, fechas de validez y una "huella" encriptada que se puede usar para verificar el contenido del certificado.
Para que exista una conexión SSL ambas partes deben poseer un Certificado de Seguridad válido.

Cliente- [Client] Máquina que conectada a una red, solicita acciones a otra que actúa como servidor.

Correo Electrónico.- (*e-mail*) Permite el intercambio de mensajes entre personas conectadas a una red de manera similar al correo tradicional. Entre las aplicaciones cliente de correo electrónico tenemos a Eudora, Mail , Pine, Pegasus, etc. La definición acerca del correo electrónico fue especificada en el RFC # 822.

DES (estándar de cifrado de datos).- Es un cifrado de bloques que cifra datos en bloques de 64 bits. DES es un algoritmo simétrico que utiliza el mismo algoritmo y la misma clave para cifrar y descifrar. DES ha sido reemplazado por DES triple.

DES triple.- Se trata del cifrado DES triple (3DES). Es una variación del algoritmo de cifrado de bloques DES que cifra el texto sin formato con una clave, cifra el texto cifrado resultante con una segunda clave y, por último, cifra el resultado del segundo cifrado con una tercera clave. DES triple es un algoritmo simétrico que utiliza el mismo algoritmo y las mismas claves para cifrar y descifrar.

Dialup.- (conexión por línea conmutada) Conexión temporal, en oposición a conexión dedicada o permanente, establecida entre ordenadores por línea telefónica normal.

E1.- Norma europea de transmisión de banda ancha formado por 32 canales individuales de 64 kbps, lo que ofrece tasas de transmisión de 2.048 Mbps.

Encriptar.- proteger archivos expresando su contenido en un lenguaje cifrado. Los lenguajes cifrados simples consisten, por ejemplo, en la sustitución de letras por números.

Ethernet.- Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus. Y que tiene un ancho de banda de10 Mbps.

Extranet.- La red usada por una empresa para conectarse con sus clientes y socios de negocios.

Firewall.- En español, barrera de fuego. Programa o equipo que separa a una red local (LAN) en dos o más partes con propósitos de seguridad.

Gateway.- O compuerta es un programa o equipo que se encarga de traducir la información contenida en dos protocolos diferentes.

GNU.- Fundación para el Software Libre (FSF - *Free Software Foundation*) Busca eliminar las restricciones de uso, copia, modificación y distribución del software. Actualmente se encuentra apoyando el desarrollo de sistemas operativos (Linux), compiladores (compilador GNU C Compiler (gcc), Perl), etc. Trata de promover, desarrollar y usar del software libre en todas las áreas de la computación.

Hardware.- Los componentes físicos de un sistema de computadora, incluyendo cualquier equipo periférico.

IANA.- Internet Assigned Number Authority. En 1999 sustituida por ICANN.

IKE.- Internet Key Exchange.

Internet.- [De inter, internacional y net, en inglés, red].- Todas las computadoras del mundo conectadas entre si, como si se tratara de una enredadera o red.

Intranet.- [De intra, interno y net, en inglés, red].- Red interna de una empresa, que parcialmente puede exponer información al exterior vía Internet.

IP o dirección IP.- [IP Address] Dirección en el protocolo del Internet que identifica a una máquina conectada.

ISP.- Siglas de Internet Service Provider (Proveedor del servicio de Internet). Empresa que proporciona el servicio de acceso a la red Internet.

KLIPS.- (Kernel IPSec) implementa AH, ESP y manejo de paquetes dentro del kernel linux.

Lista de Control de Acceso (ACL).- Lista de entidades, con sus derechos de acceso, que están autorizadas a acceder a un recurso. Solo se permite acceder a aquellos que estén en la lista.

OSI.- Interconexión de Sistemas Abiertos (*Open Systems Interconnect*). Es el protocolo en el que se apoya Internet. Establece la manera como se realiza la comunicación entre dos computadoras a través de siete capas: Física, Datos, Red, Transporte, Sesión, Presentación y Aplicación.

PIX.- Private Internet Exchange.

PKCS.- Public Key Common Standards.

Pluto.- Demonio que implementa IKE en freeswan (Linux).

Protocolo.- [Protocol] El conjunto de reglas que permite intercambiar datos entre dos máquinas.

Ruteador.- [En inglés, Router]. Dispositivo que enruta los paquetes de información electrónica tomando decisiones de tráfico, en base a las condiciones de la red.

Servidor.- [Server] Máquina conectada a otras que ejecuta una acción a solicitud de las otras (clientes).

Slip.- *Serial Line Internet Protocol*. Es una implementación de TCP/IP por líneas seriales. Para conectar un módem a Internet es necesario establecer un protocolo SLIP o PPP.

Software.- Programas informáticos; instrucciones que hacen funcionar el hardware.

TCP/IP.- Tomado de la expresión en inglés Transmission Control Protocol/Internet Protocol (Protocolo de control de transmisiones y protocolo de la Internet). Es el conjunto de Protocolos que definen la comunicación Internet.

Topología de red.- Se refiere a cómo se establece y se cablea físicamente una red. La elección de la topología afectará la facilidad de la instalación, el costo del cable y la confiabilidad de la red. Tres de las topologías principales de red son la topología de bus, de estrella, y de anillo.

Usuario.- Persona que utiliza el ordenador en general y una aplicación en particular.

VPN.- Virtual Private Network.

ANEXO 2: RESUMEN DE LA CONFIGURACIÓN DEL FIREWALL

PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz-1 security50
hostname confiteca
domain-name ciscopix.com
access-list acl-no-nat-vpn permit ip V.W.1.0 255.255.255.0 X.Y.200.0 255.255.255.0
access-list acl-no-nat-vpn permit ip P.Q.2.0 255.255.255.0 X.Y.200.0 255.255.255.0
access-list acl-no-nat-vpn permit ip M.N.3.0 255.255.255.0 X.Y.200.0 255.255.255.0
ip local pool vpn-pool X.Y.200.1-X.Y.200.254
nat (inside) 0 access-list acl-no-nat-vpn
nat (dmz-1) 0 access-list acl-no-nat-vpn
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set trans-remota esp-3des esp-md5-hmac
crypto dynamic-map vpn-dyn 10 set transform-set trans-remota
crypto map vpn-out 10 ipsec-isakmp dynamic vpn-dyn
crypto map vpn-out interface outside
isakmp enable outside
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 14400
vpngroup vpn-grupo address-pool vpn-pool
vpngroup vpn-grupo split-tunnel acl-no-nat-vpn
vpngroup vpn-grupo idle-time 1800
vpngroup vpn-grupo password ********

ANEXO 3: PARÁMETROS DE LA VERSIÓN DEL FIREWALL

confiteca# show ver

Cisco PIX Firewall Version 6.2(2)
Cisco PIX Device Manager Version 2.1(1)

Compiled on Fri 07-Jun-02 17:49 by morlee

confiteca up 1 hour 47 mins

Hardware: PIX-515, 32 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.6bf6.d465, irq 11
1: ethernet1: address is 0003.6bf6.d466, irq 10
2: ethernet2: address is 0003.479b.0387, irq 9
Licensed Features:
Failover: Disabled
VPN-DES: Enabled
VPN-3DES: Enabled
Maximum Interfaces: 3
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled
Inside Hosts: Unlimited
Throughput: Unlimited
IKE peers: Unlimited

Running Activation Key: 0x085ab201 0xc0221f3e 0x2449213a 0xb113ef7d
Configuration last modified by enable_15 at 02:46:22.216 UTC Mon Mar 13 2006

ANEXO 4: COMANDOS PIX CLASIFICADOS POR MODOS

MODO PRIVILEGIADO

pix# ?

arp Change or view the arp table, and set the arp timeout value
auth-prompt Customize authentication challenge, reject or acceptance prompt
configure Configure from terminal, floppy, or memory, clear configure
copy Copy image from TFTP server into flash.
debug Debug packets or ICMP tracings through the PIX Firewall.
disable Exit from privileged mode
enable Modify enable password
flashfs Show or destroy filesystem information
kill Terminate a telnet session
pager Control page length for pagination
passwd Change Telnet console access password
ping Test connectivity from specified interface to <ip>
quit Disable, end configuration or logout
reload Halt and reload system
session Access an internal AccessPro router console
terminal Set terminal line parameters
who Show active administration sessions on PIX
write Write config to net, flash, floppy, or terminal, or erase flash

MODO DE CONFIGURACIÓN

pix(config)# ?

aaa Enable, disable, or view TACACS+ or RADIUS
user authentication, authorization and accounting
access-group Bind an access-list to an interface to filter inbound traffic
access-list Add an access list
age This command is deprecated. See ipsec, isakmp, map, ca commands
alias Administer overlapping addresses with dual NAT.
apply Apply outbound lists to source or destination IP addresses
arp Change or view the arp table, and set the arp timeout value
auth-prompt Customize authentication challenge, reject or acceptance prompt

aaa-server Define AAA Server group
ca CEP (Certificate Enrollment Protocol)
Create and enroll RSA key pairs into a PKI (Public Key Infrastructure).
clock Show and set the date and time of PIX
conduit Add conduit access to higher security level network or ICMP
crypto Configure IPsec, IKE, and CA
configure Configure from terminal, floppy, or memory, clear configure
copy Copy image from TFTP server into flash.
debug Debug packets or ICMP tracings through the PIX Firewall.
disable Exit from privileged mode
domain-name Change domain name
dynamic-map Specify a dynamic crypto map template
enable Modify enable password
established Allow inbound connections based on established connections
failover Enable/disable PIX failover feature to a standby PIX
filter Enable, disable, or view URL, Java, and ActiveX filtering
fixup Add or delete PIX service and feature defaults
flashfs Show or destroy filesystem information
ipsec Configure IPSEC policy
isakmp Configure ISAKMP policy
global Specify, delete or view global address pools,
or designate a PAT(Port Address Translated) address
hostname Change host name
vpdn Configure VPDN (PPTP) Policy
interface Identify network interface type, speed duplex, and if shutdown
ip Set ip address for specified interface,
define a local address pool, or
toggle Unicast Reverse Path Forwarding on an interface.
kill Terminate a telnet session
link This command is deprecated. See ipsec, isakmp, map, ca commands
linkpath This command is deprecated. See ipsec, isakmp, map, ca commands
logging Enable logging facility
map Configure IPsec crypto map

mtu Specify MTU(Maximum Transmission Unit) for an interface
name Associate a name with an IP address
nameif Assign a name to an interface
names Enable, disable or display IP address to name conversion
nat Associate a network with a pool of global IP addresses
outbound Create an outbound access list
pager Control page length for pagination
passwd Change Telnet console access password
ping Test connectivity from specified interface to <ip>
quit Disable, end configuration or logout
radius-server Specify a RADIUS aaa server
reload Halt and reload system
rip Broadcast default route or passive RIP
route Enter a static route for an interface
session Access an internal AccessPro router console
snmp-server Provide SNMP and event information
sysopt Set system functional option
static Map a higher security level host address to global address
tacacs-server Specify a TACACS+ server
telnet Add telnet access to PIX console and set idle timeout
terminal Set terminal line parameters
tftp-server Specify default TFTP server address and directory
timeout Set the maximum idle times
url-cache Enable URL caching
url-server Specify a URL filter server
virtual Set address for authentication virtual servers
who Show active administration sessions on PIX
write Write config to net, flash, floppy, or terminal, or erase flash

ANEXO 5: SINTAXIS DE COMANDOS UTILIZADOS PARA LA VPN

- **access-list**

Create an access list. (Configuration mode.)
access-list *acl_name* [**deny** | **permit**] *protocol src_addr src_mask operator port dest_addr dest_mask operator port*

access-list *acl_name* [**deny** | **permit**] **icmp** *src_addr src_mask operator port dest_addr dest_mask operator port icmp_type*

no access-list *acl_name* [[**deny** | **permit**] *protocol src_addr src_mask operator port dest_addr dest_mask operator port*]

clear access-list [*acl_name* [**deny** | **permit**] **icmp** *src_addr src_mask operator port dest_addr dest_mask operator port icmp_type*]

show access-list

- **crypto ipsec**

Create, view, or delete IPSec security associations, security association global lifetime values, and global transform sets. (Configuration mode.)
crypto ipsec security-association lifetime seconds *seconds* | **kilobytes** *kilobytes*

no crypto ipsec security-association lifetime seconds | **kilobytes**

show crypto ipsec security-association lifetime

crypto ipsec transform-set *transform-set-name transform1* [*transform2* [*transform3*]]

no crypto ipsec transform-set *transform-set-name*

show crypto ipsec transform-set [**tag** *transform-set-name*]

clear [**crypto**] **ipsec sa**

clear [**crypto**] **ipsec sa counters**

clear [**crypto**] **ipsec sa entry** *destination-address protocol spi*

clear [**crypto**] **ipsec sa map** *map-name*

clear [**crypto**] **ipsec sa peer**

show crypto ipsec sa [**map** *map-name* | **address** | **identity**] [**detail**]

- **crypto map**

To create, modify, view or delete a crypto map entry. Also used to delete a crypto map set. (Configuration mode.)
crypto map *map-name* **client authentication** *aaa-server-name*

no crypto map *map-name* **client authentication** *aaa-server-name*

crypto map *map-name* **client configuration address initiate** | **respond**

no crypto map *map-name* **client configuration address initiate** | **respond**

crypto map *map-name* **interface** *interface-name*

no crypto map *map-name* **interface** *interface-name*

show crypto map [interface *interface-name* **| tag** map-name]

crypto map *map-name seq-num* **ipsec-isakmp** | **ipsec-manual** [**dynamic***dynamic-map-name*]

no crypto map *map-name seq-num*

crypto map *map-name seq-num* **match address** *acl_name*

no crypto map *map-name seq-num* **match address** *acl_name*

crypto map *map-name seq-num* **set peer** *hostname* | *ip-address*

no crypto map *map-name seq-num* **set peer** *hostname* | *ip-address*

crypto map *map-name seq-num* **set pfs** [**group1 | group2**]

no crypto map *map-name seq-num* **set pfs**

crypto map *map-name seq-num* **set security-association lifetime seconds***seconds* | **kilobytes** *kilobytes*

no crypto map *map-name seq-num* **set security-association lifetime seconds***seconds* | **kilobytes** *kilobytes*

crypto map *map-name* **set session-key inbound | outbound ah** *spi hex-key-string*

no crypto map *map-name seq-num* **set session-key inbound | outbound ah**

crypto map *map-name* **set session-key inbound | outbound esp** *spi* **cipher** *hex-key-string* **[authenticator** *hex-key-string*]

no crypto map *map-name seq-num* **set session-key inbound | outbound esp**

crypto map *map-name seq-num* **set transform-set** *transform-set-name1* [*transform-set-name6*]

no crypto map *map-name seq-num* **set transform-set** *transform-set-name1* [*transform-set-name6*]

- **ip local pool**

Identify addresses for a local pool. (Configuration mode)
ip local pool *pool_name pool_start-address*[*-pool_end-address]*

no ip local pool *pool_name pool_start-address*[*-pool_end-address*]

show ip local pool *pool_name ip_address*[*-ip_address*]

- **isakmp**

Negotiates IPSec security associations and enables IPSec secure communications.
(Configuration mode.)
isakmp client configuration address-pool local *pool-name* [*interface-name*]

no isakmp client configuration address-pool local *pool-name*

isakmp enable *interface-name*

no isakmp enable *interface-name*

isakmp identity address | **hostname**

no isakmp identity address | **hostname**

isakmp key *keystring* **address** *peer-address* [**netmask** *mask*] [**no-xauth**] [**no-config-mode**]

no isakmp key *keystring* **address** *peer-address* [**netmask** *mask*][**no-xauth**] [**no-config-mode**]

isakmp peer fqdn *fqdn* **no-xauth no-config-mode**

no isakmp peer fqdn *fqdn* **no-xauth no-config-mode**

isakmp policy *priority* **authentication** *pre-share* | *rsa-sig*

no isakmp policy *priority* **authentication** *pre-share* | *rsa-sig*

isakmp policy *priority* **encryption** *des* **|** *3des*

no isakmp policy *priority* **encryption** *des* **|** *3des*

isakmp policy *priority* **group1** | **2**

no isakmp policy *priority* **group1** | **2**

isakmp policy *priority* **hash** *md5* **|** *sha*

no isakmp policy *priority* **hash** *md5* **|** *sha*

isakmp policy *priority* **lifetime***seconds*

no isakmp policy *priority* **lifetime***seconds*

show isakmp policy

show isakmp sa

clear [**crypto**] **isakmp** sa

clear isakmp

- **nat**

Associate a network with a pool of global IP addresses. (Configuration mode.)
nat [(*if_name*)] *nat_id local_ip* [*netmask* [*max_conns* [*em_limit*]]] [**norandomseq**]

nat [(*if_name*)] **0 access-list** *acl_name*

nat [(*if_name*)] **0** *local_ip* [*netmask* [*max_conns* [*em_limit*]]] [**norandomseq**]

no nat [[(*if_name*)] *nat_id local_ip* [*netmask* [*max_conns* [*em_limit*]]]] [**norandomseq**]

no nat [(*if_name*)] **0 access-list** *acl_name*

show nat