UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

T E S I S

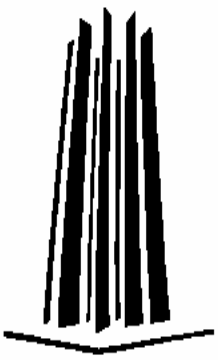
PROYECTO DE UNA RED PRIVADA VIRTUAL (VPN)A LA EMPRESA PROYECCIÓN Y ADMINISTRACIÓN EMPRESARIAL DE MÉXICO S.A. DE C.V.

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN

P R E S E N T A:

ALMAZÁN GALENO ENRIQUE

ASESORA:
CATARINA TAFOLLA RANGEL



SAN JUAN DE ARAGÓN EDO. DE MEX. 2007

AGRADECIMIENTOS

A mi mamá…..

Por apoyarme y quererme mucho, por todo esfuerzo y cada gota de sudor, por cada abrazo que me hicieron sentir que nada iba a pasar, y lo más importante, por darme la vida y darme la oportunidad de vivirla y ser alguien.

Te quiero mucho mami.

A mis abuelos…..

Por tomar esa gran responsabilidad de criarme y educarme como a un hijo propio siendo como mis padres, haciéndome una persona responsable y de bien. A mi abuela por cuidarme cuando estaba en el hospital y lo más lindo por quererme y protegerme, a mi abuelo por esforzarse cada día y apostarle a todo por mí y por creer que si podría ser alguien en la vida y como ven, ahora lo soy.

Los quiero mucho.

A mi familia…..

Por verme como su hermano menor, cuidarme y educarme como tal, por quererme mucho y alentarme cada día a ser mejor persona, pero sobre todo por confiar en mí y en lo grande que podría llegar a ser. Este pequeño triunfo por favor siéntalo también como suyo.

A mi asesora….

Por los conocimientos que aportados a este trabajo, por confiar en mí y guiarme en este último paso para terminar una etapa muy importante en mi vida, pero sobre todo muchas gracias por toda su paciencia y por alentarme cada día para ver este gran sueño y hacerlo realidad.

A mis amigos….

Por estar ahí cuando los necesitaba brindándome su apoyo y amistad incondicional, por creer en mí, alentarme y darme la mano para no caer y seguir adelante y llegar este día tan importante y especial en mi vida.

A mi angelito….

Por ofrecerme su amistad y amor incondicional, por cuidarme y amarme como mi angelito de la guarda, por cada sonrisa que me decía que todo iba a estar bien, por estar siempre ahí, al pie del cañón por cada abrazo y cada beso que hacen que me coma el mundo de un bocado y lo más importante por ser el motor para llegar hasta el día de hoy, compartir este y muchos momentos importantes y especiales en mi vida; y con ello ser lo que soy ahora. TE AMO

ÌNDICE

TEMA **PÀGINA**

Introducción.....1

Capítulo 1
Panorámica general de las redes.....2

1.1 ¿Qué es una red de computadoras y cómo funciona?.....2
1.1.1 Historia de las redes de computadoras.....3
1.1.2 Estructura de una red de computadoras.....5
1.1.3 Uso de las redes de computadoras.....7
1.2 Tipos y clasificación de las redes.....9
1.2.1 Clasificación de redes por el área que abarcan y por su topología.....9
1.3 Arquitectura de red y el modelo OSI.....16
1.4 ¿Qué es una VPN y cómo funciona?.....21
1.4.1 Elementos de una VPN.....23
1.4.2 Tipos y conexiones de VPN.....24
1.4.3 Tecnología de las VPN's.....28
1.5 Internet como medio de comunicación.....31
1.5.1 Medios de Comunicación.....31
1.5.2 Internet como distintos canales de comunicación.....32
1.5.3 Internet como nuevo "Medio de Comunicación.....36

Capítulo 2
Antecedentes del proyecto.....38

2.1 ¿Cuál es la empresa?.....38
2.2 Situación actual.....38
2.3 Propuesta de solución.....39

Capítulo 3
Desarrollo del proyecto de VPN para la empresa Proyección y Administración Empresarial S.A. de C.V......42

3.1 Insumos a utilizar en el proyecto para la instalación de la VPN.....42
3.2 Procedimiento a utilizar en el proyecto de instalación de la VPN.....43
3.3 Plano o croquis de las redes en la empresa.....46
3.4 Diagrama de Gantt del proyecto de VPN.....50
3.5 Ruta crítica o diagrama de Pert del proyecto de VPN.....52
3.6 Pruebas realizadas al proyecto de VPN.....53
3.7 Implantación del proyecto de VPN.....55
3.8 Mantenimiento del proyecto de VPN.....56

Capítulo 4
Análisis de beneficios logrados con la VPN......58

4.1 Ventajas técnicas y económicas obtenidas con la implementación de este proyecto.....59
4.2 Limitaciones técnicas y económicas obtenidas con la implementación de este proyecto.....66

Conclusiones.....71
Glosario.....72
Bibliografía.....77

INTRODUCCIÓN

En esta tesis se propone el desarrollo de un proyecto para la empresa Proyección y Administración Empresarial S.A. de C.V. y con el propósito de instalar una VPN, lo que representa una buena alternativa para la comunicación y manejo de la información entre equipos remotos no sólo para esta empresa sino para otras más las cuales cuentan con filiales localizadas en lugares lejanos.

En el capítulo uno se revisa la panorámica de lo que son las redes de computadoras, cuales son sus elementos, así como la clasificación y métodos de transmisión en las mismas. En general es un breve marco teórico acerca del tema principal del proyecto que es una VPN dándose también una explicación de que es y en que consiste este tipo red.

En el capítulo dos se presentan los objetivos del trabajo y del proyecto, así como los objetivos generales y los particulares. También se justifica la elaboración del mismo.

En el capítulo tres se explica en que consiste el proyecto, los procedimientos y los insumos necesarios para la realización del mismo; incluyendo también un listado de costos de los insumos necesarios.

Por último en el capítulo cuatro se hace un análisis de los beneficios logrados con la realización del proyecto, y se mencionan las ventajas y limitaciones del mismo para llegar a la obtención de conclusiones.

CAPÍTULO 1 PANORÁMICA GENERAL DE LAS REDES

1.1 ¿Qué es una red de computadoras y cómo funciona?

¿Qué es una red de computadoras?

A medida que crece nuestra habilidad para recolectar, procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez. En este aspecto la industria de la computación ha tenido un progreso espectacular en muy corto tiempo; ya que el viejo modelo de tener una sola computadora para satisfacer todas las necesidades de cálculo de una organización o empresa se ha reemplazando con rapidez por el modelo en red, pero ¿qué es una red de computadoras?

Una red de computadoras (también llamada red de ordenadores, red informática o simplemente red) es un conjunto de dos o más computadoras o dispositivos conectados entre sí que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (e-mail, chat, juegos), etc. También se define como conjunto de técnicas, conexiones físicas y programas utilizados para conectar dos o más computadoras. Esta conexión no necesariamente tiene que ser a través de un hilo de cobre, también puede hacerse mediante el uso de láser, microondas y satélites de comunicación.

¿Cómo funciona una red de computadoras?

La comunicación entre las computadoras se realiza por medio de “paquetes”, que en realidad son ráfagas de electricidad que corresponden con el lenguaje binario, que es el que entienden estos dispositivos para proporcionar toda la información relativa a través de la red. Para que esta información pueda ser intercambiada entre el equipo fuente y el equipo destino se necesitan dos partes fundamentales que son el software y hardware de red.

Desde una perspectiva más comunicativa se puede decir que existe una red cuando están involucrados un componente humano que comunica, un componente tecnológico (computadoras, televisión, telecomunicaciones) y un componente administrativo (institución o instituciones que mantienen los servicios). Una red, más que varias computadoras conectadas, la constituyen varias personas que solicitan, proporcionan e intercambian información a través de sistemas de comunicación.

1.1.1 Historia de las Redes

Las redes surgen de la necesidad de compartir recursos de alto costo entre varias personas. En los inicios de las computadoras, los recursos eran de un costo muy alto; en los centros de investigación era necesario que todos los investigadores tuvieran acceso a este tipo de recursos y que estos recursos fueran distribuidos de tal manera que hubiera un desperdicio de tiempo de procesamiento.

Las primeras redes de computadoras que se crearon, fueron del tipo centralizado, es decir, un procesador central, el cual tenía el control y las terminales que le enviaban las tareas a realizar al procesador. Estas redes exigían que la conexión se realizara punto a punto. El desarrollo de la tecnología permitió tener redes que comunicaban computadoras en sitios distantes, este avance obligó a crear protocolos de comunicación entre las computadoras. Estos protocolos eran propietarios de los fabricantes de las máquinas. Aquí es donde se comienza a ver la necesidad de crear de protocolos estándares para comunicar computadoras y redes de diferentes fabricantes y de diferentes tipos.

En 1973, la Agencia de Investigaciones avanzadas de la Defensa de los Estados Unidos (DARPA) inició un programa para investigar las técnicas y las tecnologías para la interconexión de redes de diversos tipos. El objetivo era desarrollar protocolos de comunicación los cuales pueden permitir a redes de computadoras comunicarse en forma transparente a través de múltiples redes.

Este proyecto fue llamado *Internetting Project*, y el sistema de redes que emergió de estas investigaciones fue conocido como Internet. El sistema de protocolos desarrollados en el transcurso de esta investigación, dio forma a lo que después se conocería como la suite del protocolo TCP/IP.

En 1883 y 1984 surgieron los primeros entornos de servidores de ficheros para las redes de área local. Entre las compañías destacadas se encuentran: Novell Inc., 3com Corporation, AT&T e IBM; aunque todas ellas diferían mostraban entornos centralizados donde una computadora hacía las veces de servidor (con sistema operativo de red instalado y los datos

compartidos) y el resto de los equipos funcionaban con una versión de sistema operativo más “ligero”.

En 1986, la National Science Foundation (NSF) de E. U. inició el desarrollo de la NSFNET (qué es?), la cual provee un servicio de comunicación muy importante para la Internet. Hacia 1990, este tipo de redes locales triunfó en el mundo de la empresa y la industria de las redes creció a una velocidad impresionante.

Hoy en día, las redes de computadoras son lago más que un entorno centralizado de gestión de archivos. El desarrollo de la tecnología ha posibilitado el incremento en velocidad de transmisión y fiabilidad lo que ha supuesto una extensión de sus capacidades. La tendencia actual se orienta hoy en día hacia las redes distribuidas (en lugar de las centralizadas, donde cada computadora es cliente, pero también puede ser servidor de datos y dispositivos).

1.1.2 Estructura de una red

Al igual que una computadora, la red posee dos partes fundamentales:

1.- Dispositivos de red: Son el conjunto de elementos físicos que hacen posible la comunicación entre el emisor y l receptor, estos son:

a) Canal de comunicación: es el medio por el cual irá la información.

b) Nodos intermedios: Son los elementos encargados de realizar la selección del mejor camino por cual circulará la información (en caso de que exista un camino), también funcionarán como emisores y receptores.

2.- Programas de red: A este tipo pertenecen todos los programas que permiten controlar el funcionamiento de la red para hacerla más fiable.

En toda red existe una colección de computadoras para correr programas de usuario (aplicaciones). Se utiliza la terminología de una de las primeras redes, denominada ARPANET, y se llaman hostales las máquinas antes mencionadas. También, en algunas ocasiones se utiliza el término sistema terminal o sistema final. Los hostales están conectados mediante una subred; el trabajo de la subred consiste en enviar mensajes entre hostales, de la misma manera como el sistema telefónico envía palabras entre la persona que habla y la que escucha. El diseño completo de la red se simplifica notablemente cuando se separan los aspectos puros de comunicación de la red (la subred), de los aspectos de aplicación (los hostales).

Una subred en la mayor parte de las redes de área extendida consiste de dos componentes diferentes: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (conocidas como circuitos, canales o troncales), se encargan de mover bits entre computadoras.

Los elementos de conmutación son computadoras especializadas que se utilizan para conectar dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación deberá seleccionar una línea de salida para reexpedirlos.

1.1.3 Usos de las redes de computadoras

Antes de conocer los usos de las redes es importante mencionar que las redes en general, consisten en "compartir recursos", y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico. Las pequeñas computadoras tienen una mejor relación costo / rendimiento, comparada con la ofrecida por las máquinas grandes.

Otro objetivo del establecimiento de una red de computadoras, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre si; esto hace que la cooperación entre grupos de individuos que se encuentran alejados, y que anteriormente había sido imposible de establecer, pueda realizarse ahora.

Usos de las redes de acuerdo al área productiva.

Dentro de las aplicaciones más elementales, podemos destacar su uso para la transmisión, proceso y almacenamiento de datos, que es consecuencia de la propia naturaleza de la red. Una extensión inmediata de estos usos es la aplicación para servicios de correo electrónico, también puede ser utilizada para ofrecer un canal “multimedia” (datos, voz, imágenes) para diálogos entre dos usuarios.

Otra área de aplicación es la de la automatización de oficinas. La combinación de la capacidad de proceso de las computadoras con la de comunicación ofrecida por la red, permite la producción más eficiente de documentos y disminuye su circulación en la oficina.

En el área comercial y bancaria, las redes de computadoras pueden ser utilizadas para dar soporte a las transacciones en forma remota.

Las redes de computadoras han causado gran impacto en el área médica principalmente en hospitales donde los pacientes son constantemente monitoreados por equipos controlados por computadoras y uno o más centros control reciben los datos de cada paciente a través de la red.

En el área gubernamental, las redes pueden ser utilizadas para integrar los sistemas de información de prevención social permitiendo una mejor y más rápida atención al usuario.

El área educativa también puede beneficiarse, con el uso de la información educativa apoyada por computadora en locales remotos de difícil acceso.

1.2 Tipos y clasificación de las redes

Hay diferentes tipos de redes de computadoras. Las diferencias entre ellas se fundamentan usualmente en la perspectiva, éstas son clasificadas según el área geográfica que abarcan, sus tipologías, o el tipo comunicación que usan y la manera en que los datos son transmitidos a lo largo de estas rutas.

1.2.1 Clasificación de redes por el área que abarcan y por su topología

Clasificación de redes por el área geográfica que abarcan.

- Red de área local (LAN): generalmente interconecta recursos de computadoras dentro de un área geográfica de tamaño moderado,. esto puede incluir un cuarto, varios cuartos dentro de un edificio o varios edificios en un campus. Como el término “de tamaño moderado” no está bien definido algunas personas cuantifican el rango de este tipo de red a unos cuantos kilómetros.
- Red de área amplia (WAN) interconecta recursos de computadoras que están ampliamente separadas geográficamente (generalmente más de 100 kilómetros) esto incluye pueblos, ciudades, estados y países; una WAN barca un área mayor de 8 kilómetros de diámetro.
- Red de área metropolitana (MAN): interconecta recursos de computación que cubren una red de área metropolitana. Por ejemplo, una gran organización de negocios con edificios localizados por toda una ciudad. Si cada edificio tiene su propia LAN independiente y esas

LAN están conectadas todas entre sí, la red resultante, es considerada una MAN.

- Red de área personal (PAN): se refiere a las pequeñas redes de computadoras que se encuentran en casas privadas. El bajo costo de las computadoras y el creciente número de casas con varios equipos han generado la necesidad de las PAN ya que los usuarios se han dado cuenta de la conveniencia de interconectarlas.
- Red de ärea global (GAN): se refiere a una conexión de WAN que cubren el planeta. Por ejemplo, la cadena Mc Donalds tiene operaciones en gran cantidad de países en todo el mundo. La interconexión de esas localizaciones forma una GAN.
- Red de área de almacenamiento (SAN): es una red dedicada exclusivamente al almacenamiento de datos; a través de una SAN los servidores dedicados al almacenamiento proporcionan acceso ilimitado mediante una infraestructura de red segura.

Clasificación de las redes por su topología. Para esta clasificación se toma en cuenta la arquitectura o la forma en que se interconectan los diferentes nodos o usuarios de la red, Existen dos tipos de topologías: física (es la forma en que están conectadas las computadoras de la red) y lógica (que es el método que se usa para comunicarse las computadoras entre sí dentro de la red). Estas son las distintas topologías:

- Malla: Es una interconexión total de todos los nodos, con la ventaja de que, si una ruta falla, se puede utilizar otra alternativa. Este tipo de red es más costoso de construir, ya que utiliza una gran cantidad de cable.[1]

1.- J. Molina Francisco, Redes de Área local, Editorial Alfaomega, México, 2004 pág. 23

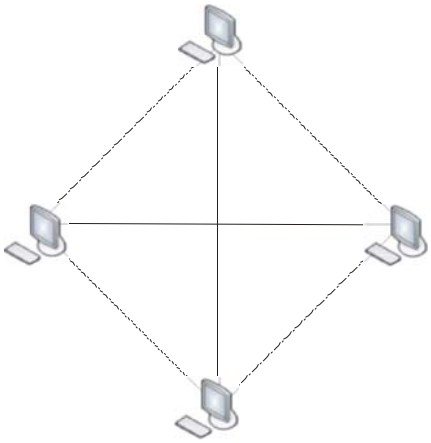


Fig. 1.1 Topología de MALLA

- Estrella: En esta topología los equipos (nodos) se conectan a un nodo central con funciones de distribución, conmutación y control. Si este nodo falla, la red queda inutilizada, pero si es un nodo de los extremos, sólo este queda aislado.[2]

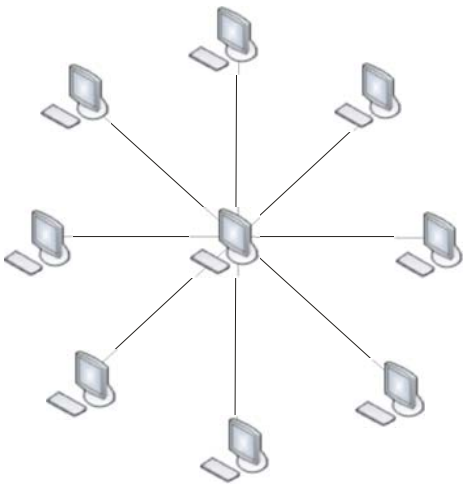


Fig. 1.2 Topología de ESTRELLA

2.- Ibídem, pág.23

- Bus: Aquí se utiliza un único cable para conectar los equipos, por lo tanto se requiere menos cable, pero el inconveniente es que si algún equipo falla automáticamente los demás quedan aislados.[3]

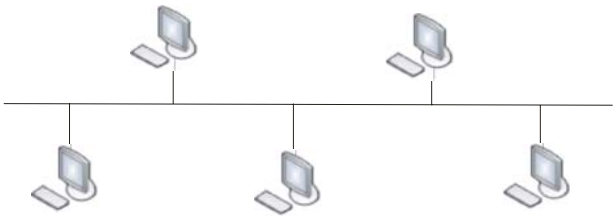


Fig. 1.3 Topología de BUS

- Árbol: Es una forma de conectar los nodos como una estructura jerarquizada. Esta topología casi no es usada, ya que si un nodo falla o un enlace quedan incomunicados entre sí varios conjuntos de nodos.[4]

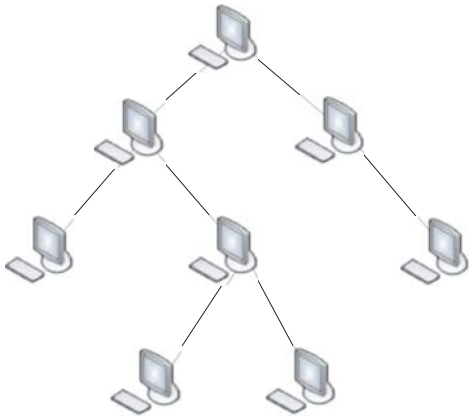


Fig. 1.4 Topología de ÁRBOL

- Anillo: En esta topología todos los nodos están conectados a una vía única unida de sus dos extremos. Al igual que en una topología de bus si falla algún enlace, deja de funcionar la red por completo.[5]

3.- J. Molina Francisco, *op. Cit.,*pág.24
4.- Ibídem, pág.24
5.- Ibídem, pág.24

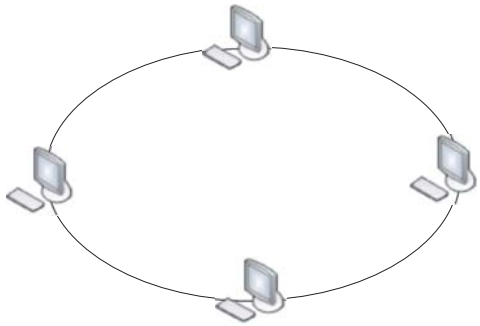


Fig. 1.5 Topología de ANILLO

- Intersección de anillo: Aquí se conectan varios anillos por nodos comunes; el inconveniente es que si fallan los nodos comunes toda la red deja de funcionar.[6]

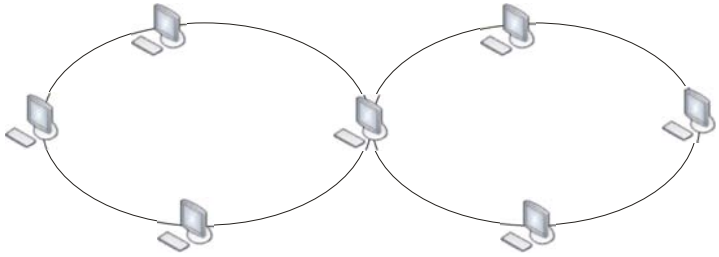


Fig. 1.6 Topología de INTERSECCIÓN DE ANILLO

- Irregular: En esta topología cada nodo debe estar conectado, mínimo por un enlace y no hay restricciones; además es la más utilizada en redes que ocupan zonas geográficas amplias.[7]

6.- J. Molina Francisco, *op. Cit.*,pág.25
7.- Ibídem, pág. 25

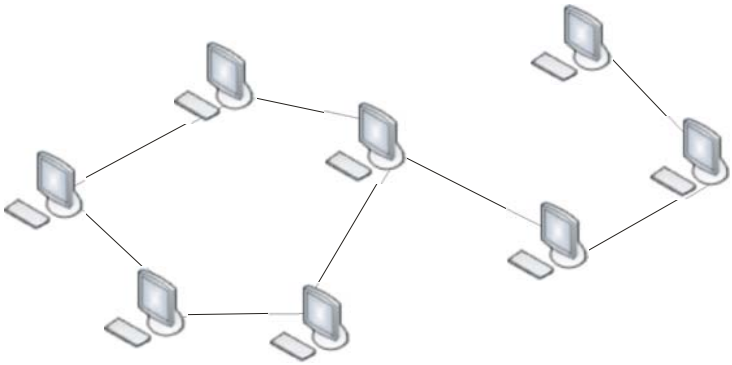


Fig. 1.7 Topología IRREGULAR

Clasificación de las redes por la forma en que la información es transmitida. Para esta clasificación se toma en cuenta la técnica empleada para transmitir información desde el origen hasta el destino. Estas redes son punto a punto y de difusión.

- Redes punto a punto: Este tipo de red consiste en nodos que sólo pueden comunicarse con nodos adyacentes que son nodos próximos entre sí. La propiedad de la adyacencia se expresa como el número de saltos requeridos para que los datos viajen de un nodo fuente a uno destino. Un salto es una conexión a, o desde, un nodo intermedio sobre la ruta de la fuente al destino. Si un nodo necesita comunicarse con otro que no es adyacente, primero transmite el mensaje al nodo adyacente y el mensaje pasa en serie a través de cada nodo intermedio hasta llegar al destino. A este proceso se le llama puenteo o enrutamiento y lo utilizan las topologías de estrella, bucle y árbol.[8]
- Redes de difusión (*broadcast*): Una red de difusión consiste en nodos que comparten un solo canal de comunicación. En contraste con un diseño punto a punto, los datos enviados por una máquina son recibidos por todos los demás nodos conectados al canal compartido. Los

8.- A. Gallo Michael y William M. Hancock, Comunicación entre computadoras y Tecnologías de redes, Editorial Thomson, Argentina, 1997 pág. 9

anfitriones que reciben una transmisión, verifican quién es el receptor del mensaje y determinan si es para ellos, de lo contrario descartan el mensaje. Así solo el nodo destino responde. Las redes de difusión emplean varias tipologías, en particular son dos, de bus y de anillo. Los sistemas de comunicaciones en satélite son también de difusión.[9]

- Las redes multiterminales emplean un concepto maestro/esclavo, en donde un nodo es el maestro de la red y los demás nodos son esclavos. En esta disposición, el maestro controla las funciones de la red y los esclavos solicitan al maestro acceso a la misma. En este tipo de red los nodos están conectados a un cable común similar a un diseño de bus, pero, a diferencia de las redes de bus, a los nodos multilaterales se les asigna un número específico para fines de comunicación; este número es usado para establecer prioridad sobre cuándo es permitido comunicarse con el sistema de control maestro. Esto permite el control total sobre la prioridad del tráfico sobre la red, así como el control total sobre su uso.[10]

Además del área geográfica y la topología, las redes pueden también clasificarse por el tipo de trayectoria de las comunicaciones que usan y la manera en que los datos son transmitidos. Dos clasificaciones particulares son circuito conmutado y paquete conmutado.

En una red de circuito conmutado se establece primero un circuito físico, dedicado entre los nodos fuente y destino antes de que cualquier transmisión de datos tenga lugar. Este circuito cerrado promueve la participación de

9.- A. Gallo Michael y William M. Hancock, *op. cit.,* pág. 11

10.- A. Gallo Michael y William M. Hancock, *op. cit.,* pág. 14

enlaces ya que se pueden usar los mismos circuitos para diferentes transmisiones, aunque no al mismo tiempo.

En una red de paquete conmutado los mensajes son primero subdivididos en unidades menores llamadas paquetes, los cuales son enviados al nodo destino uno a la vez por medio de conmutadores intermedios. Un paquete representa la unidad más pequeña de datos que puede ser transferida dentro de una red dada; cuando un paquete llega a un conmutador intermedio, el conmutador examina la dirección del destino del paquete para determinar qué trayectoria debe tomar hacia el siguiente conmutador.

Las redes de paquetes conmutados también promueven la participación de enlaces usando circuitos virtuales. Un circuito virtual es una trayectoria lógica y no física, es decir, se trata de una conexión lógica no dedicada a través de un medio compartido que da al usuario de nivel superior la apariencia de una conexión física dedicada directa entre el nodo fuente y el nodo destino.

1.3 Arquitectura de red y el Modelo OSI

La arquitectura de red es el medio más efectivo en cuanto a costos para desarrollar e implementar un conjunto coordinado de productos que se puedan interconectar; también es el plan con el que se conectan los protocolos y el software y por último también define las reglas de una red y cómo interactúan sus componentes. Esto es benéfico tanto para los usuarios de la red como para los proveedores de hardware y software.

Características de la Arquitectura ·

- Separación de funciones. Dado que las redes separan a los usuarios y los productos que se venden, evolucionan con el tiempo, debe haber una forma de hacer que las funciones mejoradas se adapten a la última. Mediante la arquitectura de red el sistema se diseña con alto grado de modularidad, de manera que los cambios se puedan hacer por pasos con un mínimo de perturbaciones.
- Amplia conectividad. El objetivo de la mayoría de las redes es proveer conexión óptima entre cualquier cantidad de nodos, teniendo en consideración los niveles de seguridad que se puedan requerir.
- Recursos compartidos. Mediante las arquitecturas de red se pueden compartir recursos tales como impresoras y bases de datos, con esto a su vez se consigue que la operación de la red sea más eficiente y económica.
- Administración de la red. Dentro de la arquitectura se debe permitir que el usuario defina, opere, cambie, proteja y de mantenimiento a la red.
- Facilidad de uso. Mediante la arquitectura de red los diseñadores pueden centrar su atención en las interfaces primarias de la red y por lo tanto hacerlas accesibles para el usuario.
- Normalización. Con la arquitectura de red se alimenta a quienes desarrollan y venden software a utilizar hardware y software normalizados. Mientras mayor es la normalización, mayor es la colectividad y menor el costo.

- Administración de datos. En las arquitecturas de red se toma en cuenta la administración de los datos y la necesidad de interconectar los diferentes sistemas de administración de bases de datos.
- Interfaces. En las arquitecturas también se definen las interfaces como de persona a red, de persona, y de programa a programa. De esta manera, la arquitectura combina los protocolos (los cuales se escriben como programas de computadora) y software apropiados para producir una red funcional.
- Aplicaciones. En las arquitecturas de red se separan las funciones que se requieren para operar una red a partir de las aplicaciones comerciales de la organización. Se obtiene más eficiencia cuando los programadores de la misma no necesitan considerar la operación.

.

Modelo OSI

La Organización Internacional para Estandarización (ISO) desarrolló un modelo de referencia para la estandarización de los protocolos de red. El modelo es conocido como el modelo de referencia para Interconexión de Sistemas Abiertos, (OSI, Open System Interconection). OSI es un modelo de siete capas, las cuales se encargan desde establecer la conexión física y vigilar que los datos enviados no se pierdan o se dañen, hasta controlar que los datos sean correctamente interpretados por diferentes aplicaciones. En el siguiente cuadro se muestran las diferentes capas del modelo OSI:

Fig. 1.8 Modelo OSI

La forma en la cual dos partes de la red se comunican es llamada protocolo, lo cual asegura que cada una de las partes de la comunicación entienda a la otra sin ambigüedad. Un protocolo puede especificar la forma en que los datos son codificados, como puede ser identificado el comienzo y el fin de un mensaje, como las direcciones de los puntos origen y destino son mostradas, y las acciones a tomar si se encuentran errores durante la transmisión. Debe existir un protocolo definido para conectar dos niveles adyacentes, pero la estructura completa de una red puede consistir de muchas especificaciones diferentes.

Por ejemplo, en el cuadro anterior la capa de red (Capa 3), tendrá especificaciones de protocolo para la capa de enlace de datos (capa 2) y para la capa de transporte (Capa 4). Esto es, a la capa 3 no le interesan las especificaciones para la capa 1 o para la capa 5, dado que esas capas no forman parte del área de interés de la capa. Esto da como consecuencia una flexibilidad considerable cuando las especificaciones son cambiadas o se agregan nuevas opciones.

A continuación de describen las diferentes capas del modelo OSI:

- Física: regula la transmisión de bits a través de un canal de comunicación. Esto implica la definición de voltajes y tiempo de duración de los bits, si la transmisión es *simplex, half-duplex* o *full-duplex*, etc.
- Enlace: a partir del canal ofrecido por el nivel físico, este segundo nivel hace que dicho canal parezca una línea de transmisión sin errores. Para esto, los bits transmitidos se dividen en cuadros que son confirmados por el receptor. Este nivel también es responsable del control del flujo para regulare la velocidad relativa de los dos procesos.
- Red: controla la operación interna de la red. Regula la comunicación entre dos computadoras de la misma y los conmutadores del paquete; de hace cargo de cómo se encaminan los paquetes y del control de congestionamiento.
- Transporte: permite la transferencia de datos entre computadoras centrales, utilizando el servicio de transmisión ofrecido por el nivel de la red. Es responsable de la optimización de los recursos de la red, posiblemente utilizando multiplexación de canales y permitiendo la comunicación entre dos procesos de distintos equipos. Hasta el nivel tres todas las computadora involucradas en la transmisión de datos ejecutan los protocolos correspondientes; a partir del nivel cuatro, solamente las computadoras inicial y final ejecutan el protocolo correspondiente.
- Sesión: ofrece a los usuarios el acceso a la red (salvo ciertas transformaciones en la codificación de los datos realizados por el nivel

seis), también permite a los usuarios establecer una conexión (enlace), llamada sesión; donde el usuario debe entregar una dirección con la cual desea conectarse. El establecimiento de una sesión implica el intercambio de parámetros, tales como la identificación del usuario, modo de transmisión, etc.

- Presentación: es la responsable de la conversión de los códigos de presentación de los datos que son transmitidos en una sesión: compresión de texto, codificación (cifrado), conversión de formatos de archivos, etc.
- Aplicación: Incluye una parte de la administración de la red y tareas de aplicación general, tales como la transferencia de archivos. Esta es la capa superior de la arquitectura del modelo OSI, a través de ella las aplicaciones obtienen el acceso a los servicios proporcionados por la arquitectura de comunicaciones.

Aunque el Modelo OSI no ha sido implantado en forma comercial y su uso no sea mas que teórico, es tomado como referencia para ubicar las funciones de TCP/IP.[11]

1.4 ¿Qué es una VPN y cómo funciona?

Ante la necesidad de comunicar puntos remotos, y lo costoso que significaría tener una WAN (Wide Area Network) que significaría tirar líneas o cables entre cada sucursal de una empresa “X” se ideó la forma de utilizar redes publicas para comunicar estas sucursales.

11.- A. Menascé Daniel, Redes de Computadoras Aspectos Técnicos y Operacionales, Editorial Campus LTDA, España, 1988 págs. 27-29

Para poder habilitar redes privadas distribuidas para comunicar de forma segura a cada uno de los nodos de una red pública, está la necesidad de aplicar un sistema de seguridad, debido a que los datos de la empresa son valiosos, y no deben ser interceptados.

Con una Red Privada Virtual (VPN), los usuarios remotos, que pertenecen a una red privada, pueden comunicarse de forma libre y segura entre redes remotas a través de redes públicas. Una definición simple es que se trata de una red de comunicaciones privada implementada sobre una infraestructura pública.

Una VPN normalmente usa la red Internet como transporte para establecer enlaces seguros y como una WAN privada, extendiendo las comunicaciones a oficinas aisladas. Significativamente, decrece el costo de las comunicaciones porque el acceso a Internet es generalmente local y mucho más barato que las conexiones mediante Acceso Remoto a Servidores.

Una VPN es considerada también como una conexión IP entre dos sitios sobre una red pública IP, es antes que nada una red virtual, implica que las trayectorias sobre las que los datos viajan entre una fuente y un destino son compartidas por otras transmisiones. Una VPN se trata también de una red privada, lo cual indica que los datos transmitidos entre una fuente y un destino no son accesibles a usuarios no autorizados.

Los datos transportados a través de una VPN son codificados de manera que sólo los nodos fuente y destino pueden decodificarlos, así una red públicamente accesible como Internet puede ser usada para transportar información altamente confidencial de manera segura.

¿Cómo funciona una VPN?

- Una vez establecida la conexión VPN, la dirección IP de nuestro equipo pasa a ser una dirección IP del servidor o RED a la que nos hemos conectado y toma como nombre, un nombre perteneciente al dominio.
- El uso del cifrado en la conexión VPN puede ser necesario en los casos en que la información que viaja a través del túnel sea delicada y requiera privacidad.
- En una conexión VPN segura el cifrado sólo tiene lugar entre el servidor del túnel y el cliente VPN y la conexión entre el servidor de túnel y el servidor de la aplicación se realiza sin cifrado.[12]

En una forma más general una Red Privada Virtual (VPN) consiste en dos máquinas (una en cada "extremo" de la conexión) y una ruta o "túnel" que se crea dinámicamente en una red publica o privada. Para asegurar la privacidad de esta conexión los datos transmitidos entre ambos ordenadores son encriptados por el Point-to-Point Protocol, también conocido como PPP, un protocolo de acceso remoto, y posteriormente enrutados o encaminados sobre una conexión previa (también remota, LAN o WAN) por un dispositivo PPTP.

1.4.1 Elementos de una VPN

Como cualquier tipo de red, la VPN también tiene distintos elementos que la conforman y que son mencionados a continuación:

- Un servidor VPN: es una computadora que acepta conexiones VPN de clientes VPN. Un cliente VPN: es una computadora que inicia

12.- www.novadevices.com/vpn.pdf, 17 octubre de 2006, Página principal

conexiones VPN a un servidor VPN. Puede ser un enrutador o una computadora individual.

- Un túnel: es aquella porción de la conexión en la que los datos están encapsulados. Los datos no tienen porque estar forzosamente cifrados.
- Protocolos de tunelaje: son estándares de comunicación utilizados para gestionar el túnel y encapsular los datos privados.
- Red de tránsito: es la red pública o compartida por la cual circulan los datos. Puede tratarse de Internet o de una intranet basada en IP privada.[13]

1.4.2 Tipos y conexiones de VPN

Las redes privadas virtuales se dividen en 3 categorías de acuerdo con el servicio de conectividad que brindan:

1) VPN de Acceso Remoto. (Remote Acces VPNs). Provee acceso remoto a la intranet o extranet corporativa a través de una infraestructura pública, conservando las mismas políticas, como seguridad y calidad de servicio, que en la red privada; también permite el uso de múltiples tecnologías como discado, ISDN, xDSL, cable, o IP para la conexión segura de usuarios móviles, *telecommuters* o sucursales remotas a los recursos corporativos.

Características:

- *Outsourcing* de acceso remoto
  - llamadas locales o gratuitas
  - difusión del acceso
- Instalación y soporte del PS (Proveedor de servicio)

13.- Ibídem, Página principal

- Acceso único al nodo central
- Tecnologías de acceso RTC, ISDN, xDSL
- Movilidad IP
- Seguridad reforzada por el cliente
  - AAA en el ISP proporciona 1° y posiblemente 2° nivel de seguridad[13]

2) VPN de Intranet. Vincula la oficina remota o sucursal a la red corporativa, a través de una red pública, mediante enlace dedicado al proveedor de servicio. La VPN goza de las mismas cualidades que la red privada: seguridad, calidad de servicio y disponibilidad, entre otras.

Característica:

- Extiende el modelo IP a través de la WAN compartida.

3) VPN de Extranet. Permite la conexión de clientes, proveedores, distribuidores o demás comunidades de interés a la intranet corporativa a través de una red pública.

Características:

- Extiende la conectividad a proveedores y clientes:
  - sobre una infraestructura compartida
  - usando conexiones virtuales dedicadas
- Los *partners* tienen diferentes niveles de autorización
  - *accses control lists, firewalls*, filtros, según decida la empresa

Hay dos tipos de conexiones VPN:

- Conexión VPN de acceso remoto o cliente - red. Una conexión de acceso remoto es realizada por un cliente de acceso remoto, primero, se implementa un servidor de Internet que se conecta a través de un enlace

dedicado (mayor a 64kbps), a un ISP. Después cada usuario de una computadora o sucursal remota debe tener configurado un acceso a Internet para poder conectarse a una red privada. El servidor de VPN provee de acceso a los recursos del servidor VPN, o a la red completa a la cual el servidor VPN esta conectado. Los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto. El cliente de acceso remoto (cliente VPN), se autentifica al servidor de acceso remoto (el servidor VPN), y para una mutua autentificación, el servidor se autentifica ante el cliente.

- Conexión VPN enrutador-enrutador o red - red. El túnel en esta conexión es realizado entre *routers* (enrutadores) o servidores, y este conecta 2 porciones de una red privada. El servidor VPN provee una conexión ruteada hacia la red en la cual el servidor VPN esta conectado. En una conexión VPN *router to router*, los paquetes enviados desde cualquier *router* a través de una conexión VPN típica, no se originan ahí. El router que realiza la llamada (Cliente VPN), se autentifica ante el router que responde (el servidor VPN), y para una autentificación mutua el router que responde, se autentifica ante el router que realiza la llamada. En resumen este tipo de enlace se usa para interconectar dos redes privadas de forma segura a través de Internet utilizando mecanismos de autenticación y encriptación que aseguran la integridad y confidencialidad de los datos.

Estas conexiones VPN tienen las siguientes propiedades:

- Encapsulado. La tecnología VPN, provee una vía de encapsulamiento de datos privados con encabezados que permiten a los mismos pasar por el tráfico interredes.
- Autenticación (hay dos tipos). Del usuario donde, para que la conexión VPN sea establecida, El servidor VPN autentifica al cliente VPN intentando la conexión y verificando que el cliente VPN tiene los permisos apropiados. Si se acepta, se usa la autentificación mutua; el cliente VPN también autentifica al servidor VPN suministrando una protección ante servidores VPN enmascarados. Otra autenticación es de los datos donde, para verifica que los datos enviados en la conexión VPN, son originados al otro lado de la conexión y no han sido modificados en el camino, los datos contienen una suma de comprobación (*checksum*) criptográfica basaba en un código conocido solo por el emisor y el receptor.
- Cifrado de los datos (encriptación). Para asegurar la confiabilidad de los datos que son enviados a través del transito interredes compartido o publico, este es encriptado por el emisor, y desencriptado por el receptor. El proceso de encriptación y desencriptación depende de que el emisor y el receptor tengan conocimiento de una llave de encriptación conocida por ambos.

Los paquetes interceptados a lo largo de la conexión VPN en el transito interred, son ilegibles para quien no conozca la llave de encriptación. La longitud de esta llave es un parámetro importante de seguridad, por lo tanto, es muy importante usar una llave lo mas larga posible. Además mientras más información es encriptada con la misma llave, es más fácil de descifrar los

datos encriptados. Con algunas técnicas de encriptación, se le da la opción de configurar cuan a menudo las llaves de encriptación son cambiadas durante una conexión.

1.4.3 Tecnologías de VPN's

La arquitectura de las VPNs se debe basar en elementos esenciales de la tecnología para proteger la privacidad, mantener la calidad y confiabilidad, y asegurar la operatoria de la red en toda la empresa. Estos elementos son:

- Seguridad: uso de túneles, encriptación de datos, autenticación de usuarios y paquetes, control de acceso.
- Calidad de Servicio: uso de colas, manejo de congestión de red, priorización de tráfico, clasificación de paquetes.
- Gestión: implementación y mantenimiento de las políticas de seguridad y calidad de servicio a lo largo de la VPN.

La tecnología de VPN está basada en la idea de los túneles. La red de los túneles se involucra al establecer y mantener una conexión de la red lógica. En ésta, se encapsulan paquetes construidos en una VPN específicos, entonces al transmitirse entre el cliente de VPN y el servidor, finalmente se encapsulan en el lado del receptor.

Para VPN's el Internet-basado, se encapsula en paquetes en uno de varios protocolos de VPN dentro de los paquetes de IP. Los protocolos de VPN también apoyan la autenticación y encriptación para guardar los túneles de seguridad.

Hay dos tipos de túneles VPN: obligatorio y voluntario. Los túneles voluntarios requieren que el cliente esté habilitado por una VPN mientras que los túneles obligatorios se utilizan cuando el cliente confía en un FEP (procesador de componente frontal o Frente Extremo del Procesador) habilitado por una VPN.

La conexión por túnel voluntario es una metodología en la cual la estación de trabajo de cliente se ofrece como voluntario para crear el túnel en la red. Para que ocurra esta conexión por túnel, el cliente debe estar habilitado por VPN con los protocolos PPTP o L2TP y software de soporte. (El servidor de túnel siempre viene con este soporte de protocolo). El cliente y el servidor deben utilizar el mismo protocolo de túnel.

Con la conexión por túnel voluntario el cliente puede tener una conexión de red que puede proporcionar transporte entre la estación de trabajo y servidor de túnel seleccionado. Frecuentemente, la estación de trabajo puede haber establecido una conexión de marcación a la red de transporte antes de que el cliente pueda configurar un túnel.

Conexión por túnel obligatorio. Si un cliente desea conectarse a través de Internet, pero no está habilitado por una VPN, puede conectarse a un FEP habilitado por una VPN en un proveedor de software independiente. En el caso de conexión por túnel obligatorio, el cliente puede operar sin el software de soporte L2TP o PPTP (estos protocolos se implementan en el FEP). Es evidente, que el FEP y el servidor de túnel deben soportar y utilizar el mismo protocolo VPN (PPTP o L2TP]) para cualquier conexión específica.

Comúnmente, el usuario que se encuentra en una máquina de cliente recibe un número telefónico especial para marcar al FEP. Por ejemplo, una corporación que tiene su propia red privada puede tener un contrato con un

proveedor de software independiente para ensamblar un conjunto de FEPs en todo el país. Estos FEPS pueden establecer VPNs a través de Internet para un servidor de túnel en la red privada de corporación. Esta configuración es conocida como conexión por túnel obligatorio debido a que el cliente está obligado a utilizar la VPN. Una vez que se ha realizado la conexión inicial, automáticamente se enruta al cliente a través del túnel.

Túneles de VPN en los Protocolos

Se han llevado a cabo varios protocolos de la red interesantes específicamente para el uso de túneles de VPN. Las tres más populares del VPN se excavan con túneles en protocolos listos para continuar compitiendo entre sí para la aceptación en la industria. Estos protocolos son entre sí generalmente incompatibles.

PPTP (Point-to-Point Tunneling Protocol): es un protocolo desarrollado por Microsoft y normalizado por la IETF (RFC 2637). Éste permite el tráfico seguro de datos desde un cliente remoto a un servidor privado. PPTP soporta múltiples protocolos de red (IP, IPX, NetBEUI). Popularizado y frecuentemente implementado por Microsoft.[14]

Túneles en la Capa del Segundo Protocolo (L2TP). L2F (Layer 2 Forwarding): es un protocolo desarrollado por Cisco Systems. Innovador en autenticación de usuarios pero no posee encriptación de datos. Fuente para el desarrollo del protocolo L2TP.[15]

L2TP (Layer 2 Tunneling Protocol): Combina las mejores características de PPTP y L2F. El protocolo como tal no posee ni autenticación de usuarios ni

14.- www.icsa.com , 22 de octubre de 2006, Página principal

15.- Ibídem, página principal

encriptación de datos pero trabaja y combina esfuerzos con otros protocolos de nivel de red, por ejemplo IPSec.[16]

La Seguridad Protocolar en Internet (IPsec o IP Secure). Realmente es una colección de múltiples protocolos relacionados. Puede usarse como un VPN completo en la solución protocolar, o simplemente como el usó de encriptación formando planes dentro de L2TP o PPTP. IPsec es un protocolo de seguridad que brinda diversos servicios a nivel de red (capa tres) del Modelo OSI, implementa algoritmos de cifrado y métodos de autenticación proporcionando elementos que garanticen la integridad y confidencialidad de los datos.[17]

En resumen, las redes privadas virtuales (VPN) suponen hoy en día la solución tecnológica más segura y rentable para la conectividad entre las oficinas centrales de una empresa, sus sitios remotos y sus teletrabajadores. Ofrecen una solución para cada empresa sin importar su localización o tamaño, funcionando sobre una infraestructura de red pública como Internet con la misma seguridad, administración y políticas de calidad de servicio que se aplican para las redes privadas (WAN) .

1.5 Internet como medio de comunicación

1.5.1 Métodos de Comunicación.

Los métodos a través de los cuales se transfieren las comunicaciones son usualmente invisibles para los usuarios. Las telecomunicaciones se iniciaron con el envío de señales telefónicas mediante cables sujetos por poleas. Si bien

16.- Ibídem, página principal

17.- Ibídem, página principal

este método se sigue usando ampliamente, otros métodos de transmisión se han vuelto comunes hoy en día, como los cables de fibra óptica y las señales de radio y microondas enviadas por satélite o transmisores terrestres.

En la mayoría de las telecomunicaciones se utilizan cables físicos. Se pueden usar distintos tipos de cables dependiendo de la clase y disponibilidad de la información transmitida. Entre mayor sea el número de *bytes* por segundo que un cable pueda transferir, más rápida será la transmisión de la información. Los cables telefónicos ordinarios no suelen ser muy rápidos para la transmisión de grandes volúmenes de información. Normalmente se utilizan cables especializados de alta velocidad cuando este tributo es importante. Se utilizan las líneas de redes digitales de servicios integrados (ISDN por sus siglas en inglés) para transmitir grandes volúmenes de información a altas velocidades. Los cables de fibra óptica también se pueden utilizar para transmisiones a gran velocidad y los cables ópticos transmiten información utilizando pulsaciones de luz láser.

En algunos casos, especialmente en sitios remotos, los cables físicos pueden no ser apropiados o no estar disponibles. En estos casos, la información puede ser transmitida por microondas u ondas de radio, utilizando satélites o transmisores terrestres. Todos estos medios de telecomunicación son complejos y están siendo constantemente mejorados.

1.5.2 Internet como distintos canales de comunicación

Internet como nuevo “Canal de Comunicación”.

Internet es un “canal” a través del cual puede transitar el tráfico de información de los medios de comunicación ya existentes. Internet este “nuevo canal” tiene algunas peculiaridades

- Es un canal universal, es decir, un canal que soporta sin dificultad el tráfico de todos los medios de comunicación.
- Es un canal omnifuncional, capaz de desempeñar funciones “conectoras” (comunicaciones de uno a uno), funciones “distribuidoras” (de uno a muchos) y funciones “colectoras” (de muchos a uno); por lo tanto es un canal que se puede personalizar.
- Es un canal bidireccional y por consiguiente interactivo; no sólo que admite la interactividad, sino que en su funcionamiento, la facilita.
- Es un canal de alcance prácticamente ilimitado, cuyo ámbito es mundial.

Este nuevo canal presenta grandes ventajas que hacen posible un desarrollo de esos medios con las limitaciones de los canales tradicionales inconvenientes, pueden ser mitigados o anulados por mejoras en la tecnología del canal, que deberán producirse durante los próximos años.

1. Una característica de Internet, de gran trascendencia, radica en el hecho de que la comunicación de éste, aunque es masiva en el sentido de que puede llegar y llega a muchos, es siempre comunicación de uno a uno. El equívoco radica en que con frecuencia tiende a imaginarse al servidor de información como un “emisor” de prensa, radio o televisión que difunde en cada uno de sus actos de comunicación un mensaje dado a una audiencia masiva. Pero las cosas en Internet no son así, sino que el servidor de éste es capaz de atender a muchos usuarios a la vez.

2. Otra característica de Internet se encuentra en la posición activa del usuario de los servicios que se ofrecen en éste. En el comportamiento típico de Internet el usuario decide cada paso y está decidiendo en cada momento si continúa recibiendo una información y en qué condiciones y con qué características la recibe.

Esta “interactividad”, que actualmente emerge también en la audiencia televisiva, es en el caso de Internet prácticamente obligada (al menos hasta ahora). Esto representa una exigencia adicional impuesta al usuario, la actitud pasiva típica de las audiencias tradicionales de radio y televisión no es posible en Internet.

3. Constituye un canal de potencia y alcance prácticamente ilimitados. Por las características técnicas de este canal, Internet es un medio masivo de alcance universal. Hay actualmente limitaciones muy importantes que sufren los usuarios de Internet pero son técnicas y comerciales que el desarrollo tecnológico permite vencer con crecimientos exponenciales en el rendimiento de los recursos. Otras más radicales derivan de las condiciones económicas y culturales.

Internet como canal (secundario) de Prensa escrita.

En diciembre de 1994, se publica el primer periódico electrónico en la Web. Los inconvenientes de la prensa electrónica derivan de las características físicas del “receptor” de la información y su conexión necesaria a la red telefónica: incomodidad de la lectura en pantalla, falta de movilidad, etc. Otro inconveniente es la reducción de la audiencia, restringida necesariamente a las personas con conexión a Internet.

Las ventajas:

- La facilidad e inmediatez de la recuperación de la información.
- La posibilidad de una actualización, corrección, ampliación.
- La facilidad, para el usuario, de edición, copia, archivado.
- Acceso a los números atrasados.
- Infinitas consultas y recuperaciones posibles.

En la segunda perspectiva:

- Remisión ilimitada a otras informaciones.
- Posibilidades abiertas por la interactividad.
- Posibilidad de difundir localmente información de interés particular.
- La posibilidad de personalización.

Internet como canal (secundario) de Radio.

En Abril de 1995 aparece el primer software de Real Audio. Los inconvenientes de la radio *on-line* son la incomodidad del receptor y la limitación de la audiencia.

Las ventajas:

- La desaparición de los problemas de frecuencia, derivados de la limitación de banda disponible.
- La desaparición de las limitaciones de alcance y los problemas asociados de potencia.

Desarrollo de los servicios, facilitados por el nuevo canal:

- Posibilidad de emitir simultáneamente múltiples canales y programas.
- Posibilidad de acceso a fondos de fonoteca.

- Posibilidades derivadas de la interactividad: de los programas abiertos al público tradicionales a los foros, la participación en línea.
- Posibilidad de personalización.

Internet como canal (secundario) de TV.

Es la TV digital por cable limitada por la infraestructura de la Red Telefónica Básica que para desempeñar la función de canal secundario de TV, Internet tiene que transmitir las señales video en tiempo real, transmisión dificultada por la escasa capacidad de las líneas.

1.5.3 Internet como nuevo “Medio de Comunicación”.

Las posibilidades de Internet no se reducen a su condición de nuevo canal para los medios de comunicación tradicionales, sino que convierten a Internet en un nuevo medio de comunicación, cualitativamente distinto de los medios existentes. Sin dejar de ser un nuevo canal, va creando un nuevo lenguaje, complejo, cuyo desarrollo está convirtiendo Internet en un nuevo medio de comunicación, tan característico y diferenciado de los demás.

Las principales posibilidades de este 'nuevo medio' son:

- Ser multilenguaje, capaz de utilizar simultánea y articuladamente los lenguajes propios de todos los medios.
- Ser hipertextual, capaz de niveles y ramificaciones de referencias en número indefinido.

- Ser personalizable, capaz de ofrecer las informaciones que cada usuario individualmente demande, en el volumen que pida y con el formato que prefiera.
- El nuevo medio puede acceder desde sus marcos a todos los demás medios, seleccionando sus materiales e integrándolos en su propia oferta informativa.

CAPÍTULO 2 ATECEDENTES DEL PROYECTO

2.1 ¿Cuál es la empresa?

La empresa Proyección y Administración Empresarial S.A. de C.V. se fundó hace 13 años con la finalidad de apoyar a la industria a solucionar sus necesidades en Recursos Humanos. Es una compañía que cree fervientemente en la comunicación y trabajo en equipo, adoptado la filosofía y forma de trabajo S.I. "Soluciones Inteligentes" como una alternativa de respuesta a todos sus clientes. Para hacer todo esto posible, la empresa presta los servicios de reclutamiento y selección de personal, *outsourcing* y maquila de nómina a distintas empresas ubicadas tanto en el Distrito Federal como en el interior de la república.

2.2 Situación actual

En al actualidad la empresa cuenta con varias sucursales en el interior de la república, en los estados de Monterrey, Tijuana, Guadalajara, Tabasco y Veracruz; estas sucursales o filiales se necesitan porque son el contacto directo con sus clientes ubicados en dichos estados.

El principal problema o la situación actual de la empresa es que cada una de sus filiales cuentan con redes independientes, organizadas cada una en grupos de trabajo por lo que la empresa necesita que haya comunicación del corporativo con cada una de las filiales puesto que es bastante la información que se necesita compartir; el inconveniente es que algunos archivos son

demasiado pesados y es imposible enviarlos por correo electrónico, así que la información se graba en CD's y en discos de 3 ½ y es enviada por mensajería.

Algo que no es muy viable es hacer estos envíos puesto que el costo por envío a largas distancias representa gastos considerables para la empresa, ya que estos se hacen constantemente. Otro aspecto importante a resolver, es poder monitorear a los usuarios ubicados en las filiales, tanto por seguridad como para darles el soporte técnico que necesitan en caso de que tuvieran problemas con sus equipos; así que mientras estén "incomunicados" el corporativo con las filiales, la empresa seguirá teniendo gastos tanto en contratar los servicios de empresas externas que le proporcionen el servicio de soporte, como gastos en llamadas de larga distancia y en comunicación por radios.

2.3 Propuesta de solución

La propuesta de solución a la situación actual de la empresa que se presenta en este proyecto es la instalación y configuración de una Red Privada Virtual (VPN) que hoy en día es una de las mejores opciones de conexión de red y comunicación que hay, con este tipo de red se busca solucionar los problemas de la empresa en cuanto a comunicación tanto con clientes como con sus filiales, logrando con ello una mejor manipulación de la información en la misma. Esta propuesta tiene varios objetivos tanto generales como específicos, pero teniendo un fin en común que es la solución a los problemas en la misma.

Este tipo de conexión de red se piensa realizar por medio de un software llamado ISA Server, que además de hacer la conexión de VPN, funciona como

servidor Firewall obteniendo con esto un doble beneficio pues con este servidor se pretende controlar la salida a Internet de los usuarios de la red, y la posible intromisión de usuarios externos que puedan afectar la misma y con ello a la información de la empresa.

Los objetivos son:

Objetivo general.

El objetivo de esta propuesta es brindar una alternativa de conexión segura y rápida, dando con esto un mejor manejo de la información a la empresa Proyección y Administración Empresarial de México S.A. de C.V. ubicada en Av. Insurgentes Sur número 1898 Piso 3 Colonia Florida México D.F. cp 01050 que cuenta con filiales en los estados de Monterrey, Guadalajara, Tijuana, Tabasco y Veracruz.

Esta alternativa es la instalación de una Red Privada Virtual (VPN); con este tipo de red se obtienen grandes beneficios, de los cuales el más importante se comenta en el párrafo anterior que es una conexión rápida y segura de la empresa con sus filiales teniendo con ello un ahorro en costos comunicación de larga distancia para asesoría y soporte técnico, también se pueden monitorear los distintos equipos de la red para evitar el mal uso de éstos y riesgos para la misma por filtrado de virus. Se pretende que el costo de este proyecto sea económico con resultados a corto y mediano plazo.

Objetivos específicos.

1 Conocer el funcionamiento de las Redes Privadas Virtuales así como el de los dispositivos y seguridad utilizado en las mismas.

2 Mostrar a la empresa Proyección y Administración Empresarial de México S.A. de C.V. una alternativa más de comunicación con sus filiales por medio de este proyecto y posteriormente llevarlo a cabo para que obtenga los beneficios del mismo.

Esta investigación está orientada a la realización de un proyecto para la empresa en la cual laboro; y es una Red Privada Virtual (VPN) que hoy en día es una de las alternativas más seguras y recientes de conexión para equipos remotos que además está creciendo a pasos agigantados.

También con este proyecto se pretende mostrar los alcances de nuevas tecnologías de comunicación, las cuales pueden ser una alternativa para hacer más accesible el intercambio y manipulación de la información entre los usuarios de una red.

La importancia de esta investigación radica en la necesidad que tienen hoy en día las empresas cuya base de comunicación entre éstas y sus clientes es Internet, que a demás cuentan con filiales en lugares remotos y con las cuales tienen constante intercambio de información. Para ello una de las mejores alternativas es una VPN que representan un avance en los últimos años en cuanto a tecnología de comunicación a distancia, seguridad y redes de computadoras se refiere.

CAPÍTULO 3 DESARROLLO DEL PROYECTO DE INSTALACIÓN DE LA VPN EN LA EMPRESA PROYECCIÓN Y ADMINISTRACIÓN EMPESARIAL DE MÉXICO

3.1 Insumos a utilizar en el proyecto para la instalación de la VPN

Para este proyecto son necesarios varios insumos, los cuales se van a utilizar en la instalación y configuración de la VPN en la empresa, estos insumos son:

- **Conexión a Internet**. Para realizar la conexión VPN se necesita tener salida a Internet (de preferencia con un mínimo de 512 kbps, pero lo mejor son 1024 kbps compartidos), esta conexión es la que servirá como canal de comunicación y transporte de la información en este tipo de red.
- **Equipos que funcionaran como servidores para cada sucursal y las oficinas centrales**. Se necesitarán 2 servidores para las oficinas centrales y uno para cada sucursal. Para este proyecto se necesitan equipos con las siguientes características mínimas: 512MB de memoria RAM, procesador Pentium 4 a 3GHz o superior, 2 tarjetas de red LAN $^{10}/_{100}$ o $^{100}/_{1000}$; las tarjetas tanto de video como módem pueden ir integradas a la tarjeta madre. Si ya se cuentan con estos equipos o ya se tienen servidores con estas características no es necesario realizar el gasto en ellos.
- **Dirección IP**. Se necesita contratar una dirección IP fija para las oficinas centrales, pues es la dirección a la que filiales se van a conectar.

- **Paquetería y Software**. Para la conexión y configuración de la VPN que se plantea en este proyecto se necesitan tres paquetes, los cuales son: Microsoft Windows 2000 Server o superior, Microsoft Internet Security & Acceleration Server 2004 Standard Edition y Remote Administrator (Radmin).

3.2 Procedimiento a utilizar en el proyecto de instalación de la VPN

El objetivo de este proyecto es comunicar a las filiales de la empresa Proyección y Administración Empresarial S.A. de C.V. ubicadas en varios estados de la república con las oficinas centrales o corporativas ubicadas en el Distrito Federal; para ello se propone la implementación de una Red Privada Virtual (VPN) utilizando una conexión o VPN de acceso remoto o de cliente.

En este tipo de VPN son necesarias dos redes, una principal y una secundaria, la red ubicada en la matriz será la red principal y a ella se van a conectar las redes en las filiales (que en este caso serán las redes secundarias), formando con ello una sola red de tipo estrella (esta tipología de red se explica en el primer capítulo). En esta red los equipos tanto locales como remotos van a poder comunicarse entre sí, permitiendo con ello un fácil acceso y manipulación de la información de toda la empresa.

Posteriormente en una segunda etapa se creará en cada filial un controlador de dominio idéntico al principal para poder tener una mejor conexión entre las filiales y el corporativo, teniendo con esto una red de tipo malla donde, si se pierde la conexión con un nodo de la red que en este caso sería cada servidor de cada filial o éste falla, la red sigue funcionando de

manera normal. Con esta topología se pueden crear o modificar cuentas de usuario en el dominio de la empresa desde cada sucursal y estos cambios se vean replicados en toda la red de la empresa permitiendo con esto una conexión aún más segura y estable.

Para que todo lo anterior sea posible tanto las oficinas centrales como cada filial deben contar con su propio servidor ISA pues lo que se va a hacer es conectar dos redes independientes que en este caso son la de la matriz y la de cada una de las filiales respectivamente, estas dos redes serán los dos extremos de la VPN.

Lo primero que se tiene que hacer es instalar y configurar todos los servidores con el software necesario para este tipo de conexión. De los dos equipos que van a estar en las oficinas centrales a uno, sólo se le instalará Windows 2000 Server y al otro así como a los de las demás filiales hay que instalar tanto Windows 2000 Server como Microsoft ISA Server 2004; el Radmin se tiene que instalar en todos los servidores y equipos en la empresa pues éste es el que se va a utilizar para monitorearlos y dar soporte vía remota.

Si ya se cuenta con equipos en la empresa que tengan las características necesarias para poder funcionar como servidores ya no es necesario realizar un gasto adicional en ellos; lo único que se tiene que hacer es instalar el software necesario para que puedan realizar esta función.

Una vez instalados los servidores con el sistema operativo y el software señalados anteriormente, lo siguiente que se debe de hacer es configurarlos. En el servidor que sólo tiene instalado Windows 2000 Server (ubicado en la matriz) se tiene que configurar un controlador de dominio y crear en él, el dominio para la empresa, esta configuración así como los cambios realizados

en el dominio se verán reflejados o replicados en cada uno de los servidores ubicados en las filiales cuando la VPN esté funcionando.

El dominio que se va a crear para la empresa puede denominarse “pae.mex” y todos los equipos y usuarios que hay tanto en la red local como en cada una de las filiales tienen que unirse a él. El dominio Active Directory es una herramienta de Windows 2000 Server; aquí se van a crear o dar de alta todas las cuentas de usuario que van a pertenecer a la red general de toda la empresa. También cada servidor se va a configurar como servidor de DNS y puerta de enlace o *gateway*, por cuestiones de organización y control en la misma.

Como se mencionó anteriormente en las características de cada servidor, cada uno de ellos deberá tener dos tarjetas de red LAN que son necesarias para la configuración de la VPN y el servicio de firewall con ISA Server pues para que se puedan llevar a cabo tiene que haber 2 redes, una interna y otra externa; así que el servidor solo funciona como *host* o conector entre estas dos redes por medio de las dos tarjetas, una vez definida tanto la red interna como la red externa se crean en ISA Server las reglas de acceso y conexión entre las mismas.

La red interna por ejemplo, sería la red de las oficinas centrales y la red externa, que es tanto Internet como la red local de cada una de las filiales y viceversa para cada servidor ISA ubicado en las mismas.

Una vez configuradas las tarjetas de red para las redes interna y externa lo que se debe de hacer es configurar ISA Server en todos los servidores que se van a utilizar, aquí lo primero que se debe de hacer es empezar a dar permisos a los usuarios de la red interna para que puedan comunicarse con la

red externa y a los usuarios de la red externa con los de la interna ya que el software al instalarse cierra por completo los accesos de ambas redes por seguridad de la red misma y de los usuarios.

Dentro de las reglas de acceso en el servidor ubicado en la matriz se deben dar de alta las conexiones de cada una de las filiales con éste. Las filiales deben crear una regla similar exactamente con el mismo nombre para que cuando la VPN se levante no haya ningún conflicto al resolver el nombre de la dicha conexión. Por último en las herramientas administrativas de Windows 2000 Server en la parte de enrutamiento y acceso remoto se configura la conexión creada en ISA Server y debe conectarse en automático, de no ser así este proceso puede realizarse de forma manual.

Una vez establecida la conexión entre una red y otra, queda levantado este servicio de VPN y por lo tanto ya puede haber comunicación entre los distintos nodos de la red que en este caso son las filiales.

3.3 Plano o croquis de las redes en la empresa

En este apartado se mostrarán los planos o diagramas de cómo están distribuidos los equipos en las distintas redes que hay en la empresa, tanto en la matriz como en las filiales, además con esto se tiene un aproximado del número de usuarios que hay en la empresa que finalmente serán beneficiados con este proyecto. Estos usuarios podrían considerarse como iniciales ya que la empresa actualmente se encuentra en expansión, por lo tanto, se está contratando más personal y con ello se tendrán que adquirir nuevos equipos de cómputo que significarán más usuarios para esta red.

A continuación se muestra el diagrama de la red ubicada en las oficinas centrales o en la matriz; esta red por lógica es la más grande en la empresa ya que físicamente en estas oficinas hay un mayor espacio que en las filiales y por tanto hay más equipos y usuarios en ésta.

Las oficinas centrales de esta empresa se encuentran ubicadas físicamente en un edificio de veintiún pisos utilizando por completo el tercero y la mitad del piso veinte. Las oficinas en las filiales utilizan espacios considerablemente pequeños por lo que el número de equipos en éstas es menor, por lo tanto los diagramas de las redes en estas oficinas son un poco más sencillos.

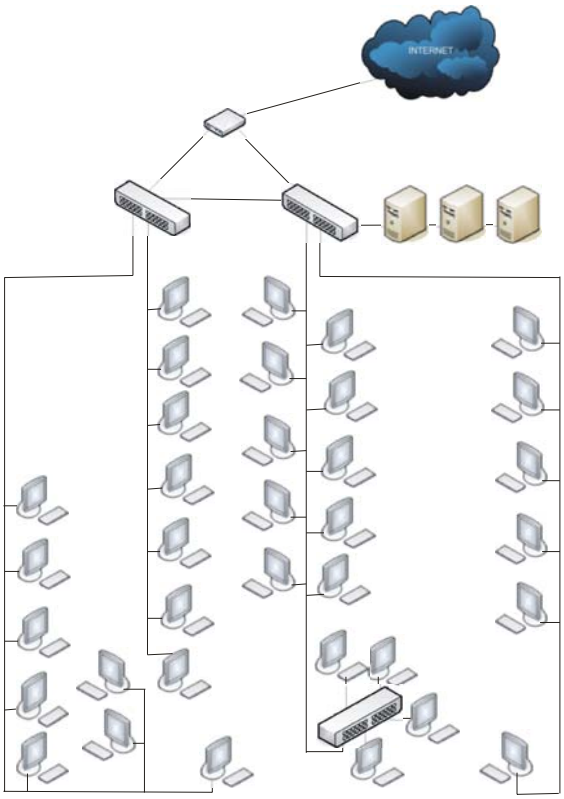


Fig. 3.1 Diagrama de la red en la matriz (piso 3)

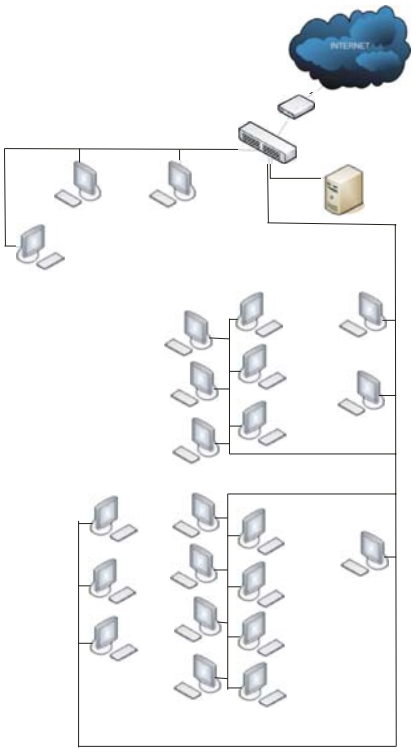


Fig. 3.2 Diagrama de la red en la matriz (piso 20)

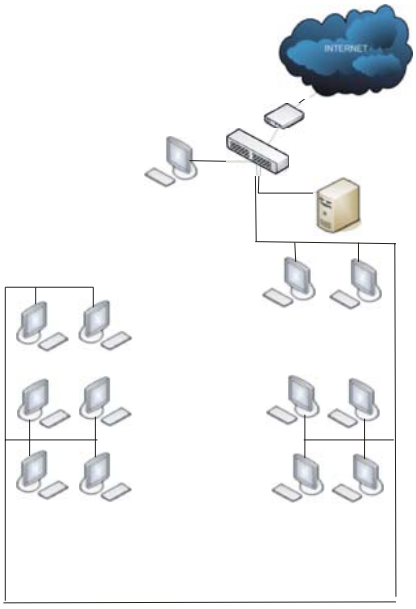


Fig. 3.3 Diagrama de la red en la filial de Guadalajara

Estos tres diagramas anteriores muestran las tres principales redes en la empresa, pues como se comentó anteriormente son los lugares en los que hay un mayor número de equipos conectados.

Los siguientes diagramas son semejantes pues solo simbolizan las redes que hay en las filiales, estos diagramas no son tan elaborados porque las oficinas son pequeñas y los equipos conectados son pocos.

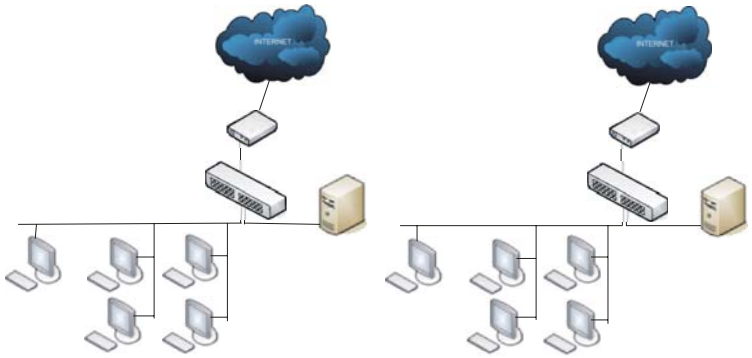


Fig. 3.4 Diagrama de la red en las demás filiales

Por último se muestra el diagrama de cómo quedaría estructurada la red general de la empresa una vez realizado este proyecto de VPN, en este diagrama se ven conectadas las filiales con la matriz por medio de túneles creados VPN, estos túneles son los que transportarán las información a través de Internet de manera segura y confiable, a demás cada servidor cuenta con su *firewall* para evitar el acceso a intrusos que pudieran dañar la red de la empresa.

Este diagrama es simbólico ya que los diagramas reales se mostraron anteriormente y éste es solo para dar a la empresa una idea general de cómo quedaría constituida su red.

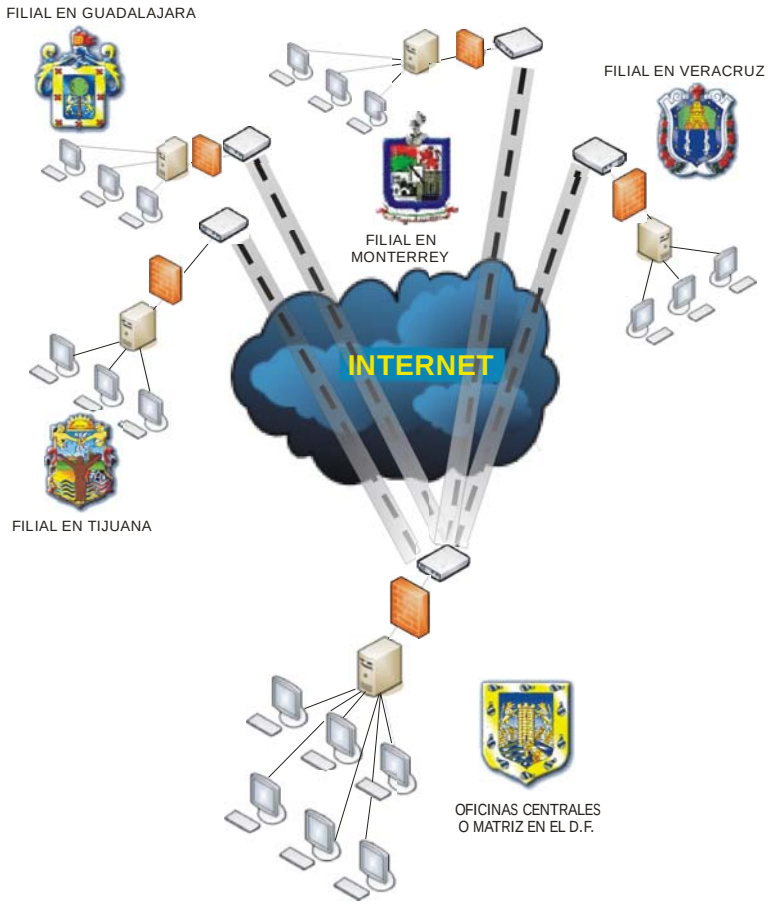


Fig. 3.5 Diagrama de la red general de la empresa unida por la VPN

3.4 Diagrama de Gantt del proyecto de VPN

Estos diagramas nos sirven para tener una mejor perspectiva del proyecto, pues nos muestran el desarrollo en cuanto a actividades que lo componen, así como la programación en tiempos de cada una. Con esto se pretende dar a la empresa una visión más amplia del proyecto que se le propone y cuanto es el tiempo aproximado en el que se realizaría.

Primero se mostrarán cada una de las etapas de realización del proyecto mediante el diagrama de Gantt que es un sencillo diagrama de barras que por un lado nos muestra en el eje “X“, las distintas tareas que se realizarán al implantar el proyecto, mientras que en el eje “Y“ se representarán los tiempos

de realización de cada una (esto contiene inicio y fin de cada tarea) por medio de barras, por lo tanto nuestro proyecto quedaría así:

Lo primero que se hace es listar cada una de las tareas y tiempos de realización en una lista, también en este caso se les asignó una letra a cada una para poder ser identificadas en el diagrama.

Tareas

A - Planeación y estudio de mercado para la implementación de la VPN (duración 15 días).

B – Adquisición de los equipos servidores y software para VPN (duración 8 días).

C – Ensamblado de equipos servidores, configuración de sistemas operativos e instalación de software para VPN (duración 8 días).

D – Configuración de software para VPN en el servidor de oficinas centrales así como de equipos terminales en dichas oficinas (duración 16 días).

E – Traslado del servidor, configuración del software para VPN en el mismo y configuración de equipos terminales en filial de Tijuana (duración 11 días).

F – Traslado del servidor, configuración del software para VPN en el mismo y configuración de equipos terminales en filial de Guadalajara (duración 11 días).

G – Traslado del servidor, configuración del software para VPN en el mismo y configuración de equipos terminales en filial de Monterrey (duración 11 días).

H – Traslado del servidor, configuración del software para VPN en el mismo y configuración de equipos terminales en filial de Veracruz (duración 11 días).

I – Conexión VPN de las oficinas filiales con las oficinas centrales.

El diagrama resultante es el que sigue:

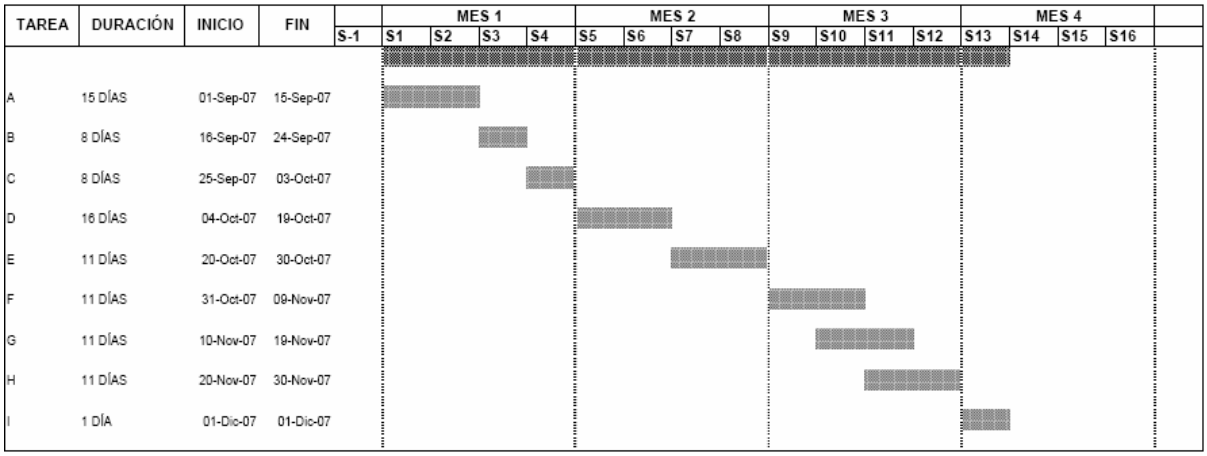


Fig. 3.6 Diagrama de Gantt del proyecto de VPN

3.5 Ruta crítica o diagrama de Pert del Proyecto de VPN

Con este diagrama se obtiene un conocimiento preciso de la secuencia planificada para la ejecución de cada actividad realizada en el proyecto y su objetivo es determinar las actividades que son necesarias, buscando con esto el plazo mínimo de ejecución del mismo.

Para la realización de este diagrama se utilizarán los mismos datos que para el anterior que son las actividades que comprenden al realización del proyecto, así como el tiempo que se necesita para realizar cada una. En este diagrama las actividades se representan con flechas y los tiempos utilizados en cada una de ellas se representan con nodos, con lo que el diagrama de Pert para este proyecto quedaría como sigue:

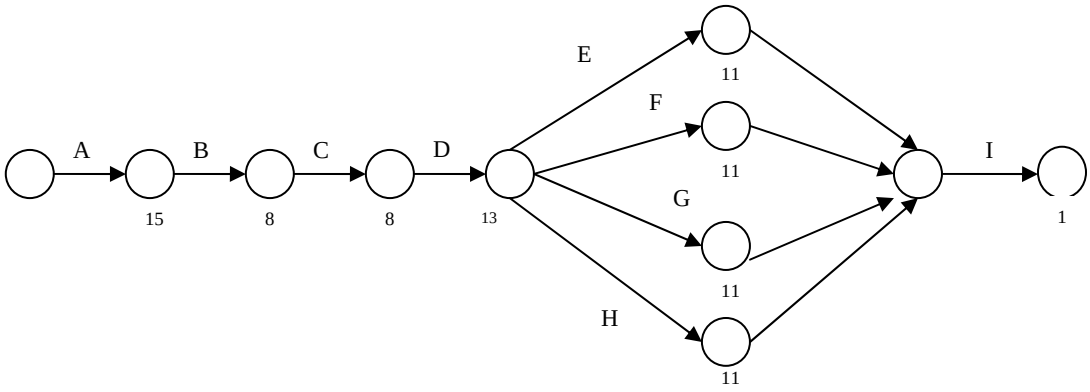


Fig. 3.7 Diagrama de Pert del proyecto de VPN

En este diagrama la ruta crítica sería "ABCDEI" porque las tareas F, G y H pueden realizarse al mismo tiempo y esto podría ahorrar el tiempo de implantación ya que se necesita la misma cantidad de él para realizarlas.

3.6 Pruebas realizadas al proyecto de VPN

Para realizar pruebas del proyecto antes de ponerlo en marcha, es necesario contar con los equipos y software necesarios para el mismo puesto que es la única forma de probar si este tipo de conexión funciona. La primera problemática que se presentó en el proyecto fue que no se tenían los recursos necesarios para hacerlas, por lo que se tuvieron que pedir prestados equipos que no se utilizaban en el momento porque ya estaban en desuso, una vez formateados se instaló lo necesario para que funcionaran como servidores y

terminales para este tipo de red; y el software para VPN, que en este caso es ISA Server, se descargó una versión demo de 30 días que fue el tiempo suficiente para probar las bondades del mismo al aplicarlo en un entorno local. Otro problema que se presentó fue la conexión a Internet pues no era la ideal para realizar este tipo de conexión pero afortunadamente funcionó, aunque no con la velocidad que se esperaba.

Una vez que los equipos estaban listos, se procedió realizar pruebas pertinentes, que constaron en crear el dominio que se utilizará en la empresa, posteriormente hay que unir algunos equipos terminales a este dominio (en este caso fueron dos) y por último, se crean las conexiones VPN pertinentes y se dan permisos a los usuarios que van a conectarse en ellas, en este caso, los servidores que van a estar en cada filial son los que se van a conectar al servidor que se encuentra en las oficinas centrales.

Es importante observar el funcionamiento de los servidores ya que éstos son quienes requieren mayor atención porque son los que nos van a servir como los puntos de conexión del túnel que se crea entre las filiales y las oficinas centrales cuando el servicio está levantado para conectar las redes de cada una.

Una vez hecho esto y observando que las conexiones VPN estaban activas y funcionando se hicieron también pruebas de transferencia de archivos de una terminal ubicada en un servidor diferente a otra ubicada en las oficinas centrales, además de utilizar también el RAdmin para controlar terminales unidas a distintos servidores y con esto se observaron los tiempos de respuesta de cada al ser manipuladas.

3.7 Implantación del proyecto de VPN

Todo proyecto tiene una implementación y se le tiene que dar mantenimiento y éste no es la excepción, así que a continuación se mencionarán estos dos aspectos importantes en el desarrollo de cualquier proyecto.

Para la implementación de este proyecto se necesita saber la problemática que tiene el cliente que en este caso es la empresa Proyección y Administración Empresarial de México, estos problemas ya están definidos en el capítulo anterior, y la solución que se le dio al cliente fue la implementación de una VPN.

Como se muestra en lo diagramas anteriores lo que se hizo después de analizar la problemática del cliente y proponer la mejor solución fue hacer un estudio de mercado para establecer qué herramientas se adecuan más al presupuesto de la empresa y con ello determinar los costos, para que una vez autorizado el proyecto se adquieran, y con ello dar comienzo esta implementación, lo siguiente que se hace es el ensamblado de cada servidor y con ello la configuración del sistema operativo adecuado a el tipo de software VPN que se va a instalar, después de instalar el sistema operativo se crea el dominio al cual vas a pertenecer los equipos de las oficinas centrales y los de las filiales.

Posteriormente ya instalado el software de VPN y configurado el sistema operativo se instala el Radmin que es el que se utiliza para poder monitorear tanto a los servidores como a los equipos terminales de cada sucursal. Una vez hecho esto se procede a trasladar cada servidor a su respectiva sucursal

para empezar a unir al domino específico a todas las terminales para poder realizar la conexión VPN que es la premisa de este proyecto.

Para esta conexión lo que se va a hacer es que en el servidor de las oficinas centrales se configuren las distintas conexiones VPN que le corresponden a cada filial y activarla para que a la hora de que se dé de alta esta conexión en la filial sólo se levante el servicio y esta quede establecida.

Una vez establecida la conexión VPN ya se podrá proveer de soporte técnico a los usuarios en las filiales a demás del traspaso de archivos de un usuario a otro como si estuvieran físicamente en el mismo lugar, ahorrando con ello tiempo y dinero de transporte de la información de un sitio a otro. También una vez levantado el servicio de VPN en la empresa en general se podrá monitorear a los usuarios remotos y locales tanto para evitar el mal uso de los equipos así como para tomar acciones o métodos preventivos para que esto no suceda como denegar los accesos a Internet que no deben tener o recepciones de correo que puedan tener virus que afecten al equipo y con ello a la información de la empresa.

Otra acción es monitorear a los servidores para verificar que funcionen correctamente y con ello garantizar a los usuarios la seguridad de su información, que es lo más importante en la empresa y que las aplicaciones que utilizan del servidor no fallen.

3.8 Mantenimiento del proyecto de VPN

Para el buen funcionamiento de la VPN se tienen contempladas dos etapas, ambas son preventivas, lo primero es hace un calendario de visitas a las

filiales, se recomienda que sea cada 3 meses para dar tanto a los equipos de cada una (servidores y terminales) realizando un mantenimiento a nivel hardware, que consta de la limpieza física del equipo, esto en la primea etapa, la segunda es que es cada mes esta limpieza sea a nivel software; en cual se realizará desde las oficinas centrales y consta en hacer depuraciones a las bases de datos que estén contenidas en los servidores de las oficinas filiales, así como un escaneo con el antivirus para estar seguros de que el los equipos están protegidos y proceder a eliminar los archivos temporales que podrían afectar el desempeño de los mismos.

También otra medida de mantenimiento es revisar mínimo una vez al mes que el sistema operativo y el software VPN estén correctamente actualizados para tener la certeza de que los equipos estén al día con ello lograr un desempeño en estos.

CAPÍTULO 4 ANÁLISIS DE BENEFICIOS LOGRADOS CON LA VPN

En éste, como en todos los proyectos hay beneficios y ventajas pero también hay desventajas y éstas pueden ser tanto de tipo técnico como de tipo económico; analizarlas nos auxiliará para determinar que tan viable y rentable es la implantación de este proyecto para el cliente, que en este caso es la empresa Proyección y Administración Empresarial de México S.A. de C.V.

En este capítulo se van a enunciar las ventajas y desventajas tanto económicas como técnicas que tiene el proyecto, en particular una Red Privada Virtual que es de lo que trata el mismo, esto con el objeto de dar a la empresa una panorámica general y una mejor opción en lo que a conexión y comunicación se refiere, y que los directivos estén convencidos de que este proyecto es bueno y acepten posteriormente que se realice y con ello cumplir como ingeniero y profesionista a la sociedad.

Como se ha mencionado anteriormente, las Redes Privadas Virtuales (VPN) crean un túnel o conducto dedicado de un sitio a otro. Los *firewalls* o ambos sitios permiten una conexión segura a través de Internet. Las VPNs son una alternativa de costo útil, para usar líneas rentadas que conecten sucursales o para hacer negocios con clientes habituales y remotos. Los datos en este tipo de red se encriptan y se envían a través de la conexión, protegiendo la información.

La tecnología de VPN proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo

privado a través de Internet. Instalando VPNs, se consigue reducir las responsabilidades de gestión de una red local.

Con base en lo anterior se pueden mencionar las ventajas y desventajas tanto económicas como técnicas de este tipo de redes.

4.1 Ventajas técnicas y económicas obtenidas con la implementación de este proyecto

A continuación se mencionarán las ventajas que nos proporcionan las VPN, que finalmente se verán reflejadas en la empresa cuando el proyecto sea aprobado e implementado.

- La principal ventaja de usar una VPN es que permite disfrutar de una conexión a red con todas las características de la red privada a la que se quiere acceder.
- El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de un equipo en esa red privada, teniendo acceso a la información publicada ahí, como: bases de datos, documentos internos, etc. a través de un canal público.
- Todas las conexiones de acceso a Internet desde ese equipo o cliente VPN se realizarán usando los recursos y conexiones que tenga la red privada.
- Diversificación de conexiones con las que podemos trabajar, como telefonía fija, ADSL, RDSI.

- Extiende la conectividad geográfica. Una VPN conecta a empleados remotos a los recursos en las oficinas centrales.
- Crecimiento en productividad de los empleados. Una solución de VPN permite a los empleados remotos aumentar su productividad de un 22% a un 45% (según la “Gallup Organization and Opinion Research”) ahorrando tiempo.
- Mejora la seguridad de Internet. Siempre en una conexión de banda ancha a Internet, hace a una red vulnerable a ataques de *hacker's* y de mas intrusos. Muchas soluciones de VPN incluyen medidas de seguridad adicional, tales como dispositivos de seguridad ("*firewall*") y antivirus de chequeo para contrarrestar las diferentes tipos de amenazas a la seguridad de la red de la empresa.
- Fácilmente escalables. Las VPNs son arquitecturas de red más escalables y flexibles que las WAN tradicionales, debido a que permiten a las corporaciones agregar o eliminar sus sistemas localizados remotamente, de forma fácil y poco costosa en función de las necesidades de la empresa.

Cuando una organización crece y más compañías deben agregarse a la red, el número de líneas arrendadas requieren aumentos drásticos. Las VPNs que utilizan Internet evitan este problema, simplemente usando el acceso geográficamente-distribuido disponible.

- Simplifica la topología de Red. La eliminación de módems y una infraestructura de red privada, simplifica la administración de la red.

- El costo bajo en una VPN. Una vez que una VPN baja el costo, está eliminando la necesidad por las líneas rentadas a largas distancias caras. La llamada para eso, proporciona el servicio de acceso remoto, los clientes de VPN sólo necesitan llamar al punto de acceso del proveedor de servicio más cercano, en algunos casos esto puede requerir una llamada de larga distancia, pero en muchos casos será una llamada local. Con las VPN's, una organización necesita sólo una conexión especializada relativamente corta al proveedor de servicio. En general, se obtiene una reducción de costos en los sistemas de comunicación de la empresa.
- Seguridad: Bajo el esquema de VPN la conexión a través de Internet es cifrada. El servidor de acceso remoto exige el uso de protocolos de autenticación y cifrado. Los datos confidenciales quedan ocultos a los usuarios de Internet, pero los usuarios autorizados pueden tener acceso a ellos a través de la VPN.
- Diseño de red simplificado: Un diseño de red con tecnología VPN se simplifica en términos de diseño de arquitectura, flexibilidad y mantenimiento, debido a que se reducen los costos asociados a la gestión de red.
- Compatibilidad: Como se aceptan la mayor parte de los protocolos de red más comunes (incluidos TCP/IP, IPX y NetBEUI), las VPNs pueden ejecutar de forma remota cualquier aplicación que dependa de estos.
- Administración centralizada: Algunos proveedores soportan la característica de administración centralizada de sus productos VPN.

Esto representa una fuerte característica de seguridad y un buen mecanismo para la resolución de problemas.

- Prioridad de Tráfico: Algunos proveedores ofrecen la funcionalidad de priorizar tráfico en sus productos VPN. Esto agrega gran flexibilidad a la empresa en cuanto a la utilización de los enlaces de Internet, debido a que se puede decidir en qué orden se preserva el ancho de banda según el tipo de tráfico permitido y de acuerdo a su importancia.
- Seguridad mejorada: Una VPN ofrece múltiples elementos de seguridad para nuestras redes, mitiga riegos externos como el falseamiento IP, el *sniffing* pasivo, la pérdida de confidencialidad y la inyección de paquetes. Además, una VPN puede proteger a nuestra intranet de virus creados en Internet.[18]
- Consolidación de recursos escasos. El hecho de tener varias oficinas y redes significa que probablemente tengamos recursos dispersos por ellas, la dispersión de recursos tiene varias consecuencias: incremento de administración, multiplicidad de elementos de hardware y software, duplicidad de esfuerzos, etc. Todo esto significa un mayor costo de propiedad (TCO).[19]

Una VPN es un método fácil para consolidar dichos recursos, lo que, en su momento, puede reducir nuestro costo total de propiedad. Además, el hardware y el software que permanecen tras la consolidación pueden aplicarse para incrementar la disponibilidad de dichos recursos.

- Transparencia para los usuarios. Otra de las ventajas principales de las VPN es la transparencia, los usuarios, las aplicaciones y, en la mayoría de los casos, incluso los *hosts*, necesitan saber que una VPN está en

18.- Oleg Kolesnikov y Brian Hatch, Redes Privadas Virtuales con Linux, Editorial Prentice Hall, Madrid España, 2003 pág.18

19.- Ibídem, pág.18

uso. Por lo tanto, la adición de software y hardware nuevo en nuestra red no necesita más configuración que la normal.

- Costo reducido. Otra ventaja que tiene que ver con el costo es que como las VPN se implementan usando una simple conexión a Internet, eliminamos la necesidad de líneas dedicadas y de infraestructura de marcación interna. El costo de un circuito dedicado al ser un enlace Frame Relay o ATM, puede ser un gasto inicial y un costo fijo significativos en la empresa. El costo del mantenimiento de las líneas telefónicas y del equipo RAS también puede ser prohibitivo. Una VPN puede llegar a ser muy atractiva al comparar las operaciones.[20]
- Facilidad de administración. Como la configuración VPN más normal, la topología red-red, es transparente para los usuarios, aplicaciones y *hosts*; estos componentes no suponen un aumento de los esfuerzos de administración o formación de la organización.[21]

Actualmente, las VPNs pueden aportar grandes beneficios a las empresas, por la diversidad de servicios que ofrecen, y que ayudan a fortalecer los objetivos de las mismas. Una estrategia de VPN debe estar basada en función a las necesidades de la empresa. Adicionalmente, se puede decir que las VPNs ofrecen muchas ventajas sobre las redes tradicionales basadas en líneas alquiladas.

En seguida se mostrará un a lista de precios de lo que se necesita para la implementación de este proyecto, este listado representa las ventajas económicas pues se muestran costos de cada componente necesario para hacer su implementación, y esto son de las características más importantes no

20.- Oleg Kolesnikov y Brian Hatch, *op. cit.,* pág.19

21.- Ibídem, pág.19

solo para nuestro cliente sino para cualquiera ya que lo que buscan las empresas es hacer el mínimo de gastos y obtener el mayor número de beneficios.

CANTIDAD	DESCRIPCIÓN DEL INSUMO	PRECIOS DE 2007
1	Equipo que funcionará como servidor	$9,623 + IVA
1	Microsoft Windows 2003 Server Estándar	$8,314.50
1	Microsoft ISA Server 2004	$21,000 + IVA
1	Radmin (paquete para 100 equipos)	$14,630
1	Contratación de una IP fija y renta del servicio de internet	$ 18,278.20 + IVA

Tabla 1. Lista de insumos necesarios para realizar el proyecto

Los precios en esta lista son vigentes durante este año 2007, tal vez parezcan elevados, pero a mediano y largo plazo proporcionan mayor rendimiento y resultan ser más caros que las llamadas de larga distancia y los envíos de información por mensajería, que además de ser costosos son más tardados.

Para ilustrar mejor lo anterior se ha hecho un pequeño análisis costo-beneficio que ayudará a sustentar mejor el ¿por qué? conviene que este proyecto sea implantado en la empresa.

Actualmente la empresa realiza gastos de envío de información y de soporte técnico, la información que más se envía es en documentos en papel puesto que los archivos son muy pesados; esta información se envía cada tercer o cuarto día.

Tomando en cuanta que el mínimo que se envía es un paquete con documentos, es costo total por envío es de $179.00, este es el costo mínimo

porque hay ocasiones en las que es costo excede los $350.00; por lo tanto en envíos se gasta alrededor de $537.00 a la semana en envíos pequeños y alrededor de $1050.00 en envíos grandes.

Otro aspecto que representa gastos para la empresa son los que se hacen por servicios de soporte técnico (que a veces no representa gran trabajo por parte de la empresa que lo ofrece), muchas veces se requiere de por lo menos 4 veces al mes de este servicio, consumiendo este gasto alrededor de $350.00 por sesión lo que nos arroja un total de $1400,00 al mes.

Por lo tanto el gasto mensual de la empresa en la adquisición de estos servicios equivale a gastar alrededor de entre $3548.00 y $5600.00 al mes. Tomando estas cifras podemos arrojar la siguiente tabla comparativa:

COSTO TOTAL DEL PROYECTO POR FILIAL		**GASTO QUE REALIZA LA EMPRESA POR FILIAL**	
EQUIPO SERVIDOR	$11,066	GASTOS MENSUALES POR CONCEPTO DE PAQETERÍA	$4,200
WINDOWS 2003 SERVER	$8,314.50	GASTOS MENSUALES POR CONTEPTO DE SOPORTE TÉCNICO	$1,400
MICROSOFT ISA SERVER 2004	$24,150		
RADMIN (PAQUETE PARA 100 EQUIPOS	$14,630		
CONTRATACIÓN DE IP FIJA Y SERVICIO DE INTERNET	$21,019		
TOTAL	**$79,179**	**TOTAL**	**$ 5,600**

Tabla 2. Lista de costos del proyecto y gastos de la empresa.

Observando la tabla anterior pareciera que los gastos mensuales de la empresa son menores que los de el proyecto en sí, pero haciendo la suma de gasto totales mensuales de la empresa, en un año se reuniría casi la misma cantidad. Por lo que en un año y 3 meses aproximadamente se recuperaría la inversión del proyecto y no se tendrían que realizar más dichos gastos.

Por lo tanto el proyecto es rentable, económicamente y por las ventajas de las VPN antes mencionadas, se tendrían más beneficios que solo los económicos y la empresa estaría más segura en cuanto a infraestructura y más comunicada pues como se mencionó antes lo que también se busca con este proyecto es centralizar las redes de la empresa en una sola y con ello tener un mejor manejo de la información por parte de los usuarios de la misma.

4.2 Limitaciones técnicas y económicas obtenidas con la implementación de este proyecto

Todo proyecto tiene ventajas y desventajas, y este no es la excepción, así que a continuación se mencionaran las desventajas que se tienen al implementar este tipo de red, que comparadas con las ventajas son menores, de lo contrario el proyecto que se plantea para el cliente no sería rentable. Estas desventajas de las VPN están relacionadas con la implementación, solución de problemas, autenticación y disponibilidad de Internet.

Considerando que los defensores de las VPN aclaman economías del costo como la ventaja primaria de esta tecnología, los detractores citan costos ocultos como la desventaja primaria de VPNs.

Entre los inconvenientes de este tipo de red podemos citar: una mayor carga en el cliente VPN puesto que debe realizar la tarea adicional de encapsular los paquetes de datos una vez más, situación que se agrava cuando además se realiza encriptación de los datos que produce una mayor lentitud de la mayoría de conexiones. También se produce una mayor complejidad en el tráfico de datos que puede producir efectos no deseados al cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (*proxy,* servidor de correo, permisos basados en nombre o número IP).

El uso de encriptación en la conexión VPN puede ser necesario en aquellos casos que la información que se vaya pasar por el túnel sea sensible y requiera privacidad. La conexión encriptada VPN requiere de bastantes recursos tanto en el servidor de túnel como en el ordenador cliente de VPN, a parte de requerir la instalación de software especial en el cliente. Hay que recordar que muchas aplicaciones y programas ya hacen dicha encriptación y el encriptar el túnel VPN no nos aporta seguridad adicional. Aplicaciones tales como el correo seguro leído por medio del interface web seguro o una conexión a una máquina multiusuario son suficientemente seguras para no requerir la encriptación adicional.

Al encriptar entre el servidor de la aplicación y el cliente de la misma, la conexión es absolutamente segura en todo su recorrido, mientras que en una conexión VPN segura, la encriptación sólo tiene lugar entre el servidor de túnel y el cliente VPN; y la conexión entre el servidor de túneles y el servidor de la aplicación se realiza sin encriptación.

- La implementación puede consumir mucho tiempo. A veces, la implementación de una VPN puede ser difícil y consumir mucho tiempo, la planificación de la configuración, la administración de las claves y la solución de problemas pueden convertir fácilmente lo que a simple vista es sencillo en semanas de trabajo.[22]
- Dificultades a la hora de solucionar problemas. Como en una VPN los datos entran en una puerta de enlace sin cifrar y la abandonan una vez cifrados, el proceso de solución de problemas puede ser complicado. Aspectos tales como la falta de sincronización de las claves, los fallos de autenticación, los paquetes eliminados y la carga y sobrecarga de la puerta de enlace pueden hacer que la localización de los problemas de una VPN sea una tarea difícil.[23]

Para hacer que nuestra VPN sea confiable, tenemos que asegurarnos de que sus administradores entiendan claramente la arquitectura de software subyacente y tengan un conocimiento global de los protocolos de Internet.

- Red+Red=Gran dominio autenticado. Debido a que estamos conectando dos redes de forma transparente, la autenticación entre ellas se convierte en un problema. ¿Confiamos en que los usuarios de la otra red van a utilizar los recursos de la nuestra en forma responsable? Además ¿Confiamos en la seguridad de la otra red? si un pirata mal intencionado obtiene acceso a la otra red, podría obtener también acceso a la nuestra.[24]

22.- ibídem, pág.19

23.- Oleg Kolesnikov y Brian Hatch, *op. cit.,* pág.20

La planificación de una VPN red-red debería implicar una coordinación estrecha con los administradores y directores IT de todas las redes. Tenemos que asegurarnos de que todos conocen bien los riesgos de seguridad asociados con el software y hardware que vamos a utilizar y de que han considerado la opción de la autenticación para mitigar los riesgos de confianza ciega.

- ¿Internet? 99% de disponibilidad. Aún con todas las ventajas de las VPN, una cosa que no podemos asegurar es la alta disponibilidad. Como las VPN confían en Internet para el transporte, un servicio VPN podría interrumpirse a veces durante caídas de Internet. Esto se puede originar no sólo en nuestro ISP, también en las redes intermedias.[25]

Si un nodo o enlace en la ruta de una red a otra se estropea, la restauración del servicio puede llevar un tiempo. Si el tiempo activo es una necesidad crítica de nuestra VPN, es posible que debamos considerar la utilización sólo de ISP que ofrezca acuerdos a nivel servicio (SLA) a sus clientes.

Esta situación difiere de las líneas dedicadas, ya que estas últimas tienen muchos menos puntos de fallo de VPN. Si el tiempo de actividad y el ancho de banda son un factor importante, tenemos que asegurarnos de comparar nuestras opciones con cuidado. En algunos casos las líneas alquiladas podrían ser más apropiadas.

- Interoperatividad entre fabricantes. Dada la cantidad de fabricantes que ofrecen soluciones VPN y la naturaleza compleja de los protocolos de las

24.- Ibídem, pág.20

25.- Ibídem, pág.20

VPN como, por ejemplo, IPSec, puede ser difícil obtener soluciones de diferentes fabricantes que sean compatibles entre sí.[26]

Estas son las desventajas y limitaciones más significativas que tiene las VPN, pero la mayoría de éstas pueden ser resueltas y esta solución muchas veces no se ve reflejada en más gastos para el cliente ya la mayoría son resueltas con una buena planeación; por esta razón el proyecto que se plantea en este trabajo es considerado viable para la empresa y puede traer muchos beneficios para la misma.

26.- Oleg Kolesnikov y Brian Hatch, *op. cit.,* pág.21

CONCLUSIÓNES

Como conclusión, las Redes Privadas Virtuales hoy en día se han convertido en una necesidad para aquellas empresas u organizaciones que cuentan con filiales y clientes que se encuentran a grandes distancias de sus oficinas centrales; además de que también son una herramienta muy eficiente y segura en cuanto a conectividad de red, manipulación de la información y seguridad se refiere.

Otro aspecto importante de este tipo de conexión de red es que su costo de implementación no es tan elevado y en cuanto a configuración es bastante accesible con los usuarios lo cual, en la actualidad, es básico para los clientes no solo de este tipo de servicio sino de cualquiera.

Así que con estos aspectos y los beneficios y/o ventajas mencionados anteriormente, se tienen las bases suficientes para ofrecer a la empresa, con la implementación de este proyecto, una herramienta confiable que cubra con sus necesidades y que traiga consigo beneficios adicionales tales como mejoras en la productividad y servicio a sus clientes.

GLOSARIO

Autenticación: Establecer la identidad de un usuario para transacciones seguras de e-commerce y VPN.

Asociación Internacional de Seguridad Computacional: (denominada ICSA, por sus siglas en inglés International Computer Security Association) - fija estándares de desempeño para productos de seguridad de información y certifica cerca del 95% de la base instalada de dispositivos de seguridad ("firewall"), antivirus, criptografía y productos IPSec.

Bit: Es la unidad más pequeña de información y la unidad base en comunicaciones.

Byte: Conjunto de bits continuos mínimos que hacen posible, un direccionamiento de información en un sistema computarizado. Está formado por 8 bits.

DES: (Estándar de Encripción de Información, 3DES, Data Encryption Standard) - Un método de criptografía estándar del NIST de clave secreta que usa un llave de 56 bits (DES) o una llave de 168 bits (3DES).

Datagramas: Son paquetes de información.

Encripción: El proceso de tomar toda la información que una computadora esta enviando a otra y codificarla de una manera que sólo la otra computadora será capaz de decodificarla.

Extranet: Una extranet es una red privada que usa los protocolos de Internet y el sistema público de telecomunicaciones para compartir, de modo seguro, parte de la información de un negocio o las operaciones con proveedores, vendedores, socios, clientes u otro tipo de negocios. Una extranet puede ser considerada como parte de la intranet de una compañía que se amplía a usuarios que están fuera de la empresa.

Firewall: Dispositivo de seguridad que controla el acceso desde Internet a una red local usando información asociada con paquetes TCP/IP para hacer decisiones sobre si se permiten o niegan accesos.

Intranet: Red TCP/IP de una empresa que utiliza los protocolos y normas abiertas que han surgido a partir de Internet .(Para fines de siglo ya habrá 4,6 millones de intranets y tan sólo 440.000 servidores de Internet (IDC))

Interfaces: Conexión que permite la comunicación entre dos o más dispositivos.

IPsec: Realmente es una colección de múltiples protocolos relacionados. Puede usarse como un VPN completo en la solución protocolar, o simplemente

como el usó de encriptación formando planes dentro de L2TP o PPTP. IPsec existe en la capa de la red (Capa Tres) en OSI.

Módem: (modulador-demodulador) modula las señales digitales que salen de un ordenador u otro dispositivo digital para convertirlas en señales analógicas para que puedan ser enviadas por una línea telefónica convencional de par entrelazado de cobre, y demodula la señal analógica para convertirla en una señal digital que pueda ser interpretada por el dispositivo.

Paquete: Fracciones de un mensaje de tamaño predefinido, donde cada fracción o paquete contiene información de procedencia y de destino, así como información requerida para el reensamblado del mensaje.

Pinchado de líneas. Espiar y obtener la información que circula por una red telefónica o informática por medio de sniffers. Similar al sniffing es el snooping, pero en este último la información obtenida es guardada en el sistema espía en forma de archivos.

PSI: Proveedores Independientes de Servicio.

Protocolo: Conjunto de reglas que posibilitan la transferencia de datos entre dos o más computadoras.

Rechazo de Servicio: (denominado DoS, por sus siglas en inglés Denial of Service) - un ataque de hacker diseñado para deshabilitar un servidor o red al saturarlo con solicitudes de servicio el cual previene a usuarios legítimos de accesar a los recursos de la red.

Red: Es una colección de estándares, basada en dispositivos que encadenan todo lo referente a la compañía, como computadoras de escritorio, anfitriones y recursos, sin sacrificar velocidad, costo o maniobrabilidad.

Routers: son dispositivos que nos permiten unir varias redes(más de dos, a diferencia de los bridge), tomando como referencia la dirección de red de cada segmento. Al igual que los bridges, los Routers restringen el tráfico local de la red permitiendo el flujo de datos a través de ellos solamente cuando los datos son direccionados con esa intención.

Router: es un dispositivo físico que une redes múltiples juntas. Técnicamente, un router es una "capa de 3 entradas", significa que se conectan redes (como entradas), y que opera a la capa de la red del modelo de OSI.

Servidores: Computadores que proporcionan servicios a las estaciones de trabajo de la red tales como almacenamiento en discos, acceso a las impresoras, unidades para respaldo de archivos, acceso a otras redes o computadores centrales.

Sniffer: Es un programa que intercepta la información que transita por una red.

Sniffing: Es espiar y obtener la información que circula por la red.

usuarios.lycos.es/elimperdible/glosario.html

Trama: Tira de bits con un formato predefinido usado en protocolos orientados a bit.

Tunel: Técnicas de encapsulado del tráfico.

BIBLIOGRAFÍA

1. A. Gallo Michael y William M. Hancock, Comunicación entre computadoras y Tecnologías de redes, Editorial Thomson, Argentina, 1997, 632 pp.

2. A. Menascé Daniel, Redes de Computadoras Aspectos Técnicos y Operacionales, Editorial Campus LTDA, España, 1988, 523 pp.

3. Barba Marti Antoni y Javier Hesselbach Serra, Inteligencia de Red, Editorial Editions Universitat Politécnica de Catalunya, Barcelona, 2002, 297 pp.

4. Black Uyless, Redes de computadores. Protocolos, Normas e Interfaces, Editorial Alfaomega, Madrid, 1995, 585 pp.

5. Cazares Hernández Laura *et. al.,* Técnicas Actuales de Investigación Documental. Editorial Trillas UAM, México, 1980, 283 pp.

6. Fitzgerald Jerry y Denis Alan, Redes y comunicación de datos en los negocios, Editorial Limusa Wiley, México, 3ra Edición, 2003, 516 pp.

7. Hernández Sampieri, Metodología de la Investigación, Editorial Mc Graw-Hill

8. J. Molina Francisco, Redes de Área local, Editorial Alfaomega, México, 2004, 525 pp.

9. López R. Miguel, Normas Técnicas y de Estilo para el trabajo académico, Editorial UNAM. México, 2000, 139 pp.

10. Oleg Kolesnikov y Brian Hatch, Redes Privadas Virtuales con Linux, Editorial Prentice Hall, Madrid España, 2003, 217 pp.

11. Raya José Luis y Cristina Raya, Redes Locales, Editorial Alfa omega, Madrid, 2002, 335 pp.

12. S. Tambawm Andrés, Redes de Computadoras, Editorial Pearson, México, 3ra Edición, 1997, 157 pp.

13. Terienbaum, Redes de Ordenadores, Editorial Prentice-Hall, México, 1991, 352 pp.

14. Zorrilla Arena Santiago, Introducción a la Investigación, Editorial Aguilar León y Cal., España, 1999, 463 pp.

16. www.novadevices.com/vpn.pdf, 17 octubre de 2006, Página principal

17. www.pcwla.com/pcwla2.nsf/0/, 15 agosto de 2006, Página principal

18. http://www.empretel.com.mx/MULTITECH/VPN/, 22 septiembre de 2006, Página principal

19. www.icsa.com , 22 de octubre de 2006, Página principal