VNIVERSIDAD NACIONAL AVFNOMA DE MEXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

ARAGÓN

"PROPUESTA DE UNA RED PRIVADA VIRTUAL (VPN) SOBRE INTERNET UTILIZANDO DIFERENTES SISTEMAS OPERATIVOS Y EL PROTOCOLO DE ACCESO PUNTO A PUNTO (PPTP), COMO UNA ALTERNATIVA PARA MEJORAR EL ACCESO Y SEGURIDAD EN REDES LAN".

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

JHONI VARGAS FLORES

ASESOR: M. en C. DAVID MOISÉS TERÁN PÉREZ

MÉXICO 2005

Agradecimientos:

A la Universidad Nacional Autónoma de México por haberme brindado la oportunidad de ser parte de esta gran institución y de la que me siento muy orgulloso.

A la Facultad de Estudios Superiores "Aragón", por haber contribuido de manera sustancial en mi formación y de la que igualmente me siento muy orgulloso.

A Dios por haberme dado licencia de llegar hasta aquí.

Muy en especial a mis Padres Benjamín Vargas Cerda y Martha Flores Rodríguez, que me han enseñado todo lo que soy, por haber hecho de mi una persona con unos valores muy firmes, y principalmente por haberme brindado la oportunidad de haber llegado hasta aquí.

A mis Hermanos: Benjamín Vargas Flores, por el apoyo, respaldo y por la ayuda siempre dispuesta. Alejandro Vargas Flores, por las diferentes formas de apoyo brindado a lo largo de esta carrera, y por ser un ejemplo de responsabilidad y fortaleza.

A mi Novia Diana Alejandrina López Martínez, por el apoyo incondicional y la ayuda proporcionada para llevar acabo este trabajo.

A mis Sobrinos que de alguna manera hacen mi vida más Alegre: Edith Alejandra Vargas Salazar, Héctor Miguel Vargas Mejía, Erick Scottie Vargas Salazar, Brenda Dayana Vargas Mejía y Paola Abigail Vargas Salazar.

A mis Tíos: Armando Alvarado y Concepción Vargas por el apoyo y confianza incondicional en los momentos que más los necesite.

A mis Padrinos Juan Salazar Granados e Hilda Pérez Suárez, por el apoyo, amistad y confianza brindado a lo largo de todos estos años.

A Margarita Flores por la ayuda que de alguna manera fue en mi niñez.

A mis Amigos de Toda la Vida: Antonio Rodríguez Díaz, Noel Salazar Villalón, Alberto Palma Castro, Ubaldo Eloy, Ángel Denova, Jesús Denova, Diego Bello, Humberto Zapote, Ángel (rabiada), Fabián López, José Manuel (El gordo), Elizabeth Rueda, Leticia (CCH), Catalina Román, Luz castañeda, Guadalupe Simón, Isaías Silva, Gerardo Pérez, y Sandra (CCH), Trinidad Salazar.

A mis Compañeros y Amigos de Carrera: Jonathan García, Adán Olmedo, Alejandro Ortiz, Rubén Morales, Arturo Jácome, Osvaldo Armida, Yadira Pérez, Maribel Román, Itzel Basurto, Diana López, Edgar Morales, Omar García, Emanuelle Carmona, Mauricio Algalan, Omar (IME), Ernesto, Omar Cortés, Sergio Espinosa, Marco Auyón, Jesús Anaya, David, Adolfo Anaya, José Compean, y Armando (Armandí).

Al M. en C. David Moisés Terán Pérez, por el tiempo y apoyo brindado para la realización de esta tesis.

A mis Revisores Ing. Fernando Márquez Chávez, Ing. Trinidad Escamilla Sánchez, Ing. Enrique García Guzmán, e Ing. Matías Artemio Nicolás Osorio, por el apoyo brindado para la realización de este trabajo.

A mis Maestros: Ing. Roberto Pérez Mera, Ing. Hugo Portilla por haber hecho una agradable instancia en la facultad.

Al M. en C. Marcelo Pérez Medel, Jefe de la carrera de Ing. en Computación por las facilidades y apoyos brindados.

Al Lic. Jorge Juárez por los consejos pronunciados.

A mis más Recientes Amigos: Hugo Salazar, Ángel Cisneros, José Carlos (Carmelo), Miguel Granados, Iván Salazar, Alejandro Merced, Luis Merced, Vanesa, Carlos Merced, Armando (fushiño), Ruth, Biny S, Dulce López, Alejandra Martínez, y Gonzalo López.

A la Familia: Vargas Cerda y Familia: Flores Rodríguez, de las que formo parte.

A todos los que de una forma u otra contribuyeron a hacer realidad este sueño, no me resta más que decirles:

Mil gracias.....

INDÍCE. **Pag.**

Capítulo I: Conceptos Básicos.

Capítulo V. La Seguridad de las VPN.

PLAN PROPUESTO.

Capítulo I: Conceptos Básicos.

En este primer capítulo, se presentan los fundamentos de las redes de cómputo, desde sus orígenes, clasificación, medios de transmisión, estándares, sistemas operativos y su seguridad.

Capítulo II: Red Privada Virtual

Aquí se describe, qué constituye a la tecnología VPN, áreas, ventajas, desventajas, y su comparación contra otras tecnologías convencionales, así como su crecimiento.

Capítulo III: Arquitecturas y Topologías.

Las VPN aparecen en una gran en una gran variedad de formas, aquí se vera cuales son las principales arquitecturas y su esquema general. También se muestra cuales son las diferentes topologías que existen hoy en día de VPN.

Capítulo IV: Protocolos Usados en una VPN.

Tres son los principales protocolos de túnel empleados para realizar una VPN, se vera como funciona cada uno, su similitud y diferencias. Pero principalmente se analiza a PPTP.

Capítulo V: La Seguridad de las VPN.

La seguridad de las VPN es una parte esencial, para hablar de seguridad se establece qué es la criptografía, el cifrado, autenticación, y cuál es la seguridad que ofrece el protocolo PPTP.

Capítulo VI: Propuesta de una VPN:

En este último capítulo, se integra los diferentes elementos para poder proponer la implantación de una VPN, basada en el protocolo (PPTP), así como mostrar la configuración del servidor basado en Windows 2000 Server, y los usuarios remotos basados en diferentes sistemas operativos desde Windows 98 hasta Windows XP.

ANEXO I: Procedimientos de configuración de Windows 2000 Server.

La información de este anexo muestra los diferentes procedimientos necesarios para la configuración del servidor VPN, funcionando como una guía paso a paso.

ANEXO II: Pruebas de Rendimiento para Windows 2000 Server Realizado por NSTL.

Las pruebas de rendimiento darán un panomarama más del uso de PPTP.

ANEXO III: Glosario.

El glosario de términos tiene la finalidad de poder ayudar a la compresión de palabras utilizadas en el presente trabajo de tesis.

Justificación.

Las razones por las que las organizaciones están tan interesadas en Internet son muchas. La ubicuidad es una, la escalabilidad es otra y, por supuesto, la accesibilidad en costo. Como respuesta a tales ambiciones, las organizaciones están luchando con el desafió de conectar socios de negocios, clientes, proveedores y ubicaciones remotas de campo, sucursales y empleados móviles directamente en línea a la red de la empresa. Sin embargo, la mayor parte de las organizaciones están de acuerdo en que el uso sin precauciones de Internet como columna vertebral de comunicaciones de la empresa, pondrá a toda la red en riesgo ante un intruso astuto.

Antes, las opciones eran obvias. Desarrollar su propia red privada, contratar un proveedor de servicio de Internet (ISP) utilizar Internet con grandes riesgos. El costo de las líneas arrendadas o dedicadas y el acceso de marcado telefónico, soportado por servidores de comunicaciones, bancos de módems y números de llamada sin costo (todos ellos requisitos críticos de las redes privadas), pueden resultar muy altos y, por tanto, fuera del alcance de muchos negocios. De manera similar, el uso de un ISP podría también ser muy costoso. Sin embargo, Si se consideran las innovaciones recientes en facilidad de uso y creciente funcionalidad, junto con constante maduración de estándares críticos para privacidad de datos, la tecnología de VPN surge como la clara elección para construir una red privada, aunque sea virtual, sobre la Internet pública.

En este trabajo de tesis se pretende dar un panorama y propuesta de una VPN manteniendo este propósito en mente.

Objetivos.

Objetivo General:

Proponer cómo una VPN basada en el protocolo de acceso punto a punto (PPTP), y diferentes sistemas operativos es una alternativa para mejorar la seguridad y el acceso a redes LAN, y al mismo tiempo convertirla en una red WAN.

Objetivo capítulo I:

Conocer las bases de las redes de cómputo, así como sus diferentes clasificaciones, tecnologías y principales problemas.

Objetivo capítulo II:

Conocer qué es una red privada virtual (VPN), bases, funcionamientos, así como sus ventajas y desventajas.

Objetivo capítulo III:

Conocer el panorama de las diferentes arquitecturas y topologías de VPN, así como los elementos que las conforman.

Objetivo capítulo IV:

Saber cuáles son los protocolos de túnel empleados por las redes privadas virtuales, así como su funcionamiento, similitud y diferencias.

Objetivo capítulo V:

Conocer cómo es la seguridad de las VPN, componentes, tecnologías y funcionamiento.

Objetivo capítulo VI:

Dar a conocer una propuesta de VPN basada en el protocolo (PPTP), explicando cómo instalar y configurar un servidor VPN basado en Windows 2000 Server, los clientes remotos basados en diferentes sistemas operativos de Windows, como una alternativa de bajo costo para mejorar la seguridad y el acceso a redes LAN.

INTRODUCCIÓN.

En 1995, el uso de Internet en los negocios se hizo casi cotidiano. La mayoría de los hombres de negocios, que habían estado ansiosos por la maravillosa explosión de Internet, ya no se resistieron. A finales de 1995, casi la mitad de los noventa muchos sitios Web eran comerciales. Las corporaciones estadounidenses lograron discernir la verdadera promesa de Internet, era accesible desde todas partes del mundo (ubicuo). Podía soportar aplicaciones a medida que aumentaban de tamaño con relativa facilidad (escalable). Y lo más importante era que los análisis habían probado que Internet resultaba la elección más accesible en costo para una red de comunicaciones que abarcara toda una empresa. Sin embargo, a medida que más y más hombres de negocios se inclinaban por cosechar los beneficios de Internet, reportes alarmantes de extraños acontecimientos surgieron en la sociedad abierta de Internet.

Internet seguía creciendo sin una autoridad centralizada. Entre 1989 y 1998, investigaciones de la industria indicaron que Internet creció un 340 por ciento anualmente. En algún lugar del proceso, atrajo a cierta comunidad de usuarios, que no compartían el mismo espíritu altruista que los fundadores tenían en mente y que practicaban las comunidades académicas, de investigación y empresariales. Como con cualquier sociedad libre, los recién llegados surgieron en parte debido a su apertura y en parte debido a la ausencia de ciertas reglas y reglamentos. Sin embargo, llegaron principalmente para divertirse y crear confusión, y quizá para causar estragos. Estos merodeadores eran los "Ángeles del Infierno" de la supercarretera de la información. Hoy en día se les conoce, casi con reverencia en ciertos círculos, como intrusos astutos.

Las incursiones de los intrusos han plagado Internet durante casi una década. Algunas hazañas han recibido tal notoriedad que en las culturas pop de Internet, los intrusos han alcanzado nivel de estrellas de rock. Al principio, las grandes juergas se limitaban a macro virus que provocaban que el software realizara erráticamente las tareas. Con el tiempo, se ejecutaron subrepticiamente hazañas más complejas con software de husmeador y con trucos de "Caballo de Troya" para robar contraseñas de usuario. Hoy, los intrusos participan en operaciones secretas a escala total con ataques de nombres amenazantes como "Ping de la Muerte", junto con sesiones de secuestro y ataques de comando de puerta secreta. La Asociación Estadounidense de Seguridad en las Ordenadores publicó un informe (Agosto de 1997), en que se tomó como muestra a una serie de negocios en Estados Unidos, además de gobiernos federales, estatales y locales. El 44 por ciento de quienes respondieron reportaron ataques externos a sus sistemas que habían sido documentados. Otro estudio reveló que las redes del Departamento de Defensa de Estados Unidos son atacadas alrededor de 250 mil veces al año.

Los intrusos crearon y siguen creando circunstancias desafortunadas para Internet. Como resultado, Internet tiene reputación de padecer graves problemas de seguridad. Por tanto, evitar Internet para aplicaciones de negocios importantes no es una elección difícil. Una encuesta de 1998 realizada por el Grupo Abierto, consorcio que dirige los estándares de seguridad, encontró que solo una de cada siete empresas (14 por ciento) deseaba vincular sus aplicaciones críticas a Internet.

A pesar de su reputación de padecer debilidades de seguridad, los beneficios potenciales de Internet no son fáciles de ignorar. En realidad, el potencial es imponente. Para ponerlo de manera muy obvia, Si no existieran los problemas de intrusos, Internet proporcionaría una infraestructura de comunicaciones ideal para redes de área amplia empresariales. En comparación, las soluciones alternativas que comprenden líneas arrendadas, redes de datos públicos (a diferencia de Internet, que es público) o proveedores de servicio de Internet (la base de las redes privadas) son costosas.

El gasto asociado con el establecimiento y la administración de una red privada propia es, quizá, la razón más apremiante por la que las empresas de Estados Unidos siguen escudriñando Internet con gran atención. Si de alguna manera se pudiera aprovechar Internet y proteger los propios activos de información contra las legiones de intrusos que operan de manera encubierta desde casas seguras de Internet, los negocios volverían a gravitar hacia Internet para realizar transacciones de negocio a negocio.

Las Redes Privadas Virtuales (VPN) están abriendo camino para que las empresas regresen a las supercarreteras de información de Internet. Los avances y la integración completa de tecnologías clave de encriptación, autenticación y protocolos de entunelamiento hacen que sea posible establecer redes privadas virtualmente seguras a través de un medio muy público como Internet. La maduración de los estándares también juegan un papel fundamental. En otras palabras, las VPN le permiten construir y operar una red empresarial basada en Internet que sea plenamente resistente a los ataques de intrusos. Las VPN también proporcionan a las empresas una alternativa viable a las costosas redes privadas que dependen de líneas arrendadas, redes de datos públicos o un ISP. El advenimiento de las VPN señala el principio de una nueva era (en la que se verá a muchos negocios migrar a Internet para soportar aplicaciones de misión crítica).

Las VPN han puesto todo el potencial de Internet al alcance de la comunidad de red corporativa.

Conceptos Básicos.

Capítulo I: Conceptos Básicos.

1.- Redes de Cómputo.

1.1.- Antecedentes históricos.

El vertiginoso avance tecnológico que han experimentado los campos de la electrónica y de la computación en los últimos 50 años, permitieron incrementar la capacidad y velocidad de los sistemas de comunicación de datos. Por esta razón se considera importante conocer el desarrollo de los ordenadores en sus diversas etapas, así como los distintos mecanismos para su interconexión.

1.2.- Breve Historia de los Ordenadores.

En 1834, el inglés Charles Babbage anticipó el nacimiento de lo que hoy se conoce como ordenador, inventando una "máquina diferencial" capaz de computar tablas matemáticas mediante un complejo sistema de engranes. En 1843, Lady Ada Augusta Lovelace (auspiciadora económica del invento de Babbage), le sugirió que utilizara tarjetas perforadas empleadas en los telares electromecánicos para proporcionarle distinta información a su máquina, esto le evitaría tener que cambiar los engranes y mecanismos al hacer un cómputo diferente (Sosa,1999).

Por otra parte, mientras trabajaba en el perfeccionamiento de su invento, Babbage concibió la idea de una "máquina analítica", capaz de tener una comunicación "inteligente", la llamó "la locura de Babbage". Después sirvió como modelo de inspiración para los futuros inventores de lo que hoy se conoce como ordenador (Gs comunicaciones, 1998).

1.2.1.-Ordenadores electrónicos.

La idea de utilizar dispositivos de conmutación, primero eléctricos y después electrónicos, fue motivada por la necesidad de crear un lenguaje sencillo con el que una máquina podría comunicarse con las personas (a través de la representación de señales eléctricas en unos y ceros en un código binario), también por que los dispositivos electrónicos son más veloces que cualquier dispositivo mecánico jamás construido (Gs comunicaciones, 1998).

2.-Evolución de las Redes de Cómputo.

El primer paso de la evolución de las redes de cómputo se inició con el empleo de terminales tontas; utilizadas únicamente para enviar información hacia un ordenador central llamado anfitriona o principal como se muestra en la Fig. 1.1

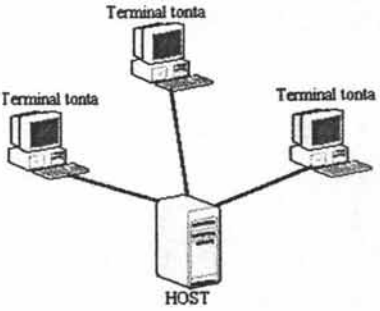


Fig. 1.1: Empleo de terminales tontas para el envió de información a un ordenador central.

Posteriormente, apareció el concepto de tiempo compartido, que consistía en la conexión de terminales tontas a un host el cual distribuía la atención a los usuarios conectados a él en diferentes tiempos. Este ordenador se encontraba enlazado a una microcomputadora (mainframe) que realizaba el procesamiento.

Con la introducción del procesamiento en tiempo real, el usuario podría ver el resultado del procesamiento de la información en cuanto la tecleaba. El incremento en el uso del tiempo compartido por más usuarios creó la necesidad del manejo de estándares para lograr agilizar la comunicación con el ordenador anfitrión, ya que cada ordenador manejaba distintos estándares.

En 1964 se crea el estándar para el intercambio de información ASCII (American Standard Code for Information Interchange), el cual consta de 128 caracteres formados con 7 bits cada uno.

El nacimiento de las microcomputadoras u ordenadores personales marco la pauta de lo que sería la revolución de la computación. La ordenador personal le permitió al usuario tener en su escritorio la capacidad del procesamiento de información y el acceso a bases de datos sin tener que depender de ninguna otra máquina (Raya-Raya, 2002).

Una vez desarrollados programas como hojas de cálculo y procesadores de texto, surge la necesidad de conectarse a otros sistemas de cómputo para lo que se diseñó un software de comunicación con el ordenador central, haciendo que la recepción y envió de información host-PC fuera más rápida y económica que host-terminal tonta.

Con las mejoras en el procesamiento y almacenamiento de información se redujeron cada vez más las diferencias entre las microcomputadoras, las PCs y las miniordenadors.

La necesidad de interconexión entre ordenadores y el hecho de poder compartir recursos e información dio como resultado la aparición de las primeras redes de área local LAN.

Conforme se extendió la implementación de LANs, la necesidad de comunicarlas se convirtió en el aspecto de gran importancia para las empresas, apareciendo las redes de área amplia WANs (Wide Area Network), obsérvese la Fig. 1.2.

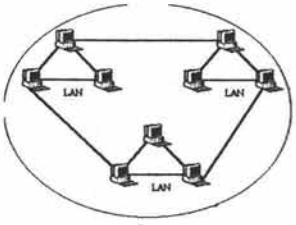


Fig. 1.2: Red de Área Amplia (WAN)

2.1 Definición de Red de Ordenadores.

Una red de ordenadores es un sistema de interconexión entre equipos que permite compartir recursos e información. Para ello es necesario contar, además de con los ordenadores correspondientes, con las tarjetas de red, los cables de conexión, los dispositivos periféricos y el software conveniente. (Raya, 2000).

Una red de cómputo es un grupo de ordenadores (y terminales, en general) interconectadas a través de uno o varios caminos o medios de transmisión. (Black, 1987)

El objetivo principal de las redes de cómputo es permitir la comunicación de datos entre los sistemas computacionales de una organización. Considerando las distancias existentes entre estos sistemas, las tecnologías para redes se clasifican de acuerdo al área de cobertura para la que fueron diseñadas (Raya-Raya, 2002).

2.2.- Clasificación de las Redes de Cómputo.

Redes de Área Local. (Local Area Network)

Una LAN provee una comunicación de alta velocidad (4-10 Mbps) y corta distancia (de algunos metros a pocos kilómetros) entre dispositivos inteligentes como ordenadores, que permite a los usuarios de intercambiar archivos o mensajes y compartir el uso de dispositivos como impresoras, ploters , servidores de archivos o de comunicaciones (Gs comunicaciones, 1998).

Redes de Área Metropolitana (Metropolitan Area Network)

Las MAN se encuentran entre las LAN y WAN, con una cobertura que comprende desde unos kilómetros hasta cientos de kilómetros, y una velocidad de transmisión de unos cuantos Kbps a Gbps, sirve como el backbone que interconecta varias LANs distribuidas o puede proveer acceso a la red metropolitana o a una red publica de cobertura amplia (Gs comunicaciones, 1998).

Redes de Área Amplia (Wide Area Network)

Las Primeras redes instaladas emplearon medios de transmisión públicos que permitieron a los sistemas de cómputo comunicarse a través de largas distancias. Las redes que comunican a un grupo amplio de usuarios separados geográficamente son identificadas como redes de área amplia (WAN).

Las WAN han evolucionado; actualmente los dispositivos conectados a estas redes pueden ser terminales inteligentes, ordenadores, estaciones de trabajo, miniordenadores e incluso LAN (Gs comunicaciones, 1998).

3.- Redes de Área Local (Local Area Network)

3.1.-Componentes de una Red Local.

Una red local esta formada, principalmente, por ordenadores con sus periféricos y por los elementos de conexión de los mismos.

1. Los ordenadores, pueden desarrollar dos funciones distintas: de servidores o de estaciones de trabajo.
2. Se entiende por elementos de conexión a los cables, tarjetas de red y otros equipos necesarios para conectar entre si los ordenadores. Dentro de los cables de conexión utilizados se encuentran:

- **Par trenzado sin apantallar (UTP)**
- **Par trenzado apantallado (STP)**
- **Cable coaxial**
- **Fibra óptica**

Además de los elementos indicados anteriormente se puede disponer también:

- **Gateway (Pasarela).** Es un sistema formado por hardware y software que permite las comunicaciones entre una red local y un gran computador (**mainframe**). Se suelen colocar en el servidor de comunicaciones.
- **Bridge (Puente).** Es un sistema formado por hardware y software que permite conectar dos redes locales entre sí. Se pueden colocar en el servidor de archivos o, mejor, en el servidor de comunicaciones.
- **Módem.** Es un periférico que permite conectar dos ordenadores a través de la red telefónica básica (Conmutada). La comunicación se puede establecer en ambos sentidos pero no simultáneamente (semiduplex) o en ambos sentidos simultáneamente (duplex). Es independiente el número de hilos de que consta el cableado de la forma de establecer la comunicación.

Tarjeta de interfase de red.

Para tener comunicación la red, el servidor y las estaciones de trabajo deben de contar con una tarjeta de interfase de red o NIC (Network Interface Card), que pueden encontrarse tanto en el interior como en el exterior del sistema de cómputo. Este adaptador será el apropiado para la topología que se desee usar.

El adaptador es una interfase entre la red y el ordenador, por lo tanto, debe de cumplir con los protocolos adecuados para evitar conflictos con los restos de los nodos o con otros dispositivos conectados al ordenador.

Los requerimientos para la operación de un adaptador como interfase de red son los siguientes:

1. Usan los protocolos adecuados según el tipo de red que se desee utilizar.
2. Tener el conector adecuado para adaptarse a la ranura de expansión o del puerto que se tenga disponible, en el caso de un ordenador portátil se utiliza generalmente el puerto paralelo.

3.2.- Arquitectura Cliente-Servidor.

Con el paso del tiempo, los usuarios de ordenadores fueron necesitando acceder a mayor cantidad de información y de forma más rápido, por lo que fue surgiendo la necesidad de un nuevo tipo de ordenador: el servidor.

Un servidor (del inglés SERVER) es un ordenador que permite compartir sus periféricos con otros ordenadores. Estos pueden ser varios tipos y entre ellos se encuentran los siguientes (Raya-Raya, 2002):

- **Servidor de archivos**. Mantiene los archivos en subdirectorios privados y compartidos para los usuarios de la red.
- **Servidor de impresión**. Tiene conectadas una o más impresoras que comparte con los demás usuarios.
- **Servidor de comunicaciones**. Permite enlazar diferentes redes locales o una red local con grandes ordenadores o minicomputadores.
- **Servidor de correo electrónico**. Proporciona servicios de correo electrónico para la red.
- **Servidor Web**. Proporciona un lugar para guardar y administrar los documentos HTML que pueden ser accesibles por los usuarios de la red a través de los navegadores.
- **Servidor FTP**. Se utiliza para guardar los archivos que pueden ser descargadores por los usuarios de la red.
- **Servidor Proxy**. Se utiliza para monitorizar el acceso entre las redes. Cambia la dirección IP de los paquetes de los usuarios para ocultar los datos de la red interna e internet y cuando recibe contestación externa, la devuelve al usuario que la ha solicitado. Su uso reduce la amenaza de piratas que visualiza el tráfico de la red para conseguir información sobre los ordenadores de la red interna.

Según el sistema operativo de red que se utilice y las necesidades de la empresa puede ocurrir que los distintos tipos de servidores residan en el mismo ordenador o se encuentren distribuidos entre aquellos, que forman parte de la red.

3.3.- Topología de una red.

Se denomina topología a la forma geométrica en que están distribuidas las estaciones de trabajo y los cables que las conectan.

Las estaciones de trabajo de una red se comunican entre sí mediante una conexión física, y el objeto de la topología es buscar la forma más económica y eficaz de conectarlas para, al mismo tiempo facilitar la fiabilidad del sistema, evitar los tiempos de espera en la transmisión de los datos, permitir un mejor control de la red y permitir de forma eficiente el aumento de las estaciones de trabajo (Raya-Raya, 2002).

3.3.1.- Topología de Bus.

En ella todas las estaciones comparten el mismo canal de comunicaciones, toda la información circula por ese canal y cada una de ellas recoge la información que le corresponde.

Esta configuración es fácil de instalar, la cantidad de cable a utilizar es mínima, tiene una gran flexibilidad a la hora de aumentar o disminuir el número de estaciones y el fallo de una estación no repercute en la red, aunque la ruptura de un cable la dejará totalmente inutilizada. Obsérvese Fig. 1.6

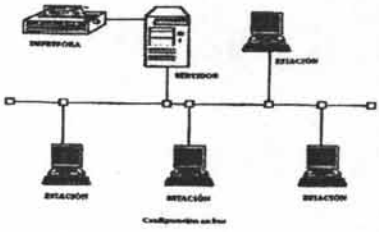


Fig. 1.6: Configuración en bus

Entre sus inconvenientes destacan:

- Es fácil de intervenir, por usuarios fuera de la red, sin perturbar el funcionamiento normal.
- La longitud no puede sobrepasar los 2.000 metros
- El control del flujo, ya que aunque varias estaciones intenten trasmitir a la vez, como hay un único bus, solo una de ellas podrá hacerlo, por lo que cuantas más estaciones tenga la red, más complicado será el control del flujo.

Es la configuración más extendida actualmente y está usada por la red ethernet.

3.3.2.- Topología de Anillo.

En ella todas las estaciones están conectadas entre sí formando un anillo, de forma que cada estación solo tiene contacto directo con otras dos. Obsérvese Fig. 1.7

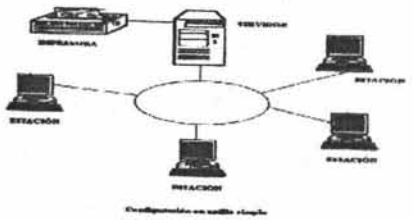


Fig. 1.7: Configuración en anillo

En las primeras redes de este tipo los datos se movían en una única dirección, de manera que toda la información tenía que pasar por todas las estaciones hasta llegar a la de destino donde se quedaba. Las redes más modernas disponen de dos canales y trasmiten en direcciones diferentes por cada uno de ellos.

Este tipo de redes permite aumentar o disminuir el número de estaciones sin dificultad; pero, a medida que aumenta el flujo de información, será menor la velocidad de respuesta de la red.

Un fallo en una estación puede dejar bloqueada la red, pero un fallo en un canal de comunicaciones la dejará bloqueada en su totalidad y, además, será bastante difícil localizar el fallo y repararlo de forma inmediata.

Su instalación es compleja y su uso esta extendido por el entorno industrial. Está usada por la red Token Ring de IBM.

3.3.3.- Topología en Estrella.

Está forma de configuración es una de las más antiguas. Todas las estaciones están conectadas directamente al servidor y todas las comunicaciones se han de hacer necesariamente a través de él. Obsérvese Fig. 1.8

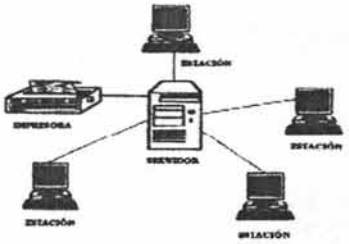


Fig. 1.8: Configuración en Estrella.

Permite incrementar y disminuir fácilmente el número de estaciones. Si se produce un fallo en una de ellas no repercutirá en el funcionamiento general de la red; pero, si se produce un fallo en el servidor, la red completa se vendrá abajo.

Tiene un tiempo de respuesta rápido en las comunicaciones con el servidor y lenta en las comunicaciones entre las distintas estaciones de trabajo.

No es muy conveniente para grandes instalaciones y su costo es caro debido a la gran cantidad de cableado y debido a la tecnología que se necesita para el servidor. Esta usada por la red Starlan de ATT o Sonet.

3.3.4.- Topología en Árbol Jerárquico.

Está formado por segmentos de red o subredes, las cuales dependen de un concentrador especifico (Gs comunicaciones, 1998).

Cada estación de trabajo compite por el acceso a la red con otras estaciones dentro de su segmento y después con otros segmentos. Obsérvese Fig. 1.9

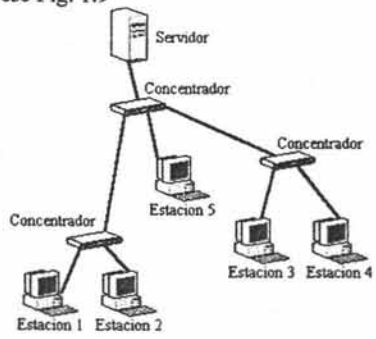


Fig. 1.9: Lan en Topología de Árbol Jerárquico.

3.4.- Señalización en LAN.

Dentro de una red de área local es muy importante considerar la forma en que los datos son codificados, así como el espectro de frecuencias utilizado en el medio de transmisión, el cual se define como señalización. Básicamente se estudian 2 tipos: baseband y broadband.

En la señalización broadband el medio se divide en frecuencias para formar dos o más canales para la transmisión. Esta señalización emplea la tecnología analógica en donde un Módem establece una frecuencia portadora sobre el medio de transmisión, para ser modificada por alguno de los métodos de modulación conocidos: Modulación por amplitud, Frecuencia o Fase. El método de modulación más usado en la señalización broadband en FSK (Frecuency Shift Keying), en el cual se generan dos frecuencias, una para representar un cero y otra para representar un uno binarios (Gs comunicaciones, 1998).

Con baseband solamente se trasmite una señal sobre el medio a un mismo tiempo. A diferencia de la señalización broadband , baseband utiliza codificación digital para la transmisión de datos , dos de los métodos comúnmente usados para la señalización baseband son el unipolar con retorno a cero y el Manchester.

El primer método es muy sencillo y se basa en la representación de un uno binario por el nivel de voltaje positivo, y un cero por la ausencia de voltaje. Tiene el inconveniente de saber dónde inicia y dónde termina un bit, para evitar esto sería necesario usar circuitos de sincronización lo cual resulta muy caro.

El otro método es el Manchester en el cual se produce una transición en la mitad de cada bit, siendo de +V a –V si el bit es un cero y al contrario si es un uno.

3.5.- Medios de Transmisión.

Se entiende por medio de transmisión a cualquier medio físico que pueda transportar información en forma de señales electromagnéticas. Los medios de transmisión permiten mandar la información de una estación de trabajo al servidor o a otra estación de trabajo y son una parte esencial de una red local (Tanenbaum, 1997).

3.5.1.- Cable de par sin Trenzar.

Este cable tiene un par de hilos sin trenzar y recubiertos de una capa aislante externa (también se le denomina como Categoría 1). Es de fácil instalación y tiene poca protección contra las interferencias externas. Es el cable telefónico tradicional. Se utiliza normalmente para transmitir voz pero no datos. El conector que se utiliza es el denominado RJ11.

3.5.1.1.- Cable de Par Trenzado.

Este cable tiene pares de hilos trenzados y recubiertos de una capa aislante externa. Es de fácil instalación y ofrece cierta protección contra las interferencias externas.

Puede estar apantallado **(STP)** con una resistencia de 120-150 ohmnios o sin apantallar **(UTP)** con una impedancia de 100 ohmnios. Los conectores que se utilizan son los denominados RJ45 y RJ11.

En función de sus características se clasifica en cuatro categorías:

- **Categoría 2:** Es un cable de cuatro pares trenzados. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 4 Mbps.
- **Categoría 3:** Es un cable de cuatro pares trenzados. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 10 Mbps (actualmente se puede utilizar en velocidad superiores) con longitudes de segmento inferiores a 100 metros y una longitud máxima de red de 500 metros.
- **Categoría** 4: Es un cable de cuatro pares trenzados. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 16 Mbps (actualmente está en desuso).
- **Categoría 5:** Es un cable de cobre de dos pares trenzados. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 100 Mbps (actualmente, al reducirse su coste es el que está siendo más utilizado).

3.5.2.- Cable Coaxial.

Es un cable formado por un hilo conductor central rodeado de un material aislante que, a su vez, está rodeado por una malla fina de hilos de cobre o aluminio o una malla fina cilíndrica. Todo el cable está rodeado por un aislamiento que le sirve de protección para reducir las emisiones eléctricas.

Se usa normalmente para datos y para los sistemas de antenas colectivas de televisión.

Trasmite una sola señal a una velocidad de transmisión alta.

En función de sus características se clasifica en dos categorías:

- **Cable coaxial grueso (10BASE5).** Tiene un grosor de 0,5 pulgadas, lleva un conector tipo N, alcanza una velocidad de transmisión de 10 Mbps y una longitud máxima de 500 metros de segmento de red. También se denomina Thick Ethernet.

- **Cable coaxial delgado (10BASE2).** Tiene un grosor de 0,25 pulgadas, lleva un conector tipo BNC, alcanza una velocidad de transmisión 10 Mbps y una longitud máxima de 200 metros de segmento de red. También se denomina Thin Ethernet.

3.5.2.1.- Cable Coaxial de Banda Ancha (10 BROAD36).

Está construido de forma muy similar al coaxial de banda base aunque puede tener mayores diámetros y con diversos grosores de aislamiento.

Su impedancia es de 75 ohmnios. Alcanza una velocidad de transmisión de 10 Mbps y una longitud máxima de 1.800 metros de segmento de red.

Puede transportar miles de canales de datos a baja velocidad.

Debido a su limitación en la velocidad de transmisión, está siendo sustituido por cableados de par trenzado de la categoría 5 y cables de fibra óptica.

3.5.3.- Cable de Fibra Óptica.

Está formado por un cable compuesto por fibras de vidrio (o de plástico). Cada filamento tiene un núcleo central de fibra de vidrio con un alto índice de refracción que esta rodeado de una capa de material similar pero con un índice de refracción menor. De esta manera aísla las fibras y evita que se produzcan interferencias entre filamentos contiguos a la vez que protege al núcleo.

Todo el conjunto está protegido por otras capas aislantes y absorbentes de luz.

Está formado por tres componentes:

- **Transmisor de energía óptica.** Lleva un modulador para transformar la señal electrónica entrante a la frecuencia aceptada por la fuente luminosa, la cual convierte la señal electrónica (electrones) en una señal óptica (fotones) que se emite a través de la fibra óptica.

- **Fibra óptica.** Su componente es el silicio y se conecta a la fuente luminosa y al detector de energía óptica. Dichas conexiones requieren una tecnología compleja.

- **Detector de energía óptica.** Normalmente es un fotodiodo que convierte la señal óptica recibida en electrones (es necesario también un amplificador para regenerar la señal).

Puede alcanzar velocidades muy altas a grandes distancias sin necesidad de usar repetidores (el producto de la distancia en kilómetros por la velocidad en Mbps no puede ser superior a 30. Por ejemplo, puede alcanzar una velocidad de 50 Mbps en una distancia de 600 metros o una velocidad 10 Mbps a 3.000 metros. Experimentalmente, se han llegado a conseguir velocidades de 200.000 Mbps).

3.6.- Métodos de Acceso.

Los métodos de acceso se refieren a las reglas que deben seguir las estaciones de trabajo para acceder al medio y transmitir su información en forma ordenada, evitando así colisiones con la consecuente pérdida de datos. Permiten también el direccionamiento de la comunicación entre estaciones (Gs comunicaciones, 1998).

3.6.1.-Acceso Múltiple con Sensibilidad de Portadora, con Detección de Colisión (CSMA/CD)

Es un método en el que la estación de trabajo censa el medio antes de hacer una transmisión; si el medio está ocupado espera un tiempo determinado antes de volver a sensar, cuando detecta que ninguna estación esta transmitiendo comienza su envió. Es posible que 2 estaciones transmitan al mismo tiempo por hacer la detección simultáneamente, por lo tanto habrá una colisión. Cuando ocurre esto, ambas máquinas vuelven a esperar un tiempo aleatorio para iniciar el proceso. Se usa principalmente en redes con topología bus (Raya-Raya, 2002). Obsérvese Fig. 1.10.

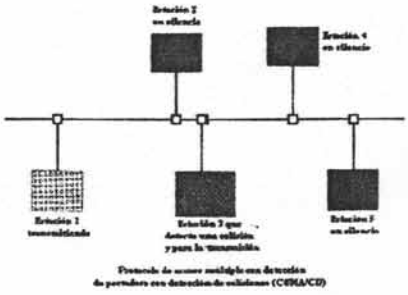


Fig. 1.10: CSMA/CD

3.6.2.-Acceso Múltiple con Sensibilidad de Portadora Evitando Colisiones (CSMA/CA)

En este tipo de método cuando una estación va a enviar un bloque de datos comprueba que la línea está libre y cuando verifica que lo está, indica que tiene intención de transmitir.

Si hay varias que se encuentran esperando, la transmisión se realiza por turno. En este turno se tiene en cuenta la prioridad de la estación y el orden en que se ha indicado que se desea transmitir, por tanto, primero transmitirá la que lo haya solicitado primero entre la que tienen la máxima prioridad y no la que lo haya solicitado primero si tiene una prioridad baja (Raya-Raya, 2002). Obsérvese Fig. 1.11

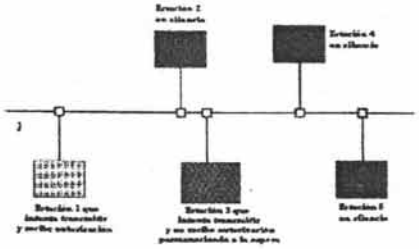


Fig. 1.11: CSMA/CA

3.6.3.-Token Passing

Este método hace circular continuamente un grupo de bits (testigo) por la red. Este testigo está formado por una cabecera, un campo de datos y un campo final (Raya-Raya, 2002).

CABECERA	CAMPO DE DATOS	CAMPO FINAL

Cuando una estación quiere transmitir ha de esperar a que llegue hasta ella el testigo vacío. En ese momento le añade unos datos, quedando el testigo formado por: la cabecera, la dirección destino, la dirección origen, el camino que ha de seguir para llegar a su destino y el bloque de datos, y lo envía a su destino.

CABECERA	DIRECCIÓN DESTINO	DIRECCION ORIGEN	CAMINO A SEGUIR	BLOQUE DE DATOS

Si la estación no desea transmitir, pasa el testigo vacío a la siguiente estación y así sucesivamente. Obsérvese Fig. 1.12

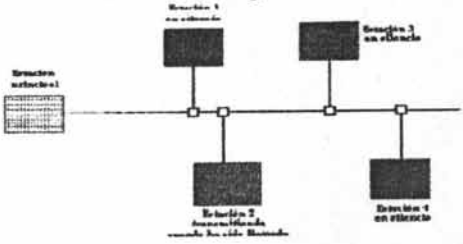


FIG. 1.12: Protocolo De Llamada Selectiva (Polling)

El testigo ocupado llega a la estación destino que recoge el bloque de datos, pone una marca en el testigo indicando si lo acepta o lo rechaza por venir con errores, y lo devuelve a la estación que lo ha enviado.

Cuando llega a la estación que lo envió, ésta lo reenvía si llega con la marca de rechazado, envía el siguiente bloque de datos o vacía el testigo para que pase a la estación siguiente.

Este protocolo cuenta con bastantes ventajas:

- Elimina por completo el riesgo de colisiones.
- Puede emplear mensajes muy largos.
- El volumen de carga es bastante alto.
- El tamaño de la red puede ser grande.

3.7.- Estándares en LAN.

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) emite los estándares que definen las características, topología, medios de transmisión de los modelos más utilizados en las LANs dentro de su proyecto 802.

Se analizan los estándares más difundidos en México, el 802.3 (Ethernet), el 802.5 (Token Ring) y uno emergente como el 801.12 (1OOVGAnyLAN) (Gs comunicaciones, 1998).

3.7.1.- Ethernet.

Como características más importantes destaca la utilización de CSMA/CD como método de acceso. Soporta velocidades de transmisión de datos de 10 Mbps. Aunque emplea una topología lógica de bus, puede utilizar topología física en bus o estrella. El medio de transmisión más empleado en las redes Ethernet es el cable coaxial grueso de 50 ohms con señalización baseband, sin embargo, existen especificaciones para otros medios de transmisión, las cuales se mencionan a continuación.

3.7.1.1.- 10Base5.

Emplea topología física de bus con cable coaxial grueso, las estaciones se conectan al medio a través de transceptores (transceiver), la distancia máxima cubierta del segmento es de 500 metros, aunque se puede añadir repetidores para aumentar el alcance.

3.7.1.2.- l0Base2.

Utiliza también topología de bus pero con cable coaxial delgado, más flexible y ligero (RG-58) y conectores BNC, soporta también velocidades de transmisión de datos de 10 Mbps señalización baseban.

3.7.1.3.- l0Broad36.

Emplea velocidades de 10 Mbps sobre una topología de bus con cable coaxial de 75 Ohms, pero a diferencia de las anteriores utiliza señalización broadband.

3.7.1.4.- 1 Base5.

Emplea señalización baseband y velocidades de transmisión de 1 Mbps a diferencia de los estándares anteriores utiliza una topología en estrella con cable de par trenzado (UTP).

3.7.1.5.- 10BaseT.

Emplea también topología en estrella con cable de par trenzado (UTP) con señalización baseband y a 10 Mbps. Es actualmente una de las topologías más utilizadas en el mercado.

3.7.1.6.- 10BaseF.

Es una de sus características muy similar a 10BaseT aunque utiliza como medio la fibra óptica lo que le da mayor inmunidad a la interferencia y mayor distancia de cobertura.

La siguiente tabla resume las características técnicas en los diferentes apartados del estándar IEEE 802.3.

Características	ETHERNET	10BASE5	10BASE2	10BROAD36	1BASE5	10BASET	10BASEF
Medio	COAX 50 GRUESO	COAX 50 GRUESO	COAX 50 DELGADO	COAX 75	UTP	UTP	FIBRA OPTICA
Señalización	BASEBAND	BASEBAND	BASEBAND	BROADBAND	BASEBAND	BASEBAND	BASEBAND
Topología	BUS	BUS	BUS	BUS	ESTRELLA	ESTRELLA	ESTRELLA
Distancia del Segmento	500 MTS.	500 MTS.	185 MTS.	1800 MTS.	250 MTS.	100 MTS.	<4 KMS>
Velocidad. de Transferencia	10 Mbps:	10 Mbps:	10 Mbps:	10 Mbps:	1 Mbps:	10 Mbps:	10 Mbps:

3.7.2.-Fast Ethernet.

Esta moderna arquitectura de red está basada en la tecnología Ethernet, pero cuenta con las siguientes variaciones que le permiten transmitir a una velocidad de 100 Mbps:

- Está construida con concentradores distribuidos que utilizan líneas dedicadas para cada ordenador.
- Los cables utilizados son: 1OOBaseTX, lOOBaseFX y 1OOBaseT4. la diferencia entre estos tres tipos de cables está en que el cable lOOBaseTX usa dos de los cuatro pares de hilos (igual que un cable UTP normal), que deben ser categoría 5 (por su mayor calidad), el cable 1OOBaseFX es el equivalente en fibra óptica del cable 100BaseTX y el cable 1OOBaseT4 utiliza los cuatro pares de hilos, que pueden ser categoría 3 ó 5.
- Necesita tarjetas de red específicas para la velocidad de transmisión de 100 Mbps.

3.7.3.- Token Ring.

Esta arquitectura de red fue creada por IBM en octubre de 1985 aunque anteriormente había comercializado dos tipos de redes locales: una red de banda base a 375 Kbps y para un máximo de 64 ordenadores, y una red de banda ancha a 2 Mbps para un máximo de 72 ordenadores.

Emplea una topología de anillo con método de paso de testigo y se puede utilizar cable de par trenzado, cable coaxial y fibra óptica.

Los datos se transmiten a una velocidad de 4 Mbps por segundo, pudiéndose conectar hasta un máximo de 8 ordenadores y a una distancia máxima de 350 metros en cada unidad de acceso multiestación (MAU) si se utiliza con cable coaxial (si se utiliza con fibra óptica puede llegar hasta una velocidad de 16 Mbps).

No obstante, como se pueden conectar hasta 12 unidades de acceso multiestación (MAU), el número de ordenadores conectados, y la distancia máxima, pueden aumentar considerablemente.

3.7.4.- 100VGAnyLAN.

Definida por el estándar IEEE 802.12 para soportar tanto a topología Ethernet y Token Ring también es una tecnología para alta velocidad (1OO Mbps). Introduce un nuevo concepto llamado Método de Acceso Prioritario por Demanda (DPAM).

3.7.5.- FDDI.

Es una tecnología más de MAN que de LAN, utiliza topología lógica de anillo y método de acceso Token Passing pero permite transmisión de datos a 100 Mbps y su medio de transmisión es la fibra óptica, por lo que accede a mayores distancias de operación. No está estandarizado por la IEEE si no por el Instituto Nacional de Estándares Americanos (ANSI) como X3T9.5.

Se utiliza principalmente para implantar un backbone de alta velocidad entre redes LAN en un ambiente de Campus.

4. TCP / IP Antecedentes.

TCP/IP no es sólo un protocolo, sino que comprende todo un conjunto muy completo de diversos protocolos que prestan diversos servicios. Las siglas TCP/IP son por el nombre de 2 protocolos que realizan todas las funciones de inicio del protocolo TCP/IP (Transmision Control Protocol y el Internet Protocol).

TCP/IP es, uno de los protocolos de comunicaciones más viejos en los estándares de redes internas. TCP/IP fue desarrollado por el Departamento de Proyectos Avanzados de Investigación de la Defensa de Estados Unidos (DARPA Defense's Advanced Research Project Agency') con el propósito de resolver los problemas de la heterogeneidad de las tecnologías de redes de cómputo. El desarrollo de este inició en 1969. El protocolo que se dio dentro de TCP/IP comenzó con el usado para construir el primer switcheo de paquetes en el mundo, ARPANET. Este es el que conduce el desarrollo del World wide Internet, hoy una de las redes heterogéneas más grandes del mundo (Gs comunicaciones, 1998).

El protocolo TCP/IP se emplea en Internet y algunas veces en redes más pequeñas, especialmente en las que conectan sistemas de computación que corren el sistema operativo UNIX®.

Es posible que el protocolo que ha sido desarrollado por el Organismo Internacional de Estándares (ISO) para el Modelo 0SI eventualmente desplazó al protocolo TCP/IP en varios ambientes. El protocolo TCP/IP será extensamente usado por varias organizaciones dentro de los siguientes 100 años. TCP/IP es ahora una forma extremadamente importante de tecnología para redes.

4.1 Arquitectura TCP/IP.

Parte del poder del protocolo TCP/IP se determina por la habilidad para permitir que diferentes tipos de dispositivos y de proveedores interoperen con cualquier otro, soportando una gran variedad de dispositivos; pero siempre se pueden presentar problemas substanciales por compatibilidad. El hardware y software de estos dispositivos necesitan ser compatibles dentro del orden, para lo cual las arquitecturas de redes han sido desarrolladas en la Construcción de redes complejas, usando una gran variedad de equipo.

En redes de ordenadores modernos las funciones de transmisión de datos se realizan por un complejo hardware y software en varios dispositivos conectados a la red. Las funciones del software empleadas en los dispositivos en red son divididos dentro del nivel independiente de funciones.

La comitiva del protocolo TCP/IP realiza una arquitectura por niveles, teniendo los 4 niveles de software obsérvese Fig. 1.3 (Gs comunicaciones, 1998)

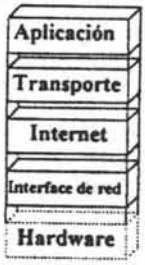


Fig. 1.3: Niveles de arquitectura TCP/IP.

Los 4 niveles de software TCP/IP son construidos sobre el entendimiento del hardware de la red que opera en el nivel inferior al software TCP/IP. El software de comunicación TCP/IP es dividido dentro de niveles.

TCP/IP hace posible desarrollar una aplicación en un ambiente dentro de Internet para facilitar la comunicación con una aplicación corriendo en otro ambiente como si ambos fueran conectados directamente. La comunicación parece simple hacia éstos, Internet puede ser un complejo integrado de muchas redes físicas y muchos ruteadores entre los dos ambientes realizando los programas de comunicación.

Cada uno de los ambientes de comunicación maneja un software que implementa los 4 niveles de la arquitectura TCP/IP para tomar las funciones de comunicación (Gs comunicaciones, 1998).

El protocolo es flexible y permite la transmisión de tramas sin errores entre diferentes sistemas.

Debido a que es un protocolo de transferencia de información, puede enviar grandes volúmenes de información a través de redes no confiables, garantizando que esta será recibida sin errores al momento de alcanzar su destino final (Gs comunicaciones, 1998).

Cuando se emplea TCP/IP, la información viaja en segmentos creados por TCP entre emisor y receptor para acceder a alguna aplicación. Los segmentos creados por TCP son encapsulados por IP, y esta encapsulación es llamada datagrama IP. El datagrama IP permite que los segmentos TCP que fuerón hechos por alguna aplicación, sean transmitidos o ruteados en la Red de Área Local o en la Red de Área Extendida.

4.2 Arquitectura de Red.

Una arquitectura de red es una serie de roles que determinan el diseño y operación de los componentes del hardware y software empleados para crear redes de ordenadores. La arquitectura de red define la serie de protocolos de comunicación que determina cómo se realiza la comunicación.

Un software del sistema de comunicación en una red de ordenadores, generalmente está conformada por una arquitectura de red particular, semejante como TCP/IP y usa una serie individual de protocolo para comunicación. A continuación, se hace mención de algunas arquitecturas de red diferentes y sistemas de comunicación que están en uso en redes de ordenadores:

- Xerox Networking Systems.
- Novell Netware.
- DECnet Phase IV.
- DECnet /0SI
- Apple Talk.
- NetBios.

Las redes TCP/IP permiten que la información sea enviada de un sistema a otro, sin que estos tengan que ser de la misma marca o fabricante. Por ejemplo, una estación con Windows® NT de Microsoft puede intercambiar información con un ordenador con Pathworks de Digital.

Siempre y cuando utilicen el mismo protocolo de comunicaciones, en este caso es TCP/IP (Gs comunicaciones, 1998).

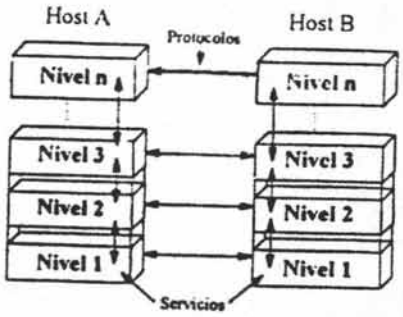


Fig. 1.4: Protocolos de comunicación y niveles de servicio.

La figura 1.4 muestra un modelo de una arquitectura de red por niveles, esto es, una interfase entre cada par de niveles y cada nivel funcional provee una serie de servicios para el nivel lateral a el. Los servicios definidos por las interfases de nivel son representados por las flechas verticales

4.3 Protocolo Orientado a Conexión.

Un proceso de implementación de un protocolo orientado a conexión proporciona un servicio similar al que proporciona un servicio telefónico. Este consiste en 3 fases distintas:

- Establecer conexión (dial a call)
- Transferencia de datos (talk over the connection)
- Deshabilitar la conexión (hang up the phone).

Una de las partes mencionadas puede ser establecida antes de que se realice la comunicación. Las 3 partes incluyen las 2 formas de comunicación asociada, y en ellas mismas el servicio de transferencia de datos.

Un intercambio de mensajes que implementa un procedimiento llamado handshake, generalmente toma el lugar en el protocolo del proceso de desarrollo de cada uno de los ordenadores dentro de la implementación en asociación, llamada una conexión entre ellos.

Con un protocolo orientado a conexión, algunas veces la transferencia de datos comprende un par de comunicaciones asociadas con un protocolo orientado a conexión, ya que el receptor sólo lo necesita para ser completamente identificado el tiempo que tarda en ser establecida la conexión. Alguna información es requerida cuando transfieren datos, esto es, para identificar la conexión con la cual el dato es asociado.

Un protocolo orientado a conexión es frecuentemente descrito como un servicio fiable y secuencial en la transferencia de datos. La conexión puede ser deshabilitada en cualquier tiempo por otra de las partes involucradas en la comunicación o por el protocolo mismo (Gs comunicaciones, 1998).

4.4 Protocolo Orientado a no Conexión.

Con un protocolo orientado a no conexión, la comunicación toma el lugar de una fase simple ya que no necesita establecer una conexión lógica entre el proceso de transmisión y recepción. El proceso del usuario toma un mensaje para implementar el proceso del protocolo e identificar el destino del proceso en el mensaje enviado.

Un protocolo orientado a no conexión está provisto de un servicio llamado datagrama. Un protocolo orientado a no conexión no contiene un servicio confiable (Gs comunicaciones, 1998).

4.5 Enrutamiento en TCP/IP.

A través del protocolo TCP/IP se encuentra el enrutamiento, proceso por el cual 2 estaciones que se comunican se encuentran y usan la mejor trayectoria de una red TCP/IP, sin importar complejidad.

El proceso tiene algunos componentes importantes como determinar las trayectorias disponibles, seleccionar la mejor trayectoria para un propósito especifico, alcanzar otros sistemas, además de modificar los formatos de los datagramas lo que permite ajustarse a una nueva tecnología (Gs comunicaciones, 1998).

Principios de enrutamiento

Existen 3 procesos principales que se ejecutan en un sistema de enrutamiento:

- El nodo final necesita saber cómo y cuando comunicarse con un ruteador.
- El ruteador necesita saber cuando determinar una trayectoria adecuada a una red remota.
- El ruteador en la red destino necesita saber cómo conectarse al nodo final.

4.5.1 Ventajas de Enrutamiento.

- Elección de la mejor ruta.
- Ajusta tecnologías de diferente nivel de enlace.
- Flexibilidad y control.
- Reporte de errores.

4.5.2 Tablas de Enrutamiento.

Todo ruteador tiene una tabla con los números de red y subred que conoce. La tabla registra cuáles conexiones del ruteador pueden ser usadas para alcanzar una red en particular, así como algunos indicativos del desempeño o costo de un enlace para alcanzar una red determinada.

4.5.3 Métrica del Enrutamiento.

La función básica de un protocolo de enrutamiento es variar información de un ruteador a otro acerca de los números de red y subred que son conocidos por éste, combinados con algunas mediciones de desempeño como son distancia, retraso del tráfico, promedio de errores y costo.

4.5.4 Enrutamiento Internet IP.

Los diseñadores de Internet definieron 5 esquemas de enrutamiento: Fig. 1.5

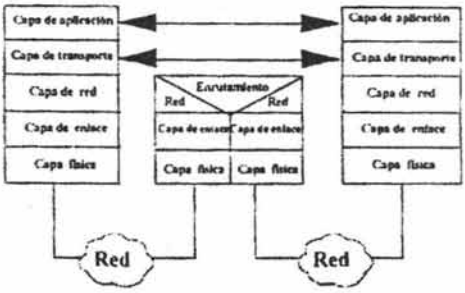


Fig. 1.5: Enrutamiento con IP.

- Enrutamiento directo: usado cuando el nodo destino está en la misma red con nodo o ruteador fuente.
- Enrutamiento indirecto: el destino no es local, así que es necesario hacer una búsqueda en una tabla de enrutamiento para determinar cuál ruteador deberá enviar el mensaje.
- Enrutamiento default: cuando una tabla de enrutamiento está incompleta, el datagrama es pasado a un ruteador default que se encargara de resolver el problema.
- Si no hay ruteador default conocido, el datagrama es descartado.
- Nodo ruteador: el nodo que genera el datagrama especifica la ruta.

4.6 Direccionamiento TCP/IP.

Cuando dos ordenadores se comunican entre ellos, uno recibe los datos que le envía la otra. Sin el protocolo TCP/IP la máquina que recibe no sabría que hacer con los datos que le llegan.

El protocolo IP se encarga de direccionar la información entre los nodos de la red. IP proporciona los mecanismos para mandar los datos, pero no garantiza que lleguen de una manera correcta. Esta segunda tarea es la que efectúa TCP.

IP forma paquetes de datos que envía a través de la red. Uno de estos paquetes puede llegar a tener hasta 65,535 bytes de 8 bits.

Para enviar los paquetes a una máquina en particular, a cada una de los ordenadores conectados a Internet se les asigna una dirección IP. Es un conjunto de 4 números separados por un punto. Esto es así por que cada uno de los 4 números que forman la dirección es un byte de 8 bits.

La dirección total tiene entonces 32 bits. Lo que permite direccionar alrededor de 43,000 millones de ordenadores. A manera de ejemplo se menciona que la ordenador de la UNAM. Que se llama Sor Juana, tiene como dirección IP el 132.248. 190.164

El último número es indicativo del ordenador (Sor Juana). El 132 de la red (la UNAM), y los dos últimos intermedios de la red (localización dentro de la UNAM). Cóndor, el servidor de gopher de la UNAM tiene como dirección IP 132.248.10.3, TCP hace dos cosas más que no hace IP: garantiza la entrega y el orden correcto de los paquetes.

TCP lleva á cabo el registro del número de puerto. Esto es importante sobre todo para la presentación de servicios de red. Es decir, cuando se requiere montar un servidor de gopher o un sitio de FTP.

TCP/IP es el responsable de que exista correo electrónico entre máquinas de distintas arquitecturas, con distintos software, localizados en lugares geográficamente muy apartados del planeta.

Por supuesto, también de que se establezcan sesiones remotas o Trasferencias de Archivos (FTP) (Gs comunicaciones, 1998).

5. Redes de Área Metropolitana.

Una red de área metropolitana es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado de cobre a velocidades que van desde los 2 Mbits/s hasta 155 Mbits/s (CSI, 2004).

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas de una cobertura superior que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

5.1.-Aplicación de Redes de Área Metropolitana.

Las redes de área metropolitana tienen muchas aplicaciones, las principales son:

- Interconexión de redes de área local (RAL)
- Interconexión de centralitas telefónicas digitales (PBX y PABX).
- Interconexión ordenador a ordenador.
- Transmisión de vídeo e imágenes.
- Transmisión CAD/CAM.
- Pasarelas para redes de área extensa (WAN).

Una red de área metropolitana puede ser pública o privada. Un ejemplo de MAN privada sería un gran departamento o administración con edificios distribuidos por la ciudad, transportando todo el tráfico de voz y datos entre edificios por medio de su propia MAN y encaminando la información externa por medio de los operadores públicos. Los datos podrían ser transportados entre los diferentes edificios, bien en forma de paquetes o sobre canales de ancho de banda fijos. Aplicaciones de vídeo pueden enlazar los edificios para reuniones, simulaciones o colaboración de proyectos.

Un ejemplo de MAN pública es la infraestructura que un operador de telecomunicaciones instala en una ciudad con el fin de ofrecer servicios de banda ancha a sus clientes localizados en esta área geográfica (CSI, 2004).

Las razones por las cuales se hace necesaria la instalación de una red de área metropolitana a nivel corporativo o el acceso a una red pública de las mismas características se resumen a continuación:

- **Ancho de banda.**

El elevado ancho de banda requerido por grandes ordenadores y aplicaciones compartidas en red es la principal razón para usar redes de área metropolitana en lugar de redes de área local.

- **Nodos de red.**

Las redes de área metropolitana permiten superar los 500 nodos de acceso a la red, por lo que se hace muy eficaz para entornos públicos y privados con un gran número de puestos de trabajo.

- **Extensión de red.**

Las redes de área metropolitana permiten alcanzar un diámetro entorno a los 50 kms, dependiendo el alcance entre nodos de red del tipo de cable utilizado, así como de la tecnología empleada. Este diámetro se considera suficiente para abarcar un área metropolitana.

- **Distancia entre nodos.**

Las redes de área metropolitana permiten distancias entre nodos de acceso de varios kilómetros, dependiendo del tipo de cable.

Estas distancias se consideran suficientes para conectar diferentes edificios en un área metropolitana o campus privado.

- **Tráfico en tiempo real.**

Las redes de área metropolitana garantizan unos tiempos de acceso a la red mínimos, lo cual permite la inclusión de servicios síncronos necesarios para aplicaciones en tiempo real, donde es importante que ciertos mensajes atraviesen la red sin retraso incluso cuando la carga de red es elevada.

- **Integración voz/datos/vídeo.**

Adicionalmente a los tiempos mínimos de acceso, los servicios síncronos requieren una reserva de ancho de banda; tal es el caso del tráfico de voz y vídeo. Por este motivo las redes de área metropolitana son redes óptimas para entornos de tráfico multimedia, si bien no todas las redes metropolitanas soportan tráficos isócronos (transmisión de información a intervalos constantes).

- **Alta disponibilidad.**

Disponibilidad referida al porcentaje de tiempo en el cual la red trabaja sin fallos. Las redes de área metropolitana tienen mecanismos automáticos de recuperación frente a fallos, lo cual permite a la red recuperar la operación normal después de uno. Cualquier fallo en un nodo de acceso o cable es detectado rápidamente y aislado. Las redes MAN son apropiadas para entornos como control de tráfico aéreo, aprovisionamiento de almacenes, bancos y otras aplicaciones comerciales donde la indisponibilidad de la red tiene graves consecuencias.

- **Alta fiabilidad.**

Fiabilidad referida a la tasa de error de la red mientras se encuentra en operación. Se entiende por tasa de error el número de bits erróneos que se transmiten por la red. En general la tasa de error para fibra óptica es menor que la del cable de cobre a igualdad de longitud. La tasa de error no detectada por los mecanismos de detección de errores es del orden de 10-20.

Esta característica permite a la redes de área metropolitana trabajar en entornos donde los errores pueden resultar desastrosos como es el caso del control de tráfico aéreo.

- **Alta seguridad.**

La fibra óptica ofrece un medio seguro porque no es posible leer o cambiar la señal óptica sin interrumpir físicamente el enlace. La rotura de un cable y la inserción de mecanismos ajenos a la red implican una caída del enlace de forma temporal.

- **Inmunidad al ruido.**

En lugares críticos donde la red sufre interferencias electromagnéticas considerables la fibra óptica ofrece un medio de comunicación libre de ruidos.

El ámbito de aplicación más importante de las redes de área metropolitana es la interconexión de redes de área local sobre un área urbana, pero otros usos han sido identificados, como la interconexión de redes de área local sobre un complejo privado de múltiples edificios y redes de alta velocidad que eliminan las barreras tecnológicas.

5.4.- Componentes de Área Metropolitana.

Los componentes de una red de área metropolitana son:

Puestos de trabajo.

Son los sistemas desde los cuales el usuario demanda las aplicaciones y servicios proporcionados por la red.

Dentro de los puestos de trabajo se incluyen:

- Estaciones de trabajo.
- Ordenadores centrales.
- Ordenadores de escritorio.

Nodos de red.

Son dispositivos encargados de proporcionar servicio a los puestos de trabajo que forman parte de la red. Sus principales funciones son:

- Almacenamiento temporal de información a transmitir hasta que el canal de transmisión se libere.
- Filtrado de la información circulante por la red, aceptando sólo la propia.
- Conversión de la información de la red, en serie, a información del puesto de trabajo, octetos.
- Obtención de los derechos de acceso al medio de transmisión.

Sistema de Cableado.

Está constituido por el cable utilizado para conectar entre sí los nodos de red y los puestos de trabajo.

Protocolos de Comunicación.

Son las reglas y procedimientos utilizados en una red para establecer la comunicación entre nodos. En los protocolos se definen distintos niveles de comunicación.

Así, las redes de área metropolitana soportan el nivel 1 y parte del nivel 2, dando servicio a los protocolos de nivel superior que siguen la jerarquía OSI para sistemas abiertos (CSI, 2004)..

Aplicaciones.

Como Sistemas de Tratamiento de Mensajes (MHS), Gestión, Acceso y Transferencia de Ficheros (FTAM) y EDI puede ser posibles aplicaciones de la red.

4.5.-Servicios de Una Red de Área Metropolitana.

La clasificación de los posibles servicios que ofrecen las redes de área metropolitana:

- **Servicios "No orientados a Conexión".**

Permite el transporte de datos sin establecer conexión previa.

- **Servicios "Orientados a Conexión".**

Es necesario establecer una conexión previa al transporte de los datos del usuario.

- **Servicios Isócronos.**

Se utilizan cuando se tienen unos requisitos estrictos de ancho de banda como son los casos de transmisión de determinados servicios de audio y vídeo. Determinadas aplicaciones requieren la transferencia constante de información a intervalos definidos (isócronos). En este caso no todas las tecnologías soportan dichas aplicaciones, tal es el caso de FDDI, si bien exige una nueva Norma FDDI-II que soporta el tráfico isócrono.

5.6.-Gestión de Redes.

La gestión se está convirtiendo en un elemento esencial para asegurar la disponibilidad tanto física como lógica de las redes metropolitanas. La complejidad de las actuales redes impone la necesidad de utilizar sistemas de gestión capaces de controlar, administrar y monitorizar redes locales, metropolitanas y extensas, a la vez que dispositivos de interconexión, servidores y clientes (Raya-Raya, 2002).

En la actualidad, existen diferentes niveles en la concepción de las herramientas de ayuda a la gestión; cada uno de estos niveles permite acometer una problemática particular del entorno de redes y en general no están integrados en un único sistema capaz de proporcionar una visión completa de los subsistemas que conforman las redes.

La tendencia en la evolución de la tecnología de gestión de redes se encamina hacia el desarrollo de productos integrados capaces de gestionar conjuntamente subsistemas de voz, datos e imagen en sus diferentes niveles: medio físico de transmisión, redes, aplicaciones, etcétera.

6.- Redes de Área Amplia (WAN).

Una WAN se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones), estas máquinas se llaman ordenadores. Los ordenadores están conectados por una subred de comunicación. El trabajo de una subred es conducir mensajes de un ordenador a otro. La separación entre los aspectos exclusivamente de comunicación de la red (la subred) y los aspectos de aplicación (ordenadores), simplifica enormemente el diseño total de la red (Guenul, 1997).

En muchas redes de área amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (también llamadas circuitos o canales) mueven los bits de una máquina a otra.

Los elementos de conmutación son ordenadores especializados que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para enviarlos. Como término genérico para los ordenadores de conmutación, se les llamara enrutadores.

6.1.-Constitución de una Red de Área Amplia.

La red consiste en ECD (ordenadores de conmutación) interconectados por canales alquilados de alta velocidad (por ejemplo, líneas de 56 kbit / s).

Cada ECD utiliza un protocolo responsable de encaminar correctamente los datos y de proporcionar soporte a los ordenadores y terminales de los usuarios finales conectados a los mismos. La función de soporte ETD (Terminales / ordenadores de usuario).

La función soporte del ETD se denomina a veces PAD (Packet Assembly / Disasembly – ensamblador / desensamblador de paquetes). Para los ETD, el ECD es un dispositivo que los aísla de la red. El centro de control de red (CCR) es el responsable de la eficiencia y fiabilidad de las operaciones de la red (Sosa,1999).

6.2.- Características de una Red de Área Amplia.

Los canales suelen proporcionarlos las compañías telefónicas, con un determinado costo mensual si las líneas son alquiladas, y un costos proporcional a la utilización si son líneas normales conmutadas.

- Los enlaces son relativamente lentos.
- Las conexiones de los ETD con los ECD son generalmente más lentas.
- LOS ETD y los ECD están separados por distancias que varían desde algunos kilómetros hasta cientos de kilómetros.
- Las líneas son relativamente propensas a errores (si se utilizan circuitos telefónicos convencionales).
- Las redes de área local (LAN) son significativamente diferentes de las redes de cobertura amplia. El sector de las LAN es uno de los de más rápido crecimiento en la industria de las comunicaciones. Las redes de área local poseen las siguientes características.
- Generalmente, los canales son propiedad del usuario o empresa.
- Los enlaces son líneas (desde 1 Mbit / s hasta 400 Mbit / s . Los ETDs se conectan a la red vía canales de baja velocidad (desde 600 bit / s hasta 56 Kbit / s).
- Los ETD están cercanos entre sí, generalmente en un mismo edificio.
- Puede utilizarse un ECD para conmutar entre diferentes configuraciones, pero no tan frecuentemente como en las WAN.
- Las líneas son de mejor calidad que los canales en las WAN.
- Debido a las diferencias entre las redes de área local y las redes de cobertura amplia, sus topologías pueden tomar formas muy diferentes.

La estructura de las WAN tiende a ser más irregular, debido a la necesidad de conectar múltiples terminales, ordenadores y centros de conmutación. Como los canales están alquilados mensualmente, las empresas y organizaciones que los utilizan tienden a mantenerlos lo más ocupados posible. Para ello, a menudo los canales "serpentean" por una determinada zona geográfica para conectarse a los ETD allí donde estén. Debido a eso la topología de las WAN suele ser más irregular.

Por el contrario, el propietario de una LAN no tiene que preocuparse de utilizar al máximo los canales, ya que son baratos en comparación con su capacidad de transmisión ("los cuellos de botella" en las LAN suelen estar en el Software). Por tanto, no es tan crítica la necesidad de esquemas muy eficientes de multiplexado y multidistribución. Además, como las redes de área local que residen en un mismo edificio, la topología tiende a ser más ordenada y estructurada, con configuraciones en forma de bus, anillo o estrella.

6.3.-Componentes Físicos.

Línea de Comunicación: Medios físicos para conectar una posición con otra con el propósito de transmitir y recibir datos.

Hilos de Transmisión: En comunicaciones telefónicas se utiliza con frecuencia el término "pares" para describir el circuito que compone un canal. Uno de los hilos del par sirve para transmitir o recibir los datos, y el otro es la línea de retorno eléctrico.

5.4.- Clasificación de Líneas de Conmutación.

Líneas Conmutadas: Líneas que requieren de marcar un código para establecer comunicación con el otro extremo de la conexión.

Líneas Dedicadas: Líneas de comunicación que mantienen una permanente conexión entre dos o más puntos. Estas pueden ser de dos o cuatro hilos.

Líneas Punto a Punto: Enlazan dos DTE

Líneas Multipunto: Enlazan tres o más DTE

Líneas Digitales: En este tipo de línea, los bits son transmitidos en forma de señales digitales. Cada bit se representa por una variación de voltaje y esta se realiza mediante codificación digital en la cual los códigos más empleados son:

NRZ (Non Return to Zero) Unipolar.

La forma de onda binaria que utilizan normalmente los ordenadores se llama Unipolar, es decir, que el voltaje que representa los bits varía entre 0 voltios y +5 voltios. Se denomina NRZ porque el voltaje no vuelve a cero entre bits consecutivos de valor uno. Este tipo de código es inadecuado en largas distancias debido a la presencia de niveles residuales de corriente continua y a la posible ausencia de suficientes números de transiciones de señal para permitir una recuperación fiable de una señal de temporización (Guenul, 1997).

Código NRZ Polar: Este código desplaza el nivel de referencia de la señal al punto medio de la amplitud de la señal. De este modo, se reduce a la mitad la potencia requerida para transmitir la señal en comparación con el Unipolar.

Transmisión Bipolar o AMI (Alternate Marks Inverted): Es uno de los códigos más empleados en la transmisión digital a través de redes WAN. Este formato no tiene componente de corriente continua residual y su potencia a frecuencia cero es nula.

Se verifican estos requisitos transmitiendo pulsos con un ciclo de trabajo del 50% e invirtiendo alternativamente la polaridad de los bits "1" que se transmiten.

Dos valores positivos sin alternancia entre ellos serán interpretados como un error en la línea. Los "0" son espacios sin presencia de voltaje.El formato Bipolar es en realidad una señal de tres estados (+V, 0, -V).

6.5.- Tipos de Redes de Área Amplia.

Conmutadas por Circuitos: Redes en las cuales, para establecer comunicación se debe efectuar una llamada y cuando se establece la conexión, los usuarios disponen de un enlace directo a través de los distintos segmentos de la red.

Conmutadas por Mensaje: En este tipo de redes el conmutador suele ser un ordenador que se encarga de aceptar tráfico de los ordenadores y terminales conectados a él. El ordenador examina la dirección que aparece en la cabecera del mensaje hacia el DTE que debe recibirlo. Esta tecnología permite grabar la información para atenderla después. El usuario puede borrar, almacenar, redirigir o contestar el mensaje de forma automática.

Conmutadas por Paquetes: En este tipo de red los datos de los usuarios se descomponen en trozos más pequeños. Estos fragmentos o paquetes, estás insertados dentro de informaciones del protocolo y recorren la red como entidades independientes.

Redes Orientadas a Conexión: En estas redes existe el concepto de multiplexión de canales y puertos conocido como circuito o canal virtual, debido a que el usuario aparenta disponer de un recurso dedicado, cuando en realidad lo comparte con otros pues lo que ocurre es que atienden a ráfagas de tráfico de distintos usuarios.

Redes no orientadas a conexión: Llamadas Datagramas, pasan directamente del estado libre al modo de transferencia de datos. Estas redes no ofrecen confirmaciones, control de flujo ni recuperación de errores aplicables a toda la red, aunque estas funciones si existen para cada enlace particular. Un ejemplo de este tipo de red es Internet.

Red Pública de Conmutación Telefónica (PSTN): Esta red fue diseñada originalmente para el uso de la voz y sistemas análogos.

La conmutación consiste en el establecimiento de la conexión previo acuerdo de haber marcado un número que corresponde con la identificación numérica del punto de destino.

6.6.- Redes Públicas.

Las redes públicas son los recursos de telecomunicación de área extensa pertenecientes a las operadoras y ofrecidos a los usuarios a través de suscripción (Guenul, 1997).

Estas operadoras incluyen a:

- Compañías de servicios de comunicación local.
- Compañías de servicios de comunicación a larga distancia. es un operador de telecomunicaciones que suministra servicios de larga distancia.
- Proveedores de servicios de valor añadido. Los proveedores de servicio de valor añadido, ofrecen con frecuencia, servicios de comunicación de área amplia como complemento a su verdadero negocio.

6.7.-Redes Privadas.

Una red privada es una red de comunicaciones privada construida, mantenida y controlada por la organización a la que sirve. Como mínimo una red privada requiere sus propios equipos de conmutación y de comunicaciones. Puede también, emplear sus propios servicios de comunicación o alquilar los servicios de una red pública o de otras redes privadas que hayan construido sus propias líneas de comunicaciones (Guenul, 1997).

Aunque una red privada es extremadamente cara, en compañías donde la seguridad es imperante así como también lo es el control sobre el tráfico de datos, las líneas privadas constituyen la única garantía de un alto nivel de servicio.

Además, en situaciones donde el tráfico de datos entre dos puntos remotos excede de seis horas al día, emplear una red privada puede ser más rentable que utilizar la red pública.

6.8.- Tecnologías.

Los protocolos de capa física WAN describen cómo proporcionar conexiones eléctricas, mecánicas, operacionales, y funcionales para los servicios de una red de área amplia. Estos servicios se obtienen en la mayoría de los casos de proveedores de servicio WAN tales como las compañías telefónicas, portadoras alternas, y agencias de Correo, Teléfono, y Telégrafo (Guenul, 1997).

Los protocolos de enlace de datos WAN describen cómo los marcos se llevan entre los sistemas en un único enlace de datos. Incluyen los protocolos diseñados para operar sobre recursos punto a punto dedicados, recursos multipunto basados en recursos dedicados, y los servicios conmutados multiacceso tales como Frame Relay[1].

Los estándares WAN son definidos y manejados por un número de autoridades reconocidas incluyendo las siguientes agencias:

- International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), antes el Consultative Committee for International Telegraph and Telephone (CCITT).
- International Organization for Standardization (ISO).
- Internet Engineering Task Force (IETF).
- Electronic Industries Association (ETA).

Los estándares WAN describen típicamente tanto los requisitos de la capa física como de la capa de enlace de datos.

7.- Sistemas Operativos de red.

La tarea principal del servidor de archivos de una red local es ejecutar el sistema operativo de red (el equivalente al sistema operativo MS-DOS compatible)

Se carga en segundo plano y funciona conjuntamente con el sistema operativo del ordenador. Cuando se indica un comando del sistema operativo, primero se prueba si es un comando local del ordenador o es un comando del sistema operativo de la red.

El sistema operativo de la red se encarga de controlar el acceso a los datos de los archivos que se encuentran en las unidades de discos compartidas del servidor, de la distribución del espacio en los discos duros del servidor y de la utilización de los periféricos compartidos (Raya-Raya, 2002).

Los sistemas operativos de red se dividen en dos grupos:

- Sistemas que utilizan el modelo cliente/servidor, éstos funcionan siguiendo el esquema de un servidor principal que proporciona soporte a las estaciones de la red. Entre ellos destacan: Microsoft LAN Manager, Microsoft Windows® NT 4, Microsoft Windows® 2000, NetWare 3.2, NetWare 4.2, NetWare 5.1 y Vines.

- Sistemas que utilizan el modelo punto a punto (peer to peer), en ellos no existe un servidor principal sino que todas las estaciones comparten sus recursos de igual a igual. Entre ellos destacan: Invisible LAN, LANtastic, Windows® 95/98, NetWare Lite y 1ONET.

7.1.- Modelos Basados en Cliente Servidor.

Estos sistemas operativos destacan en general por las grandes posibilidades de que disponen y su uso abarca desde una red pequeña hasta una gran red corporativa (Raya-Raya, 2002).

7.1.2.- Microsoft.

Microsoft cuenta con varios sistemas operativos de red que, poco a poco, han ido aumentando su cuota de mercado.

[1] Servicio de trasmisión sobre lineas de alta velocidad.

7.1.2.1.-LAN Manager.

Este sistema operativo de red (actualmente en desuso) cuenta con varios años en ejecución y se nota en sus prestaciones tanto a nivel de rapidez como de posibilidades. Conecta equipos que ejecutan MS-DOS, OS/2 y UNIX®.

Los requerimientos necesarios para su funcionamiento son:

- Una configuración mínima de memoria RAM de 8 MB.
- Soporta procesadores 386, 486 y Pentium.
- Una unidad de disco duro con suficiente capacidad de almacenamiento para el tamaño de la red. La capacidad mínima es de 30 MB.
- Una tarjeta de red.
- Cableado de red.
- (Recomendado) Una unidad de cinta u otro dispositivo de respaldo.

Detalles de la versión:

- Posibilidad de tener varios servidores de archivos.
- Se ofrece para servidor dedicado y no dedicado.
- 7,8 GB de máxima capacidad de almacenamiento en disco.
- 2 GB como tamaño máximo de un archivo.
- 8.192 archivos abiertos simultáneamente como máximo.
- Hasta 16 MB de tamaño máxima de RAM.
- 50 como número máximo de conexiones por servidor.

7.1.2.2.- Windows® NT.

El sistema operativo Windows® NT es una plataforma que trabaja en forma de cliente servidor. Es el sistema más desarrollado de la familia Windows® y fue diseñado para poder aprovechar al máximo los recursos del complejo hardware de 32 bits que existe actualmente.

Las primeras versiones que surgieron de este sistema operativo fueron diseñadas a principios de los 80, incorporando todos los beneficios de los sistemas Windows® que lo precedieron, integrando las aplicaciones al modelo Cliente-Servidor.

Sistema Operativo Multitarea, incluye procesadores INTEL RISC y Sistemas de Multiprocesamientos Simétricos Diseño de un avanzado microkernel integrando seguridad y una plataforma robusta para su manejo. Recursos compartidos de archivos e impresoras. Trabajo en forma de grupo. Soporte para múltiples protocolos. Compatible con otras redes (Banyan, VINES y Novell Netware) Manejo centralizado de restricciones a usuarios, a través de un solo ordenador, de departamentos, divisiones y grupos. Protección avanzada de datos a través de discos espejados, segmentación de discos (RAID 5) y soporte para manejo de UPS. Servicio de acceso remoto que permite conectarse vía WAN a través del discado en líneas telefónicas asincrónicas, ISDN y redes X-25. Estas tecnologías deben aplicarse con ordenadores trabajando con MS-DOS, Windows® para trabajo en grupo o Sistema Operativo Windows® NT. Servicio para Macintosh (los usuarios de este sistema pueden acceder al Windows® NT y compartir aplicaciones con otros servers de APPLE).

Puede trabajar como Sistema Operativo Distribuido aplicando el concepto de dominio pudiendo ser Server primario o en su defecto secundario (http://usuarios.lycos.es/betzweb/hobbies.html.2004).

Los requerimientos necesarios para su funcionamiento son:

- Sistemas Intel y compatibles:
- Procesador 486/33 o superior, Pentium o Pentium Pro.
- 125 MB de espacio en disco duro disponible.

- Sistemas RISC:
- Procesador RISC compatible con la versión.
- 160 MB de espacio en disco duro disponible.
- Mínimo de 16 MB de memoria RAM (recomendable 64 MB).
- Unidad de CD-ROM (a ser posible SCSI).
- Una tarjeta de red.
- Cableado de red.
- (Recomendado) Una unidad de cinta u otro dispositivo de respaldo.

Detalles de la versión:

Soporte de múltiples procesadores.

- Soporta procesadores 386, 486, Pentium, Alpha y MIPS.
- Se ofrece para servidor no dedicado.
- Sistema operativo de 32 bits.
- 402 millones de TB de máxima capacidad de almacenamiento en disco.
- Hasta 4 GB de tamaño máximo de RAM.
- 2 GB de memoria virtual por aplicación.
- Permite hasta 256 conexiones simultáneas por acceso remoto.
- Soporte de nombres de archivo de hasta 256 caracteres (NTFS).
- integra un servidor Web, un servidor Gopher y un servidor FTP.
- Proporciona PPTP (Point to Point Tunneling Protocol).
- Soporta los protocolos y transportes siguientes: TCP/IP, NetBIOS /NetBEUI, DLC y AppleTalk.
- Seguridad certificada C2.

7.1.2.3 Windows® 2000.

Esta versión cuenta con opciones excelentes y mejora notablemente funciones de Microsoft Windows® NT 4.

La familia de servidores Windows® 2000 está formada por tres versiones:

Server. Esta versión permite utilizar hasta 4 procesadores, hasta 4 GB memoria RAM e incorpora Directorio Activo, herramientas de gestión de Windows®, infraestructura de seguridad Kerberos y PKI, servicios de terminales, servicios de componentes y servicios de Internet.

Advanced. Esta versión permite utilizar hasta 8 procesadores, hasta 8 GB de memoria RAM e incorpora Directorio Activo, herramientas de gestión de Windows®, infraestructura de seguridad Kerberos y PKI, servicios de terminales, servicios de componentes, servicios de Internet, balanceo de la carga de la red y servicios de cluster.

Datacenter. Esta versión permite utilizar hasta 32 procesadores, hasta 64 GB de memoria RAM e incorpora Directorio Activo, herramientas de gestión de Windows®, infraestructura de seguridad Kerberos y PKI, servicios de terminales, servicios de componentes, servicios de Internet, balanceo de la carga de la red y servicios de cluster avanzados.

Los requerimientos necesarios para su funcionamiento son:

- Procesador Pentium 133 Mhz o superior.
- Una configuración mínima de memoria RAM de 64 MB.
- Una unidad de disco duro con suficiente capacidad de almacenamiento para el tamaño de la red. La capacidad mínima es de 1 GB.
- Una tarjeta de red.
- Cableado de red.
- Unidad de CD-ROM (a ser posible SCSI).
- (Recomendado) Una unidad de cinta u otro dispositivo de respaldo.

Sin embargo, la recomendación que se realiza para la configuración del servidor, está en función del tamaño de la red y el servicio que va a realizar en donde se va a instalar:

Servidores de pequeñas empresas. Para un servidor de una pequeña empresa que tenga hasta 50 usuarios y 25 equipos, se recomienda que cuente con 1 ó 2 procesadores Pentium II de 350 Mhz o superior, 128 MB de RAM, controladora SCSI-2 ultra rápida, dos discos de 4 GB cada uno y adaptador Ethernet de 10/100 Mbps.

Servidores departamentales. Para un servidor departamental que tenga hasta 200 usuarios (locales y remotos) o para incorporarlo en un entorno de varios servidores con un numero mayor de usuarios, se recomienda que cuente con varios procesadores Pentium III de 500 Mhz (2, 3 ó 4), 512 MB de RAM, sistema RMD con controladora SCSI-2 o SCSI-3 ultra rápida, cinco discos de entre 6 y 8 GB cada uno, adaptador Ethernet de 10/100 Mbps y controladores inteligentes 120.

Servidores empresariales. Para un servidor empresarial que tenga hasta 1.000 usuarios (locales y remotos), se recomienda que cuente con varios procesadores Pentium III de 550 Mhz (entre 4 y 8), entre 1 y 4 GB de RAM, sistema RAID con controladora SCSI-2 o SCSI-3 ultra rápida, cinco discos de entre 10 y 16 GB cada uno, adaptadores Ethernet de 10/100 Mbps y controladores inteligentes 120 (otra opción es montar un cluster con dos o más servidores departamentales que tendrán un menor coste económico).

En cuanto a las estaciones de trabajo, se necesitan ordenadores con un procesador Pentium II a 350 Mhz o superior, una configuración de memoria RAM de 64 MB y un tamaño de disco duro de entre 4 y 8 GB.

7.1.2.4 Windows XP.

Windows® XP (cuyo nombre en clave inicial fue Whistler) fue hecho público el 25 de octubre de 2001 por Microsoft. Microsoft inicialmente sacó a la venta dos versiones: Home y Professional. La versión Home está destinada al mercado doméstico, mientras que la versión Professional dispone de características adicionales diseñadas para entornos empresariales, como la autenticación por red y el soporte multiprocesador. Las letras "XP" provienen de la palabra experience (http://es.wikipedia.org/wiki/Windows®_XP.2004).

Antes de XP, Microsoft producía dos líneas separadas de sistemas operativos. Una línea estaba dirigida a los ordenadores domésticos representada por Windows® 95, Windows® 98 y Windows® Me, mientras que la otra, representada por Windows® NT y Windows® 2000, estaba pensada para el mercado corporativo y empresarial e incluía versiones especiales para servidores. Windows® XP es el intento por parte de Microsoft de ofrecer un único sistema operativo multiuso, con el inconveniente de eliminar definitivamente el soporte para los programas basados en MS-DOS del sistema operativo.

Windows® XP está basado en el código de Windows® 2000 con una nueva interfase gráfica (llamada Luna), el cual incluye características ligeramente rediseñadas, algunas de las cuales parecen inspiradas por los modernos entornos de escritorio presentes en Linux, como KDE. La pantalla de login gráfica con imágenes para cada usuario es un buen ejemplo. Incluye también un reducido conjunto de las características de seguridad de Windows® 2000 y un cortafuegos integrado (desactivado por defecto). Todo ello es parte de un esfuerzo mayor en hacer seguros los productos de Microsoft.

En noviembre de 2002, Microsoft sacó a la venta dos nuevas versiones de Windows® XP para hardware específico:

Windows® XP Media Center Edition: para ordenadores especiales, actualmente, dichos ordenadores son los "HP Media Center Computer" y la serie "Alienware Navigator". "Windows® XP Media Center Edition" debe ser vendido con uno de estos ordenadores y no puede encontrarse en tiendas.

Windows® XP Tablet PC Edition: para ordenadores portátiles especiales diseñados con una pantalla táctil que admiten escritura a mano y pantallas tamaño portarretratos.
Adicionalmente, el 28 de marzo de 2003, Microsoft hizo pública otra versión:

Windows® XP 64 Bit Edition: para fabricantes cuyo destino son los procesadores Intel Itanium.

7.2 Modelos Basados en Sistemas Punto a Punto.

Estos sistemas operativos destacan por la sencillez de su instalación y bajo coste aunque no pueden llegar a competir en posibilidades con los basados en el modelo cliente/servidor (Raya-Raya, 2002).

Están diseñados para redes que cuentan con 10-20 estaciones de trabajo.

7.2.1. Windows® 95/98.

7.2.1.1 Windows 98.

Windows® 98 (nombre clave: Memphis) es un sistema operativo gráfico híbrido entre 16 y 32 bits. Fue liberado el 25 de junio de 1998 por la empresa de software Microsoft.

Windows® 98 fue construido sobre el anterior Windows® 95, e incluía mejor soporte para estándares de hardware como USB, MMX y AGP. Otras opciones incluyen el sistema de archivos FAT32, soporte para múltiples monitores, soporte para Web TV y la integración de Internet Explorer como componente esencial del sistema.

7.2.1.2 Windows® 98 SE.

Windows® 98 SE (Segunda Edición) es una revisión del sistema operativo Windows® 98, creado por la empresa de software Microsoft. Fue liberado el 10 de junio de 1999.

Windows® 98 SE incluía un número de mejoras sobre la versión original de Windows® 98, como Internet Explorer 5, Netmeeting 3, conexiones de Internet compartidas y soporte para DVD (http://es.wikipedia.org/wiki/Windows_98_SE.2004).

Fue criticado por no ser liberado como una actualización gratuita para aquellos usuarios que poseían una copia legal del original.

No obstante, al corregir una serie de fallos, otros muchos se incorporaban a la nueva versión siendo necesario el acceso continuo al servicio de parches de Microsoft.

Proporciona una buena integración entre Microsoft Windows® y una red punto a punto, proporcionando una pasarela para conectarse a un servidor de archivos NetWare y acceder a todos sus archivos.

Los menús y funciones de la red están integradas en el propio Windows® administración y gestión de la red se realizan con varias utilidades: Panel de Control Explorador de Windows® y Entorno de red.

La protección por clave de acceso es limitada, es decir, los propietarios de los archivos pueden conceder el acceso total, sólo lectura o denegar el acceso a dichos archivos. También, se puede conceder el acceso a los equipos a nivel de usuarios pero no ofrece un mayor control de los privilegios tanto para los usuarios como para los grupos.

Los requerimientos necesarios para su funcionamiento son:

- Una configuración mínima de memoria RAM de 8 MB.
- Una unidad de disco duro con suficiente capacidad de almacenamiento para el tamaño de la red.
- Una tarjeta de red.
- Cableado de red.

Detalles de la versión:

- Soporta lectores CD-ROM.
- Soporta Sistema de alimentación ininterrumpida (SAI).

7.2.2 Windows ME.

Windows® Me (Millennium Edition) es un sistema operativo gráfico de 32-bit lanzado el 14 de Septiembre de 2000 por Microsoft Corporation.

Éste sistema operativo está basado en Windows® 95 y Windows® 98, principalmente está compuesto por actualizaciones relativamente pequeñas, como Internet Explorer 5.5. Una de los cambios más significativos fue la introducción del reproductor de medios Windows® Media Player 7, el cual estaba pensado para competir con RealPlayer, el reproductor de medios dominante en aquel momento.

Un programa completamente nuevo en el sistema operativo fue Movie Maker. Éste programa permite una edición de video básica y fue diseñado para ser sencillo de usar por el usuario común.

De todos modos, el cambio más significativo fue la complicación de mantener la compatibilidad DOS y la introducción de la utilidad de registro y restauración del sistema, con la idea de facilitar la resolución de problemas sin la necesidad de volver al intérprete de comandos.

En principio, este cambio fue un gran paso adelante: nunca más necesitaría el usuario saber emplear ese vetusto intérprete de comandos para mantener el sistema y solucionar problemas, aunque, en la práctica, la pérdida de la funcionalidad DOS es una importante barrera a la hora del mantenimiento. Como añadido, Restauración del Sistema añade problemas mayores. La eficiencia del sistema, que nunca ha sido una prioridad en Windows®, se ve reducida notablemente. Además ha sido comprobado que es poco robusta para tratar con efectividad algunos asuntos comunes y dado que recrea automáticamente los estados previos en cada reinicio del sistema, hace muy difícil al usuario inexperto hacer un cambio deseado, del tipo de eliminar un virus o un programa no solicitado.

8.- Internet

Internet se podría definir como una red que engloba una serie de redes de ordenadores con la finalidad de permitir el libre intercambio de información entre sus usuarios. Es posible tener acceso a cualquier información: desde las fotografías enviadas por el satélite Meteosat hasta información conseguida en una universidad estadounidense o bien conseguir un programa de utilidad pública que se encuentre en un ordenador australiano (Raya-Raya, 2000).

Sin embargo, conectarse a Internet es como entrar en una inmensa biblioteca.

Hay una gran cantidad de libros en interminables estanterías que contienen una cantidad enorme de información que si no se sabe cómo buscarla será totalmente inservible.

Además, Internet no es un servicio centralizado. No existe ninguna empresa a la que se pueda solicitar un catálogo de todos los servicios, de todas las bases de datos o un índice donde aparezcan todos los temas. Internet sólo se limita a establecer los procedimientos de interconexión, pero cada red o cada ordenador tiene su propio dueño.

El precio de conexión a Internet varía de acuerdo con el costo de mantenimiento de cada red, que es la que fija las tarifas a los usuarios que se conectan a ella. También es posible encontrar redes subvencionadas por los respectivos gobiernos, por lo que los centros que se conecten a ellas sólo pagan por la conexión al punto de acceso más cercano (Sosa,1999).

8.1 Tipos de acceso

Existen tres formas de acceso a Internet:

- A través de un proveedor de acceso. Para ello, se necesita disponer de un módem o de un ruteador, software de comunicaciones y una cuenta en un proveedor de acceso a Internet. Lo que se puede obtener está en función de lo ofrecido por la empresa que varía desde el correo electrónico únicamente a toda la gama de servicios. Ello determina el costo del servicio que es mayor cuantos más servicios ofrezca la empresa, al que habría que añadir el costo de la llamada telefónica (Raya-Raya, 2000).

- Con un nodo propio. Para ello, se necesita disponer de un módem o una línea punto a punto, software que implemente TCP/IP y permiso de acceso al nodo de Internet. Con este método se dispone de un acceso completo Internet pero a una velocidad que estará determinada por la velocidad del módem, o de la línea punto a punto, y que nunca debería bajar de 28.800 bps. El coste estará determinado por el precio del módem más la tarifa de la llamada telefónica.

- A través de otras redes. Para ello, se necesita disponer de una conexión de una red que disponga de acceso a Internet a través de un módem o de un ruteador. Se deberá disponer de la tarjeta de conexión a la red, de un redirigidor de paquetes ODJ o NDIS y de TCP/IP (con Windows® también se necesitará el módulo Winsock). Con este método se dispone de un acceso completo a Internet a la velocidad permitida por el módem o ruteador. El costo estará determinado por la tarifa de la línea utilizada (RTB, Frame Relay, X25, RDSI) para la conexión a la red que tiene acceso a Internet y el software TCP/IP.

Es importante hacer constar que la velocidad de la transmisión va a tener gran influencia tanto en el tiempo dedicado a la conexión, el tiempo de transferencia de archivos y, sobre todo, al costo de la sesión.

8.2 Intranet.

Intranet es un término relativamente nuevo y puede utilizarse para definir una red privada que utiliza el conjunto de protocolos TCP/IP y no está conectada Internet.

Durante muchos años las redes con protocolos TCP/IP accedían a Internet para tener acceso a las múltiples utilidades que estaban disponibles.

A partir de 1994, empezó a ganar adeptos una opción que consistía en utilizar dichos protocolos y las posibilidades que brindaban los servicios disponibles en Internet, pero sin permitir el acceso a Internet. De esa manera surgió el concepto de Intranet (Raya-Raya, 2000).

Entre sus múltiples ventajas se encuentran:

- Interoperabilidad. Se tiene acceso a todos los servicios de Internet pero restringidos al uso interno de la empresa y a todos los productos de la red.
- Escalabilidad. Se puede dar acceso fácilmente a nuevos usuarios de la empresa a dichos servicios sin molestias para los que ya la están utilizando.
- Seguridad. Se produce una gran mejora en la seguridad de la red local al evitar el acceso de usuarios no autorizados a nuestros servicios Internet.
- Disminución de los costes. Permite una disminución drástica de los costes de correo, papel y de la factura telefónica al simplificar las comunicaciones internas y el intercambio de información.

- Aumento de la efectividad. Si está bien diseñada, permite una mejora de la efectividad al tener acceso de forma sencilla a una serie de servicios que simplifican el trabajo y mejoran el tiempo de acceso a la información.

8.3 Extranet.

El concepto Extranet es una mezcla de Internet e Intranet y sirve para definir a una red privada virtual que utiliza a Internet como medio de transporte de la información entre sus propios nodos. También recibe el nombre de VPN (Virtual Private Networks) (Raya-Raya, 2000).

Gracias a una Extranet se pueden unir dos Intranets que se encuentran situadas en distintas ubicaciones utilizando X25, RDSI, líneas punto a punto o frame relay.

Para ello, es necesario que cada una de las Intranets disponga de acceso a un proveedor de acceso de Internet (ISP). Una vez en Internet, los datos serán transmitidos por distintas rutas alternativas hasta llegar a la sede destino.

Para evitar la conexión de personas no autorizadas a las Intranets, será necesario contar con cortafuegos (firewalls) y proxies que autentifiquen los accesos, así como proceder a una encriptación de los paquetes que van a viajar desde una sede a la otra.

Uno de los protocolos que permiten crear un túnel seguro a través de Internet es el protocolo PPTP.

De esta manera, se tendrá una gran reducción de costes para la empresa y una alta fiabilidad.

9.-Redes y Seguridad.

La seguridad es un concepto relativo, pues los mecanismos que minimizan la vulnerabilidad de un bien o recurso en un determinado caso, pueden ser insuficientes en otro caso. Esta suficiencia o insuficiencia vendrá determinada por la importancia de los bienes y recursos que posea, de forma que un ordenador que solo contenga contabilidad doméstica puede considerarse seguro sin la presencia de ningún mecanismo, mientras que un ordenador que contenga la contabilidad de una empresa debe poseer mecanismos para asegurar la imposibilidad de manipulación de la misma (Smith, 1997).

Las amenazas a la seguridad pueden clasificarse, atendiendo a la intencionalidad de las mismas en accidentales o intencionadas.

Las amenazas accidentales son las que se producen sin necesidad de un intento premeditado, como por ejemplo una avería en el sistema.

Las amenazas intencionadas pueden variar desde el examen casual de la información de un ordenador hasta ataques sofisticados utilizando conocimientos especiales sobre el sistema.

Si en lugar de atender a la intencionalidad se atiende al daño ocasionado, las amenazas a la seguridad se clasifican en pasivas y activas.

Las amenazas pasivas son las que no conllevan ninguna modificación en la información que posee el sistema y por tanto no se modifica ni su operación ni su estado.

Las amenazas activas suponen una alteración del sistema y un cambio en su estado de operación. Aunque obviamente las amenazas activas son mucho más perjudiciales que las pasivas, estas deben ser tenidas en cuenta pues en muchos casos pueden convertirse en activas con la intervención de un agente distinto.

La seguridad adquiere cada vez más importancia a medida que la red informática se encuentra presente en más aspectos de la economía mundial, aspectos como el comercio electrónico, la transacción de información confidencial a través de la misma, etcétera.

Obviamente, la seguridad es un tema que debe inquietar a cualquier organización que hoy día decida conectar su red a otras sobre Internet. Basta echar un vistazo a las estadísticas para tomar conciencia del riesgo que se corre: el número de incidentes contra sistemas conectados casi se duplica cada año, según el Computer Emergency Response Team Coordination Center (CERT-CC). Y no es raro, si se tiene en cuenta el vertiginoso crecimiento de Internet en los últimos años, que implica, por una parte, nuevas redes susceptibles de ser atacadas, y por otra, nuevos atacantes en potencia.

Lo cierto es que tal y como están las cosas, atacar una red conectada a Internet que no haya sido protegida de un modo "especial" (es tan frecuente como erróneo creer que una filosofía de seguridad tradicional, basada en contraseñas y protección de archivos, es suficiente para protegerse en Internet), es relativamente fácil si se sabe cómo, y mucho más aún si se utilizan sistemas operativos antiguos que no han sido actualizados ni debidamente "parcheados". En la red es posible encontrar, sin mucho esfuerzo, listas de debilidades tanto de protocolos como de sistemas operativos, así como guías que señalan los pasos a seguir para explotar dichas debilidades.

Todas las líneas actuales de investigación en seguridad de redes comparten una idea: la concentración de la seguridad en un punto. Se obliga a que todo el tráfico entre la red que se pretende proteger y las redes externas pase por un mismo punto. Este punto se conoce con el nombre de cortafuego, y físicamente puede ser desde un simple ordenador hasta un complejo conjunto de redes separadas por ruteadores.

El empleo de un cortafuego presenta enormes ventajas sobre los enfoques de seguridad en redes tradicionales (que requieren la seguridad individual de cada ordenador conectado, y por tanto sólo pueden justificarse en entornos con un reducido número de máquinas), permitiendo concentrar todos los esfuerzos en el control de tráfico a su paso por el cortafuego (Smith, 1997).

9.1.- Peligros y Modos de Ataque.

Últimamente se ha visto aparecer en la red diversas taxonomías de vulnerabilidades y tipos de ataques. Aquí tenemos una lista con los tipos de ataques que actualmente se pueden realizar sobre Internet, explicando brevemente en qué consiste cada uno y qué debilidades aprovecha (http://www.securityfocus.com.2003).

- **Sniffing** : Este ataque consiste en escuchar los datos que atraviesan la red, sin interferir con la conexión a la que corresponden. Se utiliza principalmente para obtener contraseñas, y en algunos casos para obtener información confidencial. Para proteger los contraseñas contra el sniffing basta con emplear mecanismos de autenticación y encriptación.

- **Spoofing:** Es el nombre que se le da a los intentos del atacante por ganar el acceso a un sistema haciéndose pasar por otro que dispone de los privilegios suficientes para realizar la conexión. El ataque que más se suele utilizar sobre conexiones TCP es el conocido como adivinación del número de secuencia. Se basa en la idea de que si un atacante puede predecir el número inicial de secuencia de la conexión TCP generado por la máquina destino, entonces el atacante puede adoptar la identidad de máquina "confiada".

- **Hijacking:** Consiste en robar una conexión después de que el usuario ha superado con éxito el proceso de identificación ante el sistema. El ordenador desde el que se lanza el ataque ha de estar en alguna de las dos redes extremo de la conexión, o al menos en la ruta entre ambas. El único método seguro para protegerse contra este tipo de ataques es el uso de encriptación. .

- **Ingeniería Social:** Son ataques que aprovechan la buena voluntad de los usuarios de los sistemas atacados. Un ejemplo de ataque de este tipo es el siguiente: se envía un correo con el remite "root" a un usuario, en una gran red académica (donde frecuentemente los usuarios no conocen a los administradores), con el mensaje "por favor, cambie su contraseña a murcia1". El atacante entonces espera un poco, y entra con esa contraseña. A partir de ahí puede emplear otras técnicas de ataque (bugs del sistema para obtener un control total de la máquina, confianza transitiva para entrar en otras máquinas de la red, etcétera). Ante este tipo de ataques la mejor defensa es educar a los usuarios acerca de qué tareas no deben realizar jamás, y qué información no deben suministrar a nadie, salvo al administrador en persona.

- **Explotar Bugs del Software:** Aprovechan errores del software. A la mayor parte del software se le ha añadido la seguridad demasiado tarde, cuando ya no era posible rediseñarlo todo. Además, muchos programas corren con demasiados privilegios, lo que les convierte en objetivo de los intrusos, que únicamente han de hacerse con una copia del software a explotar y someterlo a una batería de pruebas para detectar alguna debilidad que puedan aprovechar. Entre los posibles ataques que se pueden efectuar está el desbordamiento de pila, consistente en introducir datos en la pila a través de funciones de entrada salida, de forma que permitan modificar las posiciones de retorno de las funciones y con ello ejecutar código que permite al atacante tomar control del sistema. Esta secuencia de ataques, se conoce como exploits. La solución a este problema de desbordamiento se realiza a través de funciones de entrada/salida limitada, Las funciones strcpy(), strcat(), gets(), son potencialmente vulnerables.

- **Confianza Transitiva:** En sistemas Unix® existen los conceptos de confianza entre hosts y entre usuarios. Se dice que un sistema es confiado para otro cuando desde el primero, cualquier usuario puede establecer una conexión al segundo sin necesidad de dar una contraseña. Se dice que un usuario sobre un sistema es confiado para otro sistema cuando ese usuario, desde el primer sistema, puede establecer una conexión al segundo sin necesidad de dar una contraseña. Así, cualquier atacante que tome el control de una máquina, probablemente podrá conectarse a otras gracias a la confianza entre ordenadores y/o entre usuarios

- **Ataques Dirigidos por Datos:** son ataques que tienen lugar en modo diferido, sin la participación activa por parte del atacante en el momento en el que se producen. El atacante se limita a hacer llegar a la víctima una serie de datos que al ser interpretados ejecutarán el ataque propiamente dicho.

- **Caballo de Troya:** Un programa que se enmascara como algo que no es, normalmente con el propósito de conseguir acceso a una cuenta o ejecutar comandos con los privilegios de otro usuario.

- **Denegación de Servicios:** Estos ataques no buscan ninguna información contenida en las máquinas atacadas ni conseguir acceso a ellas. Únicamente van encaminados a impedir que sus usuarios legítimos puedan usarlas. El caso más típico es el mail bombing: envío de cantidades ingentes de correo a la máquina atacada hasta saturarla. Puesto que es casi imposible evitar todos los ataques de denegación de servicio, lo más importante es configurar los servicios para que si uno de ellos es inundado, el resto permanezca funcionando mientras se encuentra y soluciona el problema.

- **Enrutamiento Fuente:** Los paquetes IP admiten opcionalmente el enrutamiento fuente, con el que la persona que inicia la conexión TCP puede especificar una ruta explícita hacia él. La máquina destino debe usar la inversa de esa ruta como ruta de retorno, tenga o no sentido, lo que significa que un atacante puede hacerse pasar por cualquier máquina en la que el destino confíe (obligando a que la ruta hacia la máquina real pase por la del atacante). Dado que el enrutamiento fuente es raramente usado, la forma más fácil de defenderse contra esto es deshabilitarlo en el ruteador.

- **Adivinación de Contraseñas:** Un elevado porcentaje de penetraciones en sistemas se deben al fallo del sistema de contraseñas. El fallo más común es la mala elección de contraseñas por parte de los usuarios. Este se suele llevar a cabo en dos formas básicas. La primera consiste en intentar entrar usando pares cuenta-contraseña conocidos o asumidos (muchos sistemas operativos disponen de cuentas administrativas con contraseñas por defecto, que pese a no ser comentadas en los manuales del sistema, son conocidas por los atacantes). El segundo modo en que los intrusos obtienen las contraseñas es mediante el uso de crackers (programas que comparan un diccionario de términos contra archivos de contraseñas robados). Para protegerse contra estos ataques es vital tanto la educación al usuario sobre cómo elegir su contraseña, como mantener asegurado el archivo de contraseñas, de modo que no pueda ser robado.

- **ICMP Redirect y Destination Unreachable:** muchos mensajes ICMP recibidos en un ordenador son específicos a una conexión particular o son disparados por un paquete enviado por ese host. La intención es limitar el alcance de los cambios dictados por ICMP. Desafortunadamente las viejas implementaciones de ICMP no usan esta información extra, y cuando llega uno de esos mensajes, todas las conexiones entre el par de ordenadores que intervienen en la conexión que propició el mensaje se ven afectadas. Además, con la opción redirect, alguien puede alterar la ruta a un destino para que las conexiones en las que esté interesado pasen por su máquina, de forma que pueda intervenirlas. Los mensajes redirect deben obedecerlos sólo los hosts, no los ruteadores, y sólo cuando estos provengan de un ruteador de una red directamente conectada.

9.2 Elementos de Seguridad.

Una vez conocidos los peligros a los que los usuarios se enfrentan se necesitan medios para proteger los sistemas contra ellos. En principio, limitando el tráfico entre la red y las externas, a aquel que se considere seguro, o al menos que esté justificado, limitar el número de ataques posibles. El filtro de paquetes y los servidores proxy permiten esto. Además, si se decide permitir que se pueda acceder a las máquinas desde el exterior, se habrá de asegurar de que los intentos de conexión provienen de quienes dicen provenir. Para ello no se puede fiar de las contraseñas convencionales, puesto que un ataque por sniffing daría la contraseña al atacante.

Con estos métodos de autenticación se soluciona este problema. Por último, si se cree que la red puede ser objeto de un ataque hijacking, se necesita alguna técnica para impedirlos. En este caso se necesitara encriptar la conexión (Smith, 1997).

Los métodos a aplicar en una red para ofrecer barreras de seguridad son:

- Métodos criptográficos: redes privadas virtuales, IPSec, SSH (Secure Shell)
- Seguridad perimetral: cortafuegos, NAT (Network Address Traslation) e IDS (Intrusión Detection System)
- Seguridad en el sistema centralizado (envolventos y/o proxies)

Descritos los métodos, los elementos utilizados por dichos métodos son:

- **Criptografía**: Mediante el uso de la criptografía se intenta proteger la información a base de codificarla de una forma desconocida a los elementos que no forman parte de la comunicación: algoritmos de clave privada o simétricos (DES, TDES, IDEA, RC4 y Skipjack), algoritmos de clave pública o asimétricos (RSA). Las aplicaciones básicas de los algoritmos criptográficos son: el cifrado es la encriptación de un mensaje con una clave; la firma digital para protegerlos contra la falsificación, permitiendo al receptor probar la fuente y la integridad de los mismos, una función hash segura.
- **Autenticación**: La autenticación es el proceso seguido por una entidad para probar su identidad ante otra hasta ahora segura. Se distinguen dos tipos de autenticación: la de un usuario a una máquina durante la secuencia de login inicial, y la de máquina a máquina durante una operación. Las contraseñas tradicionales son demasiado débiles para usarlos sobre una red, y por tanto se usan contraseñas no reusables. Estos cambian cada vez que se usan, y por tanto no son sensibles al sniffing. El método de autenticación por dirección IP del host (o bien su nombre DNS) es susceptible de ser atacado mediante spoofing con relativa facilidad, y por tanto se usan técnicas de criptografía, contando con un Centro de Distribución de Claves (KDC) para la distribución y verificación de las mismas. El KDC más conocido es Kerberos[2].

[2] Protocolo de autenticación para ejecutarse en un cliente y demostrar su identidad.

- **Filtro de Paquetes**: Los ruteadores permiten realizar un filtrado de paquetes en base a la información contenida en sus cabeceras. Básicamente, la información que se suele examinar es: la dirección IP origen, la dirección IP destino, el tipo de protocolo (TCP, UDP o ICMP), el campo de opciones IP, el puerto origen TCP o UDP, el puerto destino TCP o UDP, el campo de banderas TCP y el tipo de mensaje ICMP. Además de la información contenida en el paquete, se puede tener en cuenta la interfase de red por la que llega el paquete. El hecho de que los servidores de servicios Internet residan en ciertos números de puertos concretos, permite al ruteador bloquear o permitir la conexión a esos servicios simplemente especificando el número de puerto apropiado en el conjunto de reglas especificado para el filtro de paquetes. El filtro de paquetes es transparente a los usuarios, es decir, no requiere conocimientos ni cooperación por su parte.

- **Servidores Proxy o Pasarelas**: Son aplicaciones que permiten redirigir el tráfico del nivel de aplicación a través de un cortafuego en el acceso a una red (ejemplo con Socks, Sock-et-s) y/o puentear con otra aplicación, dentro de un sistema centralizado. En este último caso también se llama envolvente. Al cliente le presentan la ilusión de que está tratando directamente con el servidor real. El servidor real cree que está tratando directamente con un usuario en el ordenador donde está corriendo el proxy. Este sistema no siempre es transparente al usuario, puesto que algunos proxies requieren software cliente especial, o bien el software estándar utilizándolo con procedimientos especiales. Los servicios proxy sólo son efectivos usados en conjunción con un mecanismo que restrinja las comunicaciones directas entre los ordenadores internos y externos (bien con un dual-homed host, bien con filtro de paquetes).

Red Privada Virtual.

Capítulo II. Red Privada Virtual.

1.- Fundamentos de las Redes Privadas Virtuales.

1.1.- Antecedentes.

Una de las necesidades vitales de las organizaciones modernas es la posibilidad de compartir información, particularmente apremiante para aquellas que se encuentran diseminadas, con sedes en diferentes zonas y secciones de la organización que no se encuentran en el mismo entorno físico.

Hace unos años todavía no era tan importante el conectar usuarios a Internet para cuestiones de trabajo, pero a medida que ha pasado el tiempo las compañías han querido que las redes LAN trasciendan más allá del ámbito de la oficina e incluyeran a los trabajadores y centros de información de otros edificios, ciudades, estados o incluso otros países, y tenían que invertir en hardware y servicios de telecomunicaciones costosos para crear redes amplias de servicio, WAN. Sin embargo ya con Internet, las compañías tienen la posibilidad de crear una red privada virtual que demanda una inversión relativamente pequeña de hardware y utiliza Internet global para la conexión entre los puntos de la red.

Durante un tiempo, las grandes corporaciones habían solucionado el problema mediante sistemas de comunicación como líneas punto a punto y complejas instalaciones de interconexión. Aunque efectivas, estas soluciones quedaban fuera del alcance de organizaciones de menor tamaño y con recursos económicos y técnicos más escasos.

Las redes tipo LAN (Local Area Network) permiten conectar entre sí varios ordenadores en una misma oficina. Con la aparición de las nuevas tecnologías hoy en día es posible conectar esta red LAN (uno o más ordenadores) a Internet. Esta conexión puede ser de varias maneras:

- Unidireccional: conexión a Internet desde la red LAN para consulta de información.
- Bidireccional: el acceso es en ambas direcciones, desde la LAN hacia Internet o bien desde Internet hacia la LAN.

Las últimas alternativas de comunicación, como ADSL, han hecho que la desventaja operativa desaparezca, permitiendo ya a pequeñas y medianas empresas disponer de su propia red de comunicación privada. Ahora, las centrales y tiendas o sucursales disponen de su propia red de comunicación privada. Ahora, pueden intercomunicarse y compartir información de forma sencilla y segura, con inversiones muy inferiores a las de hace muy poco tiempo.

Las LAN tradicionales son redes esencialmente restringidas, por lo cual se puede intercambiar información entre los ordenadores sin pensar en la seguridad de la información; pero Internet no es seguro, por lo tanto las VPN usan protocolos especiales que permiten encriptar información y permitir únicamente a la persona autorizada desencriptar esa información con un identificador que comprueba que la transmisión se ha hecho desde una fuente confiable.

1.1.1 -¿Qué es una red privada virtual?

A continuación se citan algunas definiciones que han dado diferentes autores de cómo definir a una VPN por sus siglas en ingles (Virtual Private Network), y en español Redes Privadas Virtuales.

"La VPN (Red Privada Virtual), es un método utilizado para conectar a dos redes o dispositivos mediante una vía común. Una VPN utiliza a internet para crear un túnel (o conexión) virtual entre dos dispositivos geográficamente separados de modo que operen como si se encontraran en la misma red física."[1]

"Un proceso de comunicación cifrado o encapsulado que transfiere datos desde un punto hacia otro de manera segura;

[1] Sosinski B. y Moskowits J., aprendiendo Windows 2000 server en 24 horas

La seguridad de los datos se logra gracias a una tecnología robusta de cifrado, y los datos que se transfieren pasan a través de una red abierta, insegura y enrutada."[2]

"Las VPN mantienen las mismas normas de seguridad y administración que una red privada. Son el método más efectivo en cuanto a costo de establecer una conexión virtual punto a punto entre usuarios remotos y una red de una empresa cliente."[3]

"Una VPN es una red desplegada en una infraestructura compartida y emplea la misma seguridad, dirección, y políticas aplicadas en una red privada." [4]

"Las redes privadas son redes de área amplia (WANs) que conectan LANs dispersas, por lo general entre una oficina central y oficinas de sucursal o clientes de ordenadores remotos en oficinas caseras, o ambos. La comunicación suele ser una línea de telecomunicación principal o una columna vertebral que consta de líneas arrendadas o fibra dedicada."[5]

Una Red Privada Virtual (VPN) es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones geográficas. 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.

Una Red Privada Virtual es una red privada que se extiende, mediante un proceso de encapsulación, y en su caso, de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un túnel definido en la red pública. En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignándole a su ordenador remoto las direcciones y privilegios de la misma, aunque la conexión la haya realizado por medio de un acceso a Internet público (http://www.eltallervirtual.cl/modules.php?name=News&file=article&sid=626.2004).

Por qué Virtual?

Virtual porque al momento del establecimiento de una conexión VPN el cliente virtualmente extiende la red de la empresa hasta donde él esté, esto lo hace trabajar lógicamente dentro de la misma empresa, pero dentro de un concepto "virtual"

Por qué Private?

Privada porque el concepto de privacidad se mantiene una vez implementada la VPN. La privacidad en las comunicaciones de la empresa es parte esencial en las políticas de seguridad. Las comunicaciones a través de VPN mantienen su privacidad sobre medios públicos ya que van encapsuladas dentro de un túnel encriptado y autentificado y solo se mantienen circulando dentro de la red de la empresa (la que incluye la conexión virtual VPN)

Por qué Network?

Junto con ser obvio que las VPN trabajan a nivel de red el por que network es porque son capaces de interconectar, extender y comunicar redes o segmentos de redes. Las VPN también pueden crear túneles de comunicación internos entre una maquina y un servidor dentro de la red de una empresa. (hay empresas que tienen VPN dentro de sus propias redes para asegurar comunicaciones con servidores críticos)

---

[2] Brown S., ingeniero de cortafuegos y VPN en Cable&Wireless.
[3] Mason A. G. consultor para ISP en Reino Unido.
[4] Cisco Security.
[5] Leon D. Consultor en tecnología de información con UNISYS.

1.1.2 ¿Cómo funcionan?

Cuando se establece una conexión entre dos nodos de VPN, el túnel de VPN en realidad se desempeña como un enrutador en la parte superior del protocolo de Internet. Si la dirección de destino de un paquete está destinada a un nodo terminal de VPN, hablando en términos generales, el servidor de túnel o puerta de enlace de seguridad *de origen* realiza varias operaciones (Brown, 2001):

1. El protocolo de entunelamiento agrega un encabezado "externo" al paquete original. El encabezado externo contiene la dirección del nodo de VPN que termina el túnel.

2. El servidor de túnel o puerta de enlace de seguridad selecciona la clave de encriptación apropiada para operaciones de autenticación y encriptación. Cada túnel resultante utiliza su propia clave de encriptación.

3. Se encripta el encabezado IP original y la carga de paquete o los datos de transporte. En el caso de IPSec, también se autentica el encabezado externo, establecido por el mismo.

4. El paquete IP entunelado (autenticado y encriptado) se enruta a través de Internet al punto final de destino de la VPN. El punto final podría ser un host, como una estación de trabajo de usuario remoto, u otra puerta de enlace de seguridad .(Clark, 2001).

1.1.3 Redes Privadas Virtuales: una WAN mágica.

Si Internet es la tierra prometida y las redes privadas son otras tierras sagradas, entonces la tecnología de VPN es la WAN mágica, porque a través de ella, se hereda lo mejor de ambos mundos. Las VPN proporcionan a las empresas la seguridad, el desempeño, la disponibilidad y el ambiente de multiprotocolo de una red privada a través de la económica y ubicua Internet. Para el registro, las VPN proporcionan vínculos seguros de transporte de datos, llamados túneles, a través de las líneas de comunicación públicas de Internet.

Los túneles seguros se establecen entre dos nodos o sitios de Internet mediante las tecnologías de encriptación, autenticación y validación de datos que trabajan en concierto. Las VPN utilizan autenticación sólida para establecer el túnel, encriptan los paquetes o datagramas de IP para mezclar los datos para su protección, luego emplean verificaciones de integridad de datos para asegurar que los paquetes arriben sin alteración a su destino. En otras palabras, las VPN permiten que la información privada se transmita a través de Internet pública sin sufrir ataques de intrusos. En efecto, Internet se transforma en su propia red virtualmente privada (Clark, 2001).

1.1.4 La Realidad de las VPN.

Las VPN son un avance tecnológico importante y piedra angular en la evolución de Internet o redes de área amplia, dependiendo de cuál lado de la moneda tome en cuenta. Internet ya está cambiando la manera en que las empresas hacen negocios. La mezcla de encriptación, autenticación y técnicas de validación de datos para distinguir a las VPN en Internet es en realidad una innovación notable, y las VPN deben probar que son un nuevo catalizador importante en este cambio. La manera en que la cultura de una organización debe conducir los negocios en una economía global depende de la confiabilidad, seguridad y disponibilidad de la red organizacional. A su vez, la propia VPN depende de la conveniencia con que la tecnología se desempeñe e integre con tecnología de Internet. A medida que maduren los ciclos de vida de las tres tecnologías básicas que componen las VPN, la tasa de adopción aumentará, estableciendo a las VPN a la vanguardia del despliegue WAN.

La maduración de los estándares tecnológicos de VPN es crítica para este proceso. Como se sabe, los estándares aseguran interoperabilidad entre soluciones de vendedores competidores.

Los estándares de VPN, aunque están madurando, en esencia aún se encuentran surgiendo, y su implantación en ofertas de vendedor no es homogénea por completo (Clark, 2001).

1.2.1.-Áreas de la Red Privada Virtual.

Las VPN se presentan en cuatro áreas

Se utiliza el término área, puesto que así es cómo se describen muchos artículos. Las áreas simplemente significan implementaciones de VPN. Las VPN no son nuevas, pero añaden un nivel de tecnología de cifrado a los servicios de Internet (Brown, 2001).

Intranet Una VPN de Intranet se crea entre la oficina central corporativa y una oficina de ventas remotas, o entre las oficinas centrales y las dependientes. La figura 2.2 ilustra una Intranet típica. La única diferencia es que se tiene acceso a la Intranet desde fuera de la red, lo que significa que el acceso viene desde el exterior. Normalmente, sólo se utiliza dentro de la red de una compañía y únicamente acceden los empleados de la misma. A una VPN de Intranet sólo acceden los empleados, pero el acceso viene desde El exterior y no del interior.

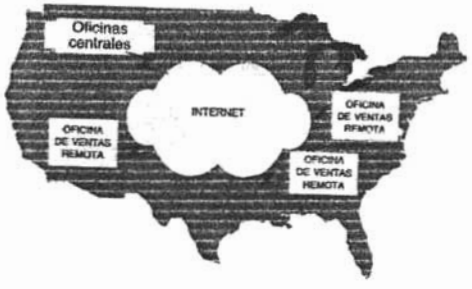


Fig. 2.2: Una VPN de Intranet.

Acceso remoto Una VPN de acceso remoto se crea entre las oficinas centrales y los usuarios móviles remotos. La figura 2.3 ilustra uno de los tipos de acceso más comunes de las VPN. Con el software de cifrado cargado en un ordenador portátil, un individuo establecerá un túnel cifrado al dispositivo de la VPN en las oficinas centrales.

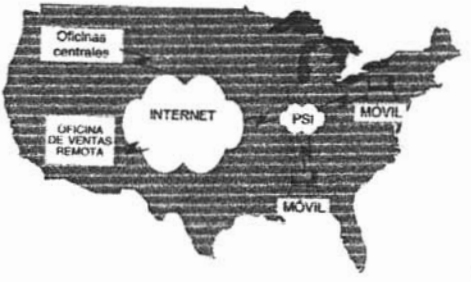


Fig. 2.3: Una VPN de acceso remoto.

Extranet Una VPN de Extranet se crea entre la empresa y sus clientes o proveedores. En la figura 2.4, la Extranet permitirá el acceso con el HTTP normal utilizado por los navegadores web actuales, o permitirá que se realice la conexión utilizando otro servicio y protocolo acordados por las partes involucradas. Aquí es donde el comercio electrónico tiene su mayor impacto. Esta configuración le dará a la empresa la capacidad para realizar transacciones de manera segura y efectiva con sus principales socios comerciales y con clientes que generan ingresos.

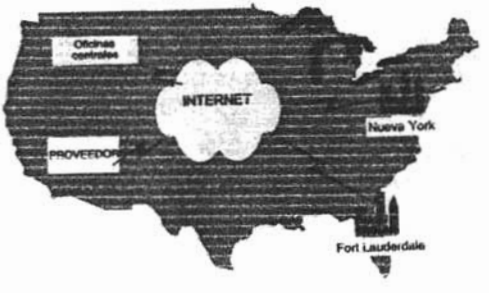


Fig. 2.4: Una VPN de Extranet.

VPN interna Una cuarta área, de la cual no hacen uso las compañías actualmente, es una VPN interna. ¿Qué motivos harán que una compañía utilice una VPN interna? Algunos de estos motivos son los estudios sobre seguridad que indican que los ataques por empleados internos ocupan el primer lugar.

El Instituto de Seguridad de Cómputo (CSI), junto con la participación de la oficina de la Brigada contra el crimen computacional internacional del FBI, de San Francisco, realiza un estudio anual de empresas, agencias gubernamentales, instituciones financieras y universidades de Estados Unidos. Los resultados del "Estudio del crimen y seguridad en computación de 1998 se muestran. En el cuarto punto que es el más perturbador en términos de pérdidas financieras debidas a empleados. Los resultados se muestran lista las pérdidas financieras de estas organizaciones. La Fig. 2.5 se muestra una VPN interna.

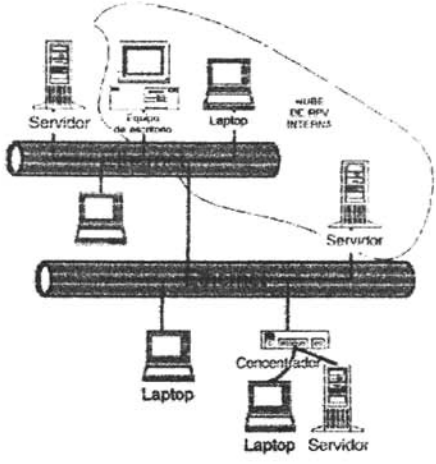


Fig. 2.5: Una VPN interna.

Con esta VPN interna, es posible que dentro de los límites de la empresa se pueda crear un túnel. Todo el tráfico que una compañía considere crítico puede pasar por un cable cifrado y almacenarse de manera segura sin que sea manipulado indebidamente. Los registros financieros, las reuniones ejecutivas y demás, pasarán de manera segura desde el origen hasta su destino en el interior de la red de una compañía.

1.2.2 Componentes de una Red Privada Virtual.

Las VPN consisten en hardware y software, y además requieren otro conjunto de componentes. Estos componentes son simples requisitos que garantizan que la VPN sea segura, esté disponible y sea fácil de mantener. Los requisitos actuales caen dentro de un rango de atributos que una organización debe considerar cuando implementa o diseña una VPN. Estos componentes son necesarios ya sea que un ISP proporcione la VPN o un cliente haya decidido instalar una por sí mismo (Brown, 2001).

Disponibilidad

La disponibilidad se aplica tanto al tiempo de actualización como al de acceso. No basta que el usuario tenga autorización para acceder a los servidores corporativos las 24 horas del día, los 7 días de la semana, si no puede conectarse debido a problemas en la red.

Lamentablemente, muchos de estos problemas están fuera de su control y a veces incluso del control del ISP local. Si utiliza una VPN de retransmisión de tramas o ATM, es probable que obtenga algunas garantías de su ISP sobre la disponibilidad, pero no sobre Internet.

Control

Algunos ejecutivos temen que si alguien más administra y controla la VPN de su compañía, hay una mayor posibilidad de brechas en la seguridad. En realidad, los servicios administrados de VPN pueden ser de gran ayuda para la compañía debido a la capacitación, experiencia, supervisión meticulosa y funciones de alerta que ofrecen algunos proveedores de servicios administrados.

Una consideración significativa es que sin importar qué tan grande sea la organización, es probable que sólo cuente con una red privada virtual; puede tener otros puntos de acceso, pero seguirá siendo una VPN corporativa.

¿Cuánto desea invertir en capacitación, certificación y equipo para que el departamento de Tecnología de información (TI) acelere la tecnología y las cuestiones de las VPN?

Compatibilidad.

Para utilizar tecnologías VPN e Internet como medio de transporte, la arquitectura interna del protocolo de red de una compañía debe ser compatible con el IP nativo de Internet. Además, debe ser capaz de interpretar los protocolos de red de la compañía al nivel 3 (el nivel de red) del modelo de la Organización Internacional de Normalización (ISO). Esto implica que una compañía debe estar al tanto del IP y saber que si los protocolos SNA o IPX están en ejecución, no se puede establecer una conexión directa a Internet, a menos que convierta primero el SNA o IPX a IP. Muchos dispositivos hacen esto, por ejemplo una compuerta, pero añaden otro nivel de complejidad a la red. Además, si va a utilizar Internet, debe usar la convención de asignación de direcciones que utiliza Internet (basada en la Estructura del direccionamiento del Protocolo Internet). Por lo tanto, si tiene una empresa que trabaje con Macintosh, se deberá traducir las direcciones de las máquinas a direcciones "públicas válidas" que utiliza Internet.

Seguridad.

La seguridad lo es todo en una VPN; nunca será suficiente hacer hincapié en ello. Una VPN *no* es la red privada de una compañía; otros pueden interceptar, recolectar y analizar los datos. No obstante, se puede tratar con las amenazas que conciernen a la seguridad. La seguridad abarca todo en una VPN, desde el proceso de cifrado que implementa y los servicios de autenticación que se eligen hasta las firmas digitales y las autoridades emisoras de certificados que utiliza. La seguridad también abarca el software que implementa los algoritmos de cifrado en el dispositivo de la VPN. Si emplea un sistema operativo basado en VPN, ¿cuáles son las partes vulnerables del mismo? Debe comenzarse a comprender que la seguridad juega un papel importante en las VPN.

Interoperabilidad.

Puesto que la tecnología VPN es relativamente nueva desde el punto de vista de la implementación, surgen muchos problemas de compatibilidad a partir de la seguridad, el usuario y las normas de cifrado. Existen muchos productos de proveedores que ofrecen hardware, software, cifrado y esquemas de autenticación para la tecnología VPN; por lo tanto, es muy difícil elegir alguno. Una consideración importante es dónde encaja la VPN en su organización ¿Se le busca una interoperabilidad usuario a usuario final, o piensa en una conectividad de VPN LAN a LAN? Tomar esto en consideración ayudará a determinar a los vendedores, fabricantes, proveedores de software e incluso los requisitos de consulta.

Asegurarse de buscar una certificación. La Asociación Internacional de Seguridad en Computación (ICSA), una compañía aseguradora de seguridad establecida en 1989, certifica productos de seguridad en computación. Su meta es mejorar la interoperabilidad de los productos de seguridad y certificarlos adecuadamente; los proveedores envían sus productos a ICSA para obtener una certificación. Las normas del Protocolo de seguridad en Internet (IPSec), las que probablemente se incluirán entre las normas de seguridad en el futuro, están certificadas por ICSA.

Misión de ICSA.

ICSA es una organización independiente que procura mejorar la seguridad y la confianza en computación global por medio del conocimiento y de la certificación continua de los productos, los sistemas y la gente. Los servicios de ICSA incluyen investigaciones relacionadas con la seguridad, publicaciones de conferencias, membresía profesional, consorcios basados en proveedores y en usuarios, así como certificaciones.

Confiabilidad.

Cuando una compañía decide instalar el producto VPN de un ISP, está a merced del ISP Una frustración que sienten los ejecutivos es que cuando se cae la red, no tienen el control para supervisar o arreglar la situación. Se resignan a sentarse y esperar a que alguien más corrija el problema. Debido al número de clientes que puede tener un ISP típico, puede pasar mucho tiempo antes de que los recursos estén disponibles para corregir el problema. Incluso cuando los problemas se resuelven, no se notifica a los clientes inmediatamente, de tal modo que se hace más grande el retraso.

Autenticación de Datos y Usuarios.

La autenticación de VPN consiste en autenticación de datos y usuarios. La autenticación de datos reafirma que el mensaje ha sido enviado completamente y que no ha sido alterado en ninguna forma. La *autenticación de usuarios* es un proceso que permite que el usuario tenga acceso a la red. Es importante que se ofrezcan ambas en cualquier tecnología VPN. Tal vez quiera que usuarios externos tengan acceso a su red interna. Esto requiere una autenticación segura y la verificación de usuarios antes de que los usuarios externos entren a la red interna.

Debe haber una manera de proporcionar una verificación adecuada para permitir el acceso interno y una autorización para permitir a los usuarios autenticados sólo el acceso a los servicios que requieran.

Sobrecarga de Tráfico.

En todo tipo de tecnologías existen sacrificios: velocidad contra desempeño seguridad contra flexibilidad. Las VPN caen en la misma categoría. Cuando se habla de tamaños de paquetes, paquetes cifrados, encabezados, etcétera , la sobrecarga entra en juego.

Si un dispositivo de la VPN cifra cada paquete que sale de los adaptadores de red, entonces puede imaginar el tipo de capacidad procesamiento de CPU que se necesita en esa máquina. Si la VPN encapsula cada paquete, puede incrementar el tamaño del paquete y por lo tanto afectar la utilización del ancho de banda.

Uno de los modos de las normas de seguridad en IPSec añade una sobrecarga a cada paquete en busca de más seguridad. Ahora experimentará cuello de botella en los enlaces; la conexión del ISP se saturará y es probable que necesite un conducto mayor. Para reducir esto, debe decidir qué tipo de tráfico necesita proteger. Las transmisiones generales, las transmisiones múltiples y el tráfico similar no necesitan cifrarse; sin embargo, necesita autenticarse. Los dispositivos de las VPN pueden agregar autenticaciones a estos paquetes sin la sobrecarga asociada al incremento del tamaño del paquete, y el receptor puede estar seguro de que los datos no han sido adulterados.

Mantenimiento.

Debe decidir qué tipo de tecnología y qué tipo de soporte necesita su compañía. ¿Usará el servicio de VPN administrada por un ISP o la construirá el cliente con los propios recursos de su compañía? Si decide implementar el cliente la VPN, ¿cuenta con el equipo de seguridad? ¿Puede responsabilizarse su departamento de Tecnología de Información de los aspectos de seguridad? La actualización en la seguridad debe ser tan preocupante como lo es la revisión del software en busca de virus: sólo es bueno hasta el último virus conocido.

Sin Repudio.

Sin repudio es el proceso de identificar positivamente al emisor de tal manera que no pueda negarlo. Esto tiene enormes implicaciones para los proveedores, mayoristas, vendedores y para los principales socios comerciales. El comercio electrónico, los documentos legales y las negociaciones financieras se basan en saber quién realiza el pedido.

Si existe aunque sea un poco de incertidumbre, una compañía no puede garantizar quien realizó el pedido. Para que el comercio electrónico en Internet se vuelva una opción viable, debe existir un proceso sin repudio.

1.2.3 ¿Quién soporta las Redes Privadas Virtuales?

Muchos ISP pequeños compiten con proveedores más grandes para ofrecer servicios de VPN. Conforme difieren las tecnologías VPN, también lo hacen las implementaciones de las redes privadas virtuales por parte de los ISP. Algunos ISP buscan solamente dispositivos de hardware para cifrado mientras que otros buscan soluciones en el software. Una diferenciación común entre los dos es que supuestamente los dispositivos de hardware para cifrado pueden cifrar y asegurar paquetes más rápidamente que los dispositivos de software. Existen algunas estadísticas en el desempeño del software que contradicen esto, por lo que no debe ser un factor decisivo. Si una compañía tiene que manejar miles de conexiones de VPN, es posible que piense en un dispositivo de hardware, pero primero debería pensar en las estadísticas sobre el desempeño del software, ya que es posible que se pague por un servicio que no se necesita (Brown, 2001).

Los ISP también experimentan con los túneles de VPN más recientes y con los protocolos de seguridad que se usarán en un futuro en Internet. Los tres principales protocolos de seguridad que existen actualmente son: el Protocolo de reenvío de nivel 2 (L2F), el Protocolo para establecimiento de túneles punto a punto (PPTP) y el Protocolo de seguridad en Internet (IPSec). Estos protocolos deben ser soportados por cualquier ISP. El Protocolo de reenvío de nivel 2 y el Protocolo para establecimiento de túneles punto a punto se habían combinado en lo que se conoce como el Protocolo para establecimiento de túneles de nivel 2 (L2TP).

Otros aspectos importantes para los clientes son el desempeño, el estado latente y la seguridad. Aun cuando muchos ISP buscan la manera de ofrecerles a sus clientes Contratos a nivel de servicio (SLA) y contratos de Calidad de Servicio (QoS), se basan en normas para los aspectos de seguridad.

1.2.4 El crecimiento de las Redes Privadas Virtuales.

Internet ha crecido más allá de las expectativas de cualquiera, y algunas estimaciones establecen que habrá más de 250 millones de usuarios dentro algunos años. Los estudios difieren de uno a otro, pero se coincide que entre 60 y 100 millones tienen acceso a internet actualmente. La alta tasa de crecimiento de internet y el número de usuarios, así como la cantidad de tráfico en el web y los registros de dominios individuales han desatado la tendencia hacia arriba de esta tasa de crecimiento. El Departamento de Comercio de Estados Unidos estimaba que para el año 2000 habría más de un millón de empresas conectadas a Internet. Esto ilustra claramente el impacto que tiene y tendrá Internet en el nuevo siglo. Se realizaron muchos estudios sugiriendo que para el cambio de siglo, entre 50 y 80 por ciento de todos los negocios utilizarían algún tipo de servicio de VPN. También sugieren que las corporaciones multinacionales de Estados Unidos con al menos 200 usuarios remotos pueden ahorrar más de $1.5 millones de dólares en 4 ó 5 años al emplear Internet en vez de líneas rentadas (Clark, 2001).

Los ISP han intentado manejar las crecientes solicitudes para el acceso a Internet con más bancos de módems y conductos con mayor ancho de banda. Desafortunadamente, incluso con esta demanda, los ISP siguen perdiendo dinero al proporcionar el acceso básico a Internet. Esto es evidente por el hecho de que muchos ISP han comenzado a cancelar su servicio de acceso mensual o de acceso ilimitado.

Siendo éste el caso, los ISP deben ir ahora tras los clientes empresariales y corporativos, y deben ofrecer lo que estos negocios pidan.

El acceso global, la investigación de mercado, las ventas, la recopilación de datos y el apoyo a clientes son sólo una pequeña parte de las solicitudes hechas por los clientes empresariales a los ISP. Los negocios requieren estos servicios, así que los ISP deben ofrecerlos. Sin embargo, estos nuevos servicios tienen un precio. Uno es el desempeño; el tráfico adicional que estos nuevos servicios generan es una pesada preocupación sobre la actualización de la infraestructura de los ISP. Otra área importante es la seguridad. Vaya a la definición previa de una VPN y vera por qué no se trata de una "red privada". Cualquiera que esté en Internet potencialmente tiene el poder de ver los datos que pasan por la red, tener acceso a ellos, modificarlos y utilizar esa información para su beneficio propio. Por lo tanto, la duda es ¿la seguridad está implementada de tal manera que sea posible hacer negocios lo suficientemente confiables como para que Internet se utilice como medio para conducir una empresa? No muchos ISP quieren tener la responsabilidad de garantizar la seguridad de los datos conforme viajan por la red. Entonces, ¿será la ocasión para que los vendedores quienes ofrecen productos para Internet, como enrutadores y los llamados cortafuegos, garanticen la seguridad? No necesariamente, pero los datos pueden protegerse al comprender los riesgos de seguridad y los procedimientos asociados para prevenirlos, además de emplear el sentido común.

Las VPN juegan un papel importante en el proceso que permite a las compañías conducir sus negocios en una forma menos cara.

Algunas de las razones por las que muchos negocios utilizarán las VPN para conducir sus negocios son las siguientes:

- Las VPN utilizan internet como su medio de transporte.
- Internet es un medio propicio tanto para clientes comerciales como privados.
- Internet se extiende por todo el mundo.
- La conductividad en Internet es extremadamente eficiente en el mercado actual, y muchos ISP procuran mantener la conexión.
- Las VPN son flexibles, dinámicas y escalables.
- Las VPN (en algunos casos) pueden utilizar la inversión que la compañía haya hecho en hardware.
- La tecnología base de las VPN es el conjunto de protocolos TCP/IP de internet, lo cual la hace más fácil de comprender e implementar que una tecnología completamente nueva.

2. Hardware de Redes Privadas Virtuales.

Uno de los mercados de mayor crecimiento para proveer soluciones VPN consiste en ofrecer soluciones VPN integradas en el hardware, las cuales en una única caja incluye toda la funcionalidad requerida para VPN, eliminando la necesidad de añadir software y hardware a un firewall existente o un router y, en la mayoría de los casos, cualquier hardware para la conexión WAN (Collado et al. 2004).

Uno de los propósitos de estos productos VPN es no cargar las funciones VPN desde un firewall o router que no tienen potencia computacional para sostener funciones como la encriptación.

No todos los productos ofrecen las mismas características. Otras soluciones VPN hardware abarcan desde cajas centradas en la encriptación hasta sistemas que sostienen todos los aspectos de una conexión a Internet, incluyendo conexiones WAN, routing, VPN, DNS, y servicios e-mail, entre otros.

Integrar varias funciones en un producto simple puede ser particularmente atractivo para los negocios que no tienen los recursos necesarios para instalar y mantener diferentes servicios de red y que tampoco quieren fuentes externas para sus operaciones VPN.

Incluso, puede resultar algo muy positivo, debido a que esta caja pasa a ser ahora el único punto de fallo. Esta acepta que todas las funciones de seguridad controlando las comunicaciones con Internet pueden fallar cuando un único servicio se cae; pero al menos, un enlace de comunicación roto no significa que los atacantes pueden entrar en la Intranet a través de ese enlace. Sin embargo, es completamente diferente poner un servidor de Redes Privadas Virtuales (VPN), correo electrónico o un servidor Web en la misma caja, ya que si ésta falla, entonces los empleados pueden perder algunos servicios internos también.

Las funciones importantes de cualquier VPN son: encriptación, autenticación, túneles, y gestión de claves. Dependiendo de qué protocolo se planee usar para la construcción de la VPN, se hace un énfasis diferente en cada una de estas funciones. PPTP, por ejemplo, se centra en tunelización e incluye encriptación débil, y L2TP soporta autenticación fuerte de usuarios; por otro lado, IPSec soporta encriptación y gestión de claves, pero todavía necesita trabajar más para ser usado con autenticación fuerte de usuario (Collado et al. 2004).

3.1 Características.

La principal diferencia entre los productos es el número de túneles simultáneos que pueden soportar y los servicios añadidos que son introducidos en los productos. Por ejemplo, el número de túneles puede variar desde 8 hasta 2000. Algunos productos incluyen gestión de ancho de banda y soporte extensivo para sistemas de autenticación de usuario, y otros productos han incluido servidores Web y e-mail (Collado et al. 2004).

Algunos de los servicios están disponibles en más de un producto. Si no se necesitan todos los servicios listados para un producto particular, es buena idea comprobar si existen soluciones parciales, es decir, productos que ofrezcan servicios separados e independientes.

Para la gestión de claves, muchos de los productos dependen de un servidor de certificados que se ha instalado en una estación Windows® o Unix® y debería ser seguro contra manipulaciones y tener un acceso muy restringido para el personal interno.

Generalmente, se espera que estas soluciones hardware mejoren las funciones VPN, especialmente la encriptación, más rápido que su software homólogo. Sin embargo, determinar el rendimiento actual de estos productos es difícil.

A pesar de que muchos de los dispositivos hardware ofrecen el mejor rendimiento posible para la VPN, es necesario decidir cuantas funciones se quieren integrar en un único dispositivo. Para pequeños negocios o pequeñas oficinas sin un número elevado de personal, especialmente aquellas con experiencia en seguridad de redes, se beneficiarían de productos que integran todas las funciones VPN así como un firewall y quizá uno o dos servicios de red. Algunos productos, normalmente los más caros, incluyen suministro dual de potencia y características de recuperación para asegurar fiabilidad. Pero se necesita determinar qué servicios de red son cruciales para las operaciones de la compañía; después de priorizar estos servicios, se puede tomar la decisión de si debería ser instalado en un único producto.

No se debe pasar por alto la importancia de integrar el control de otras funciones de red, como reserva de fuentes o control de ancho de banda. Algunas compañías ya incluyen estas características en sus productos, y es un paso que ganará mayor soporte en el futuro. Si se están buscando prestaciones, los productos hardware para VPN normalmente ofrecen un mejor rendimiento que los productos software. Las versiones más básicas de estos productos incluyen paquetes de autenticación, túneles, encriptación y gestión de claves así como los sistemas de autenticación de usuarios. Productos más avanzados ofrecen otros servicios dentro del mismo paquete y soportan miles de túneles simultáneos (Collado et al. 2004).

3.-Software de Redes Privadas Virtuales.

Se consideran dos clases de software. Una está compuesta de los productos que proveen servicios VPN para una LAN. La segunda clase de productos son aquellos que pueden ser usados para comunicación ordenador a ordenador sin la necesidad de una pasarela segura (Collado et al. 2004).

Los productos que proveen servicios VPN para una LAN cubren una completa gama de características de tunneling[6] y VPN, algunos ofreciendo soporte para protocolos Redes Privadas Virtuales (VPN) como PPTP, IPSec, ..., y otros usando características propias de tunneling y gestión de claves.

La evolución de VPN, sus requisitos de infraestructura (certificados digitales por ejemplo) y el actual mercado de las redes han hecho las soluciones LAN centralizadas más prioritarias que las soluciones ordenador a ordenador.

3.1. Características.

Las soluciones software VPN para una LAN presentan requerimientos similares a otras soluciones:

- Soporte de Protocolos: Primero, se debe considerar qué protocolos transmitirán a través de VPN sólo IP o IPX y NETBEUI, ... Muchos gateways soportan sólo IPSec, lo cual está bien para redes IP, pero que no ayudan si se trata de NetWare sobre IPX.

- Integración con Sistemas Existentes: También es necesario considerar como integrar el producto con el resto de sistemas de gestión de red y seguridad. Por ejemplo, muchos sistemas dependen de sistemas particulares para la autenticación de usuarios; si ya se está utilizando un sistema particular para la autenticación de usuarios remotos, entonces seleccionando una pasarela que es compatible con el sistema actual de autenticación, se simplificará la configuración y gestión de las pasarelas.

- Expedición de Certificados Digitales: Si se planea usar un sistema de autenticación basado en certificados digitales, entonces se debe pensar en cómo los certificados serán distribuidos y verificados.

- Mantenimiento Multisitio: Se debe considerar que, probablemente, los productos serán instalados en más de un sitio. Por este motivo es necesario mantener una política de seguridad lo más consistente posible sobre todo si el producto soporta administración sincronizada de múltiples sitios.

- Soporte de Algoritmos Criptográficos: No todos los productos soportan los mismos algoritmos criptográficos(Collado et al. 2004). Los algoritmos IPSec, los algoritmos para encriptación DES CBC y otros algoritmos de autenticación, deberían ser suficientes para aquellos usos considerados de riesgo medio; si el tráfico soportado es de riesgo alto, el producto escogido debería soportar variabilidad automática de claves, incrementando la dificultad de descifrar una clave cuando ésta es interceptada (esto es, la clave expira antes de que pueda ser interceptada).

[6] Encapsulacion de datos en paquetes Ip.

- Registro de Incidentes: Cada pasarela seguro debería tener una forma de registrar los eventos de seguridad (incidentes) e informar de ellos. Incluso, sería interesante que el sistema pudiese generar algún tipo de alarma cuando alguna actividad persistente tiene lugar.

Hay distintas razones por las que se podría inclinar por soluciones software en lugar de por productos hardware:

- Primero, el precio. Algunos de los productos software son relativamente baratos o incluso de distribución libre.

- Segundo, se puede estar familiarizado con el sistema operativo o no, en el cual se ejecuta el software, lo cual conlleva que la administración de la VPN sea más atrayente. Por último, los servicios y rendimiento de los productos software puede ser todo lo que se necesite. Si se está construyendo una pequeña VPN o bien sosteniendo pequeñas cantidades de tráfico, esto puede no requerir el rendimiento y precio encontrado en muchos de los productos hardware.

Muchos de los productos software para la creación de VPN usan protocolos propietarios y métodos no estándar de intercambio de claves, limitando su interoperabilidad. Pero, algunos de estos mismos productos han llegado a ser compatibles con IPSec, mejorando su interoperabilidad.

4. Ventajas de las Redes Privadas Virtuales.

El diseño de red es un área donde la tecnología VPN realmente puede ser benéfica desde el punto de vista de diseño arquitectónico, flexibilidad y mantenimiento.

La necesidad de un diseño WAN complejo, de cálculos del desempeño del enlace, ajustes en el tamaño de los conductos de ancho de banda redundancia, ya no representa un problema para una organización. En ese punto, la principal preocupación es la conexión a Internet de su proveedor ISP local, quien manejará todos los problemas asociados con su conexión.

Antes de Internet, una organización padecía el inconveniente de tener que diseñar e instalar un conjunto de líneas rentadas en ciertas ubicaciones. Era necesario tomar en consideración el tiempo de inactividad, los enlaces redundantes y los problemas de ampliación y desempeño. El tipo de arquitectura de línea rentada lamentablemente no se ampliaba fácilmente y era extremadamente caro. La figura 2.6 ilustra lo que tiene que enfrentar un administrador de una red típica cuando diseña una WAN sobre líneas rentadas. El administrador de red debe preocuparse por el flujo de tráfico entre departamentos ubicados en distintos puntos geográficos, edificios y ciudades, y crear el tamaño de conducto adecuado para este tráfico. Después, tiene que lidiar con las cuentas de acceso de los usuarios remotos por marcación y la carga adicional de instalar enlaces redundantes en caso de que el enlace de comunicación principal falle (Brown, 2001).

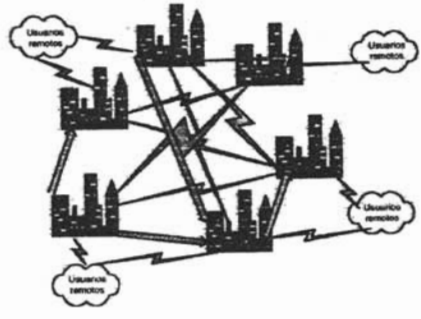


Fig. 2.6: Diseño de una WAN.

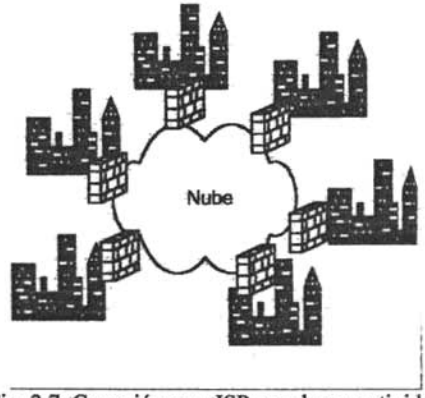


Fig. 2.7: Conexión a un ISP para la conectividad de una WAN

Con la arquitectura VPN, todo el trabajo se redujo. Como se muestra en la figura 2.7, todo lo que se requiere es una conexión a Internet, y él se encarga del transporte. Ahora la red WAN puede ser escalable, redundante y estar basada en normas (TCP/IP), y soportar capacidades de administración distribuidas.

4.2. Administración Centralizada.

Algunos proveedores soportan la característica de administración centralizada para sus productos VPN. Esto representa tanto una característica de seguridad sólida como un excelente mecanismo para solucionar problemas. Suponiendo que se tiene ocho sitios distintos todos conectados a Internet y todos protegidos por una combinación cortafuego/VPN o por algún otro dispositivo VPN, como se muestra en la figura 2.8.

Si surgiera un problema al conectar una aplicación de una máquina cliente en un departamento a un servidor en otro departamento a través de la VPN. Las dificultades surgen cuando se trata de involucrar al personal de varios departamentos de información y coordinar algún tipo de proceso de diagnóstico para resolver el problema de una manera oportuna (Brown, 2001).

Fig. 2.8: Estación de administración centralizada.

Al tener un proceso de administración centralizado, se eliminan todos los problemas de coordinación. Todo lo que se necesita es tener en línea al usuario final y al técnico de la VPN; y al monitorear ambos extremos de la VPN, se puede comenzar a aislar el problema con facilidad.

Contar con esta característica de administración centralizada simplifica en gran medida los procesos de mantenimiento y la solución de problemas infraestructura de la VPN. Elimina la necesidad de personal de varios departamentos de información y reduce sus cargas de administración.

4.1. Beneficios de las Redes Privadas Virtuales para el Usuario Final.

Los negocios actuales deben ir a donde esté el cliente, ya sea que esté en la puerta de al lado o al otro lado del mundo. Esto añade una carga a la organización puesto que demanda una fuerza de trabajo móvil y geográficamente dispersa, lo cual significa que se requiere acceso día y noche para estudiar informes de los perfiles del cliente, desarrollar presentaciones e investigar clientes potenciales; sin importar si son las 14:00 horas en Nueva York o las 5:00 horas en Tokio, el acceso a la red debe estar disponible. Con el acceso a del ISP y la tecnología VPN existe la oportunidad de cerrar tratos, verificar contratos, etcétera.

Debido a que la compatibilidad es un problema importante diferentes protocolos de red, debe haber una manera de superar esto. Internet ha resuelto este problema. Técnicamente es *una* red que utiliza *un protocolo* que se inventó hace 30 años y ha resistido los análisis científicos lo cual hace que sea confiable para las necesidades de los negocios (Brown, 2001).

4.3.1. Pagar Solo lo que se Requiere.

Además de los costosos cargos telefónicos de larga distancia en los que se incurre, están los costos de las sucursales y las oficinas remotas. Con líneas rentadas, retransmisión de tramas u otra infraestructura, se tiene que pagar por el tiempo de inactividad. Aun si no está utilizando el conducto, se está cobrando. En el caso de Internet, sólo se paga por el tiempo en línea, lo cual generalmente consiste en una llamada local además de una cuota mensual. Esto genera grandes ahorros para una oficina pequeña que tiene que pagar sus propios costos de telecomunicaciones.

4.3.2. Acceso a Datos.

En un escenario normal, un proveedor necesita una propuesta, un contrato u otro documento como presentación ante el cliente. Comúnmente debe marcar a la red corporativa y acceder a alguna Intranet. Con la VPN instalada puede establecer una conexión directa al servidor en cuestión y transferir el material apropiado, eliminando la necesidad de preguntarle al cliente potencial si tiene una línea al exterior que pueda utilizar para establecer una conexión por marcación. Las VPN también ofrecen al usuario remoto diferentes tipos de acceso hacia la organización, a través de diferentes aplicaciones.

4.3.3. Asignación de Prioridades de Tráfico.

Varios proveedores ofrecen asignación de prioridades de tráfico a través de sus productos VPN. Esto añade gran flexibilidad a la utilización de tráfico de una compañía mediante su enlace con Internet. Ya que las VPN ofrecen acceso a una Extranet, a una Intranet o a servidores internos de una organización, es posible decidir que sólo se permita pasar libremente cierto tipo de tráfico, con el fin de conservar el ancho de banda, mientras que otro tipo de tráfico queda en cola de espera, según su importancia. En las instalaciones de ciertas topologías se puede dirigir todo el tráfico de la VPN a través de un enlace y todo el tráfico que no es de la VPN a través de otro. Tener este tipo de flexibilidad es una característica, considerando cuánto poder de procesamiento de CPU se requiere para examinar cada paquete.

4.4. Beneficios de un Alcance Global.

Con Internet se obtiene el acceso global que permite que cualquier usuario en el mundo se conecte a la LAN de una compañía, siempre y cuando exista un proveedor ISP en esa área.

Esto hace que una organización pueda extender su presencia en todo el mundo y vender sus productos a cualquiera que pueda desearlos, lo cual brinda a las pequeñas empresas una enorme oportunidad de crecimiento y a las grandes empresas un alcance aún mayor. Debido a que el presupuesto de los departamentos de mercadotecnia de muchas organizaciones pequeñas es fijo, Internet permite que estas compañías tengan un mercado potencial de 5 mil millones de personas. Lo que es más excitante es que Internet todavía es una Internet americana; esto no significa que Estados Unidos la controle, sino que la utiliza en su mayor parte. Con el crecimiento de otros países en Europa, Asia y América, Internet será extremadamente importante en el siglo veintiuno.

4.4.1. Teleconferencias.

Aunque hoy en día esta tecnología tiene mucha demanda, no se utiliza sobre Internet como podría hacerse. Esto se debe principalmente a los problemas en el desempeño. La teleconferencia continuará creciendo, y los ISP tendrán una demanda creciente para proporcionaría.

Si bien es cierto que un cliente no podrá disfrutar la teleconferencia desde cada oficina pequeña en todo el planeta, contará con la capacidad de establecer una teleconferencia en puntos estratégicos a través del mundo, ahorrando tiempo y dinero. Aquí es donde se establecerán sociedades estratégicas entre organizaciones e ISP que tienen un alcance global y que pueden ofrecer algún tipo de calidad de servicio. Cuando un ISP puede ofrecerle a una organización garantías de algún tipo de calidad de servicio entre varias ciudades importantes en el mundo, ese ISP se volverá un socio. Debido a que la organización dependerá de él para proporcionar la infraestructura de red que demanda la teleconferencia, no se arriesgará a utilizar otro ISP para enviar el tráfico en ruta hacia su destino.

4.4.2 Telefonía IP.

Mientras que hoy en día la telefonía IP no tiene tanta demanda como la teleconferencia, es un servicio de rápido crecimiento que demandará el mismo tipo de garantía de calidad que demanda la teleconferencia. La curva de crecimiento potencial de la telefonía IP probablemente aventaja a la curva de la teleconferencia debido a los ahorros en el costo que pueden lograrse utilizando a Internet como un medio de comunicación en las llamadas diarias.

4.5. Beneficios para los ISP.

Los ISP pueden disfrutar de los beneficios de la tecnología VPN. Serán capaces de ir al encuentro de sus clientes con todos los tipos de servicios que demandan los negocios actuales. En un futuro próximo, las compañías telefónicas cobrarán por el paquete y eliminarán las llamadas locales gratuitas. Esto es inevitable debido a las leyes de desregulación que se están aprobando en el territorio de Estados Unidos por el Congreso de ese país. Los ISP harán lo mismo cobrando a sus clientes de negocios una cuota basada en paquetes. Además, los ISP ofrecerán protección de cortafuegos, consultas para el usuario final, y diseño y administración de las redes de sus clientes.

Actualmente, las compañías de mayor tamaño ya ofrecen estos servicios, así que las compañías pequeñas seguirán su ejemplo. Más del cincuenta por ciento de los proveedores de red ofrecen algún tipo de servicio de VPN (Clark, 2001).

4.5.1. Negocios Nuevos.

Conforme Internet se convierte en un transporte para comercio global, la conexión a Internet de las empresas se volverá extremadamente importante. Las asociaciones de negocios entre las compañías y sus proveedores de ISP se volverán comunes. Lo más probable es que se establezcan alianzas entre las organizaciones que necesitan acceso global y los ISP que pueden proporcionar ese acceso. Además, conforme las nuevas tecnologías de Internet se vuelvan más comunes e Internet2 comience a funcionar, los ISP comenzarán a ofrecerles a sus clientes nuevos productos y servicios, precisamente de la misma manera en que las compañías telefónicas ofrecen servicios adicionales a sus clientes, como las llamadas en espera e identificador de llamadas.

4.5.2 Servicios Administrados.

Entre más y más complicadas se vuelvan las redes, las organizaciones comenzarán a agrupar la administración de sus redes. Puesto que algunas de ellas contratan servicios de consultoría externos, las tecnologías de conectividad en red que están siendo desarrolladas cambian demasiado rápido para que cualquier organización pueda mantenerse actualizada.

Con el uso de las VPN, la seguridad se volverá crítica y muchas organizaciones decidirán dejarla a los profesionales. Los ISP que tengan mucha experiencia en seguridad y en redes, y que tengan las capacidades de red requeridas por las compañías, tendrán gran demanda por parte de los clientes que desean un proveedor único para satisfacer todas sus necesidades de conectividad en red.

4.5.3. Internet como Ventaja Competitiva.

Internet es una herramienta de Ventaja Competitiva. Si la misión es ofrecer el servicio de Internet más rápido y menos costoso para una compañía entre dos puntos, entonces es posible que Internet y las VPN sean herramientas de Ventaja Competitiva. En cualquier decisión de administración sana, una compañía debería esforzarse por proporcionar un producto de calidad en un tiempo razonable (Clark 2001).

5. Desventajas de las Redes Privadas Virtuales.

5.1. Infraestructura de Red del ISP.

¿Por qué la infraestructura de red del ISP añadirá un costo adicional a una compañía?
Obsérvese las figuras 2.6 y 2.7; todos los puntos de acceso de infraestructura de red corresponden al ISP que proporciona la conexión a Internet. No obstante, la figura 2.8 revela un problema potencial. ¿Cuántos puntos de entrada se desea tener en una organización?

Desde el punto de vista de la seguridad, debería tener uno, pero desde un punto de vista realista relacionado con el trabajo, no puede pagarse el costo de tener sólo uno. La figura 2.8 muestra una sola forma de llegar a la organización.

Si el enlace a Internet falla, la red queda aislada. Si un ordenador esta fuera de la red, ningún trabajo se terminará en esa estación; el usuario necesitará moverse a otra estación.

Muchas Organizaciones que utilizan internet para el comercio experimentan este mismo tipo de problema. La figura 2.9 ilustra lo que tiene que hacer una compañía en caso de falla importante de su enlace a Internet. Deberá tener ya sea un enlace secundario o algún tipo de equipo de acceso remoto para dirigir los negocios. Aquí es donde se comienza a ver los costos adicionales; no es que la tecnología le cueste más dinero a la compañía, sino que la compañía no está en condiciones de pagar por el tiempo de inactividad (Clark, 2001).

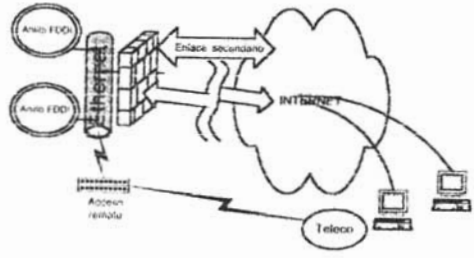


Fig.2.9: Falla del enlace principal.

5.2. Equipo de VPN.

¿De dónde viene todo este equipo y cuánto cuesta? Se está añadiendo equipo muy complejo a la red de una corporación.

Puede tratarse de una configuración independiente o de alguna otra combinación que utiliza otros tipos de equipo, por ejemplo, un dispositivo VPN con un servidor RADIUS de autenticación de usuarios. ¿Va a colocarse este equipo en una subred o en una red nueva? ¿Qué hay respecto a añadir equipo para Servicio de Acceso Remoto (RAS). Los usuarios necesitarán alguna manera de establecer su autenticación y de obtener autorizaciones ¿Se utilizará el RAS de un proveedor o tiene alguna máquina interna que ejecute algún tipo de base de datos de usuario? ¿Existe algún otro tipo de hardware y/o software que se añadirá, como enrutadores, concentradores, cableado y CSU/DSU Ahora multiplíquese esto por el número de sitios que tienen y se podrá obtener una cifra aproximada de los costos capitales.

Costos de Mantenimiento.

Al igual que con otro equipo de hardware que se tenga, es muy probable que se cuente con contratos de mantenimiento para este equipo. Se pueden seleccionar contratos para hardware, software, o para ambos.

¿El contrato de mantenimiento incluye características de actualización gratuitas? Se habla de características de interoperabilidad con las futuras normas de seguridad IPSec, PPTP y L2TP para las VPN de Internet. ¿El contrato de mantenimiento cubre estas actualizaciones y cuando están disponibles? (Brown 2001)

Una preocupación importante será el tiempo de inactividad. ¿Cuánto tiempo le tomará a un proveedor reparar o remplazar el equipo y a qué precio? La porción del gasto será insignificante comparada con el costo de no poder realizar los negocios. Pero esto conlleva a una consideración importante; cada proveedor ofrece líneas de contratos de mantenimiento, con precios variables. Normalmente van desde 4 horas a 24 horas y pueden abarcar los fines de semana. Cada uno de estos tipos de contratos tiene una escala de precios distinta; por lo que se trata de otro gasto en que se incurre con el uso de esta tecnología.

Licencias.

Otro aspecto de las VPN son las licencias; algunos proveedores no implementan esta característica, otros la agregan a sus productos de cortafuego y algunos las incluyen sobre la marcha. Las licencias no son las mismas para todos los productos; para ciertos proveedores, significan el número de usuarios simultáneos que pasan a través de un dispositivo de red. Mientras que algunos añaden una cuota de licencia simple a un enrutador, lo cual permite conexiones VPN ilimitadas, otros basan sus cuotas de licencias en el número de túneles que se pueden crear. Si se sabe para qué se va a utilizar la VPN, se puede calcular el número de usuarios, túneles, etcétera. que serán necesarios. Hay que al menos asegurarse de obtener un contrato de licencia que pueda ampliarse. No debe comprarse una licencia para servidor de alto desempeño cuando sólo puede obtener una licencia para 1000 usuarios (Brown, 2001).

Costos de la Solidez del Cifrado.

Qué problemas podrían acarrear los costos de la solidez del cifrado de las VPN y por qué afectarían a una compañía como una organización. ¿Dónde están los costos adicionales en que se incurre con la solidez del cifrado? Cuando se habla de cifrado, los gobiernos regulan los algoritmos de cifrado utilizados, ya que los consideran un tipo de arma. Por lo tanto, el algoritmo de cifrado en sí no es la causa del costo adicional, sino más bien son los procesos que se deben llevar a cabo para resolver los problemas de seguridad potenciales relacionados con la interferencia del gobierno. La Fig. 2.10 ilustra el problema con distintas características de solidez del cifrado.

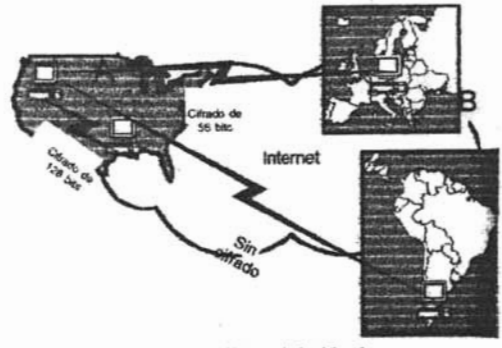


Fig. 2.10: solidez del cifrado.

Esta figura muestra las características de solidez del cifrado para ciertos países que están proyectados bajo las leyes de control de exportación de Estados Unidos y la solidez de entrada permitida en los países receptores.

Comenzando con la terminal en la parte alta del noroeste de Estados Unidos, se puede ver que deben usarse diferentes características de solidez del cifrado para cada país. Son las siguientes:

- Solidez del cifrado de 128 bits o ilimitado en comunicación interna. El gobierno de Estados Unidos no regula la solidez del cifrado que se usa internamente.

- Cifrado DES de 56 bits entre Estados Unidos y el Reino Unido. Estados Unidos transigió al facilitar su política DES de 56 bits, y es muy probable que el Reino Unido siga sus pasos.

- Sin cifrado para Sudáfrica. *En 2001*, los algoritmos de cifrado de cualquier tamaño eran ilegales para usarse en este país.

Administración.

Alguien tendrá que responsabilizarse de la supervisión y del mantenimiento de la VPN, ya sea el propietario o el ISP. Si el ISP provee un servicio de administración entonces éste se incluye en la tarifa por el servicio. En la mayoría de los las actualizaciones normales y las actualizaciones de correcciones puede manejarse vía telefónica si el dispositivo VPN es un dispositivo de sistema operativo como UNIX® o un tipo de enrutador. Con los dispositivos de hardware generalmente existe un disco flexible que se carga en el dispositivo, de tal forma que al encender el hardware se instalará la nueva revisión. En cualquier caso, sólo se requiere un poco de coordinación ya que probablemente se necesitará reiniciar el dispositivo (Clark, 2001).

Si el personal interno está manejando las tareas administrativas debe disponer de los procedimientos de administración para este nuevo hardware. Si se están instalando estos dispositivos en varias ubicaciones, se necesitará administrarlos en forma remota. Los dos tipos de acceso que se requerirá son los siguientes:

- *En banda.* Aquí es donde se puede crear un túnel de administración cerrado entre los dispositivos VPN de tal forma que pueda administrarlos remotamente a través de Internet.

- *Fuera de banda.* Esta configuración coloca un módem de cifrado en los puertos de consola de los dispositivos VPN en diferentes ubicaciones. Se necesitara tener esta configuración en caso de que no pueda tener acceso en banda a un dispositivo VPN.

Personal de Seguridad.

Este costo adicional será uno de los mayores desembolsos de la compañía en términos de recursos técnicos y financieros requeridos para implementar y vigilar la tecnología VPN. El aspecto de la seguridad de la VPN recae en la solidez del algoritmo de cifrado en el que se basa. Si se implementa esta tecnología personalmente, se debe estar seguro de que se está implementando los algoritmos de cifrado más sólidos disponibles.

Si una organización opta por una solución VPN administrada por parte de un ISP, las responsabilidades de seguridad no han cambiado, sólo se han reducido. El ISP no será el consultor en seguridad; la responsabilidad de éste recae sólo en administrar la infraestructura instalada. La organización decidirá las políticas de seguridad corporativas y el ISP las implementará. De acuerdo, los ISP ayudarán a definir las políticas de seguridad y harán recomendaciones, pero no dirán qué es lo más adecuado para la organización. Por lo tanto, se necesitarán algunos técnicos que se responsabilicen de definir las políticas de seguridad de la compañía y que actualicen los cambios a esa política.

6. Comparación de los VPN con las Tecnologías Convencionales.

Otra forma de aproximarse a las VPN es comparándolas directamente con otras tecnologías.

6.1. Las VPN Frente a RAS.

Actualmente, muchas empresas están intentando ser flexibles en lo que se refiere a los organigramas de personal. Poder trabajar desde casa es una opción muy atractiva para mucha gente, especialmente si son padres solos o viven a gran distancia de la oficina (Fowler,1999).

Además, muchas empresas necesitan una fuerza de trabajo móvil. El personal de ventas y los ingenieros de mantenimiento necesitan viajar para realizar su actividad. Tradicionalmente, sólo hay dos opciones posibles: abrir los recursos de la Intranet al mundo exterior o mantener un grupo de módems a través de los cuales puedan conectarse los usuarios. Ambas soluciones tiene desventajas importantes.

Proporcionar recursos por Internet significa que dichos recursos están disponibles para todas las personas que están en Internet, no sólo para los usuarios a los que están dirigidos. Esto puede significar riesgos de seguridad serios. Si los recursos están comprometidos, podrían verse afectados por la revelación no autorizada de secretos comerciales, de información registrada y de la propiedad industrial. No sólo eso, si hay relaciones de confianza entre servidores, un servidor comprometido puede infectar a los demás. Desde una perspectiva empresarial, esto se traduce en pérdidas financieras exponenciales (González et al, 2004).

Si al contrario se opta por mantener un grupo de módems, los costos se pueden disparar rápidamente. Los servidores PPP, los módems, las placas multipuerto, las líneas telefónicas, las llamadas a larga distancia y los costes de administración aumentarán. Además, se podría ser víctimas de una guerra de marcación telefónica, un método que todavía está en práctica que podría comprometer la red interna. Nuevamente esto podría constituir pérdidas financieras para la empresa.

6.2. Las VPN Frente a Líneas Dedicadas.

Cuando se conectan redes geográficamente distantes, lo normal es utilizar líneas dedicadas. Aunque el nombre puede llevar a cierta confusión, las líneas dedicadas pueden ser cualquier cosa, desde las tradicionales T (T1, T3 o análogas europeas, E), líneas OC (OC3, OC12, OC48, OC192) o enlaces inalámbricos (microondas, RF o satélite). Las líneas están "dedicadas" porque el ancho de banda que proporcionan es de su propietario. Las líneas dedicadas son buenas para algunas aplicaciones. Se tiene una base de datos esencial para el funcionamiento del negocio que necesita mucho rendimiento, una línea dedicada podría ser una buena elección porque ofrece un ancho de banda garantizado (Gonzáles et al. 2004).

Además se puede negociar líneas dedicadas según el rendimiento que se necesite. Si se estuviera en Nueva York, probablemente no se daría cuenta de que el servidor de bases de datos está en San Francisco, si utilizamos una OC-3. Otra ventaja de la líneas dedicadas es que siempre están (o deberían estar) disponibles. Como controlamos el equipo que mantiene la conexión, se tiene un control razonable sobre ella. Esto no siempre es así, porque estas líneas normalmente pasan por una nube WAN; sin embargo, la nube WAN está muy controlada y normalmente tiene enlaces redundantes con capacidad de recuperación automática ante fallos. La probabilidad de que se experimente una caída como resultado de una falla de una nube WAN es relativamente baja. Si la base de datos se replica regularmente, se necesitará consultas constantes o actualizaciones cada 24 horas, por lo que probablemente se debería optar por una línea dedicada.

Aunque una línea dedicada tiene ventajas en determinadas situaciones, puede ser muy costosa. Dependiendo de donde se este, una simple T1 puede constar más de 5000 dólares por la instalación, 2500 dólares al mes por el servicio y 5000 por el CPE (Customer Premise Equipment, equipo terminal del cliente). Sólo el primer año, podría llegar a 40000 dólares, y esto sin contar los costos de personal, de equipo, etcétera.

A todo esto se debe añadir el coste de la conexión a Internet. Reacuérdese que este cálculo sólo tiene en cuenta la conectividad entre dos redes, más redes equivalen a más costos.

Se confía en los ISP y en las empresas de telecomunicaciones en lo que respecta a la conexión a Internet, pero no se debería hacer. Ellos tienen un acceso completo a los datos que atraviesan sus líneas. ¿Qué evita que uno de los empleados haga "sniffing" de los datos? Muchos proveedores de servicios tienen "sniffers" en sus redes a efectos de solucionar problemas, pero ¿operan los "sniffers" éticamente, teniendo la confidencialidad de los clientes como una de sus prioridades principales? Si se necesita confianza absoluta en las comunicaciones entre dos puntos, el proveedor de servicios no es una buena solución.

Arquitecturas y Topologías.

Capítulo III. Arquitecturas y Topologías.

1.-Introducción a la Arquitectura.

Existen innumerables opciones para la instalación de las VPN, desde las independientes basadas en caja negra y las VPN basadas en enrutador hasta las VPN basadas en software y en cortafuego. Además de estas arquitecturas, existe una amplia variedad de servicios y características que pueden implementarse en estos dispositivos (Scott et al. 1999).

1.1 VPN Proporcionada por un Proveedor de Servicios de Red.

Ésta puede ser una manera fácil y eficiente de conectar una organización a Internet y disfrutar los beneficios de una VPN. El proveedor de servicios de red establecerá un dispositivo en las oficinas de la compañía el cual creará el túnel de VPN. Aunque, esto no es un requisito absoluto; algunos ISP pueden instalar un conmutador PPTP frontal en las oficinas, el cual creará en forma automática los túneles de VPN para su tráfico. El destino final de las comunicaciones descifrará los paquetes y entregará los datos a su anfitrión.

También se podría agregar un cortafuego a este tipo de ambiente, por lo general justo enfrente de un dispositivo de red o entre ellos. De manera similar a la vieja forma de instalar una DMZ, el enrutador interno se conecta a un puerto del cortafuego, el otro puerto del cortafuego se conecta al enrutador externo y el puerto serial del enrutador externo se conecta al ISP. También debe encargarse de asuntos tales como el direccionamiento IP, el enrutamiento y el correo. La Fig. 3.1 ilustra una solución VPN de un proveedor de servicios de red común.

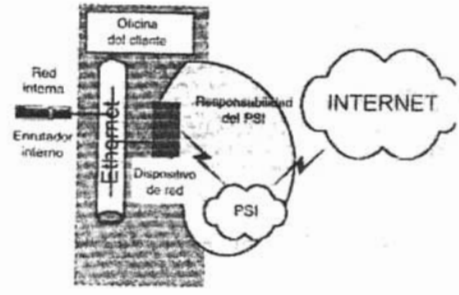


Fig. 3.1:VPN proporcionada por el proveedor de servicios de red.

El ISP instalará un dispositivo en la red o tendrá un conmutador de VPN frontal en las oficinas para crear el túnel de VPN. Si el dispositivo está en el mismo establecimiento, es más probable que se trate de un dispositivo basado en sistema operativo, como un servidor UNIX® o una caja negra, ya que esto permite la administración remota de ese dispositivo.

Un criterio aquí es definir quién se hace cargo de cada responsabilidad. En la Fig. 3.1 las líneas de responsabilidades están claramente definidas. El proveedor de servicios se encarga del equipo asociado con las comunicaciones de ese dispositivo. Observe la figura 3.2; se ve un escenario diferente. Se ve un límite borroso entre las líneas de responsabilidades. Esto debe hacer que se tomen mejores precauciones al responder a los cortes de comunicación.

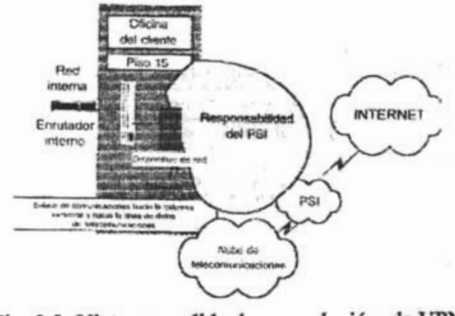


Fig. 3.2: Vista expandida de una solución de VPN proporcionado por ISP.

1.1.1 Seguridad.

El proveedor de servicios de red no será el responsable de la seguridad, aun proporcionando el equipo. La seguridad de las VPN se basará en normas aceptadas por la vasta comunidad de la sociedad Internet. Los ISP primero proporcionan servicios de Internet y en segundo lugar servicios de VPN, pero son las acciones de los usuarios las que podrían haber ocasionado problemas en la seguridad. Supóngase que se desea un túnel de VPN hacia un sistema heredado antiguo. El acceso está garantizado y el usuario aplica un viejo truco para ganar privilegios de administrador en ese dispositivo. ¿Es su culpa, ya que se permitió la comunicación? o ¿es del ISP por no decirle que no debía permitir esos tipos particulares de servicios hacia ese dispositivo? Después de todo, están proporcionándo una solución de VPN; deberían ser expertos. En este caso se deberá contratar un equipo de seguridad externo para formular esa política de seguridad y hacer que el ISP la implemente.

1.1.2 Control de Cambios.

Se necesita saber quién hace los cambios en el control de la política de acceso y cuánto le toma implementar estos cambios. El proveedor puede estar disponible o puede estar ocupado resolviendo los problemas de otro cliente. Sería prudente que de darse cuenta de que se requiere un poco de tiempo para realizar un proceso de control de cambios. Pueden pasar meses antes de que se decida añadir otro servicio. Los cambios que solicite serán para
accesar a un servicio o a un destino en particular, lo cual puede ser otorgado arbitrariamente por el administrador. Por lo general toma días el simple hecho de obtener los permisos necesarios. Después, para rastrear el control de cambios, normalmente deberá llenar algún formulario para notificarle al proveedor de servicios administrados que se está a punto de cambiar algo a través de la solicitud.

1.1.3 Solución de Problemas.

En cualquier tipo de escenario de VPN, cuando las cosas van mal u ocurren problemas o, cuando se desarrollan problemas intermitentes, los problemas intermitentes son los más difíciles de diagnosticar; ocurren, desaparecen y luego vuelven ocurrir. Se reúne a un equipo técnico y a los consultores, pero si el problema no se manifiesta por sí mismo o si ellos no han visto un problema similar podrían pasar semanas antes de resolverlo. Aun supervisando, el tráfico analizando los datos; no siempre se revela la causa. Se necesita seguridad de que en el contrato se detalle con claridad la disposición del ISP para invertir tiempo en resolver el problema y en diagnosticarlo sin importar cuánto tiempo se requiera. Por supuesto, esto se añade en el costo del contrato.

1.1.4 Características.

Las características son una consideración muy importante si la organización gusta de probar nuevas tecnologías. Si una compañía desea utilizar Internet para las teleconferencias o emplear la telefonía IP, realmente debe discutirlo con el proveedor. Si su compañía decide que necesita una configuración diferente de la que se implementó originalmente. El ISP es responsable de cientos de cuentas y tratará de ofrecerle un servicio completo, pero debe ser responsable por el servicio de la mayoría. Es posible que no se le permita implementar una aplicación específica. La redundancia, la tolerancia frente a las fallas, y la sincronización son sólo algunos de los casos especiales.

1.1.5 Autorización.

Una compañía necesita saber cómo y cuando se añadieron usuarios a una base de datos lo cual les permitirá crear el túnel de VPN hacia su organización. Estando la base de datos en el dispositivo VPN del proveedor o en algún servidor interno bajo su control se puede obtener acceso a él y, de lo contrario, se requiere tiempo para que una autorización del usuario se vuelva efectiva.

Esto es importante en el caso de un empleado despedido; si un empleado deja la compañía es muy importante que su acceso se restrinja de inmediato, no después de un día. De lo contrario, llegaría una mañana y encontraría que esa persona estuvo conectada la noche anterior a uno de sus servidores. En situaciones como ésa es imperativo que se tenga ya sea acceso inmediato a la base de datos para revocar los privilegios de acceso o que cuente con una manera de contactar al proveedor en forma inmediata para llevar a cabo esta tarea.

1.1.6 Utilización de la Red.

Es importante estar consciente de cómo funciona la red en general. El propietario o el ISP deben vigilar el enlace para el uso del tráfico en el ancho de banda. Aun si el propietario tiene una VPN manejada por un proveedor de servicios, esto no necesariamente le garantiza que el proveedor instalará capacidades de supervisión de red para su compañía. No obstante, la mayoría de los ISP sí ofrecen algún tipo de servicios de supervisión de VPN.

La organización, como muchas otras, se conectará a la VPN y se olvidará de ello. Después comenzará a crecer y a requerir más servicios de VPN, lo cual aumentará el ancho de banda. Se necesitara una manera de implementar un análisis de tendencias en esos enlaces y deberá estar listo para una actualización mucho antes de que se necesite.

1.1.7 Utilización de Dispositivos.

Los dispositivos VPN son justo como cualquier máquina o pieza de software ubicada en alguna parte de una organización. Alguien tendrá que observar el desempeño, vigilar su salud y prevenir los problemas. Es conveniente recordar que, las máquinas no pertenecen a la compañía. Por consiguiente, no se pueden controlar. El tráfico diario, el número de usuarios y procesos de administración de claves y de cifrado consumen bastantes recursos del CPU. Debe conocerlos con el fin de actualizarlos cuando sea necesario.

1.1.8 Aplicaciones Cliente.

Con el fin de que los ordenadores portátiles creen un túnel de VPN, es necesario instalar software especial en ellas. Se deben preparar a todos los ordenadores portátiles, equipos de escritorio y demás, y darles mantenimiento. Comprando un servicio de VPN es una de esas áreas grises de las cuáles tendrá que responsabilizarse la organización. Sería imposible para el ISP lograra esta tarea, pero una vez que haya cargado el software, él le ayudará a resolver los problemas de conexiones al dispositivo VPN. El principal problema ocurre si ya existe software cargado en esas máquinas y crea conflictos con el software.

1.1.9 Administración de Claves.

En cualquiera de las ofertas de VPN por parte de los ISP o en las diferentes arquitecturas de VPN, la seguridad de las claves es un asunto de suma importancia. Al igual que en cualquier procedimiento de respaldo/restauración que tenga una compañía, las claves de la VPN deben ser parte de un procedimiento rutinario. No se trata de la generación y el mantenimiento de las claves, sino de dónde obtenerlas si requiere duplicarlas. En estas arquitecturas, las claves generadas y administradas deben guardarse en un lugar seguro, no sólo para propósitos de seguridad sino también para recuperarlas. Éstas incluyen claves públicas, claves de dispositivo y cualquier certificado del que se sea responsable.

1.2 VPN Basadas en Cortafuego.

Las VPN basadas en cortafuego probablemente sean la forma más común de implementación de VPN hoy en día, y muchos proveedores ofrecen este tipo de configuración. Esto no significa que las VPN basadas en cortafuego sean superiores a otras formas de VPN, sino más bien se trata de una base establecida a partir de la cual se puede crecer. Actualmente es difícil encontrar una organización conectada a Internet que no utilice algún tipo de cortafuego. Debido a que estas organizaciones ya están conectadas a Internet, todo lo que se necesitaría es añadir software de cifrado.

Lo más probable, si una organización ha adquirido recientemente un cortafuego, es que incluya la capacidad para implementar tecnología de cifrado de VPN. Por tecnología VPN se hace referencia a algún tipo de esquema de cifrado proporcionado con el dispositivo.

Si se desea un esquema de cifrado distinto, lo más probable es que se necesite comprar alguno. Muchos proveedores incluyen su tecnología de cifrado propietaria sin costo adicional con el producto (Brown, 2001).

Existen muchos proveedores entre los cuales elegir cuando se considera una VPN basada en cortafuego, y los productos están disponibles en todas las plataformas. Un aspecto importante de la seguridad es el sistema operativo subyacente. No existe un dispositivo que sea 100 por ciento seguro, así que al crear la VPN en ese dispositivo, necesitará asegurarse de que el sistema operativo subyacente sea seguro. Si se observa la figura 3.3 podrá verse por qué la tecnología VPN debería ubicarse en el nivel más bajo de la pila de OSI. Entre más arriba se encuentre en la pila, se presentarán mayores oportunidades de que ocurran intrusiones en la seguridad de las capas inferiores de las que depende. La Fig. 3.4 ilustra una VPN basada en cortafuego.

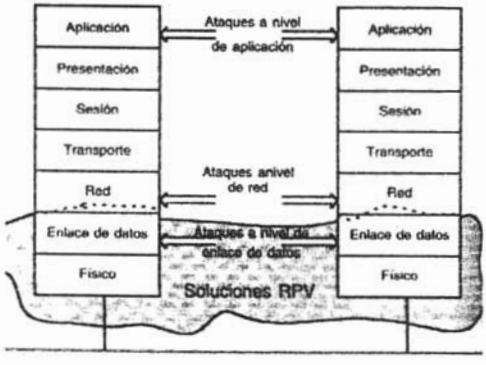


Fig. 3.3: Topología VPN en la pila de OSI.

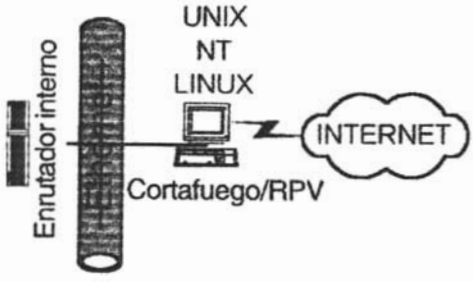


Fig. 3.4: VPN basada en Cortafuegos.

Aunque esta figura ilustra un producto VPN basado en cortafuego sencillo, su implementación no es tan simple. La mayoría de las organizaciones tiene instalados estos sistemas, así que añadir el software de VPN no es muy difícil.

Se debe decidir qué tipo de Norma VPN se desea. Ya sea la norma PPTP, L2TP, o IPSec que aún está siendo desarrollada

1.3. VPN Basadas en Caja Negra.

En el escenario de caja negra, un proveedor ofrece exactamente eso, una caja negra. Se trata básicamente de un dispositivo cargado con software de cifrado para crear un túnel de VPN. Algunas cajas negras vienen con software que se ejecuta en un equipo cliente de escritorio para ayudar a administrar ese dispositivo, y otras pueden configurarse a través de un explorador web. Se cree que estos tipos de dispositivos de cifrado de hardware son más veloces que los tipos de software, ya que crean túneles más rápidos bajo demanda y ejecutan el proceso de cifrado con mayor rapidez. Aunque fuera verdad, no todos ofrecen una característica de administración centralizada, y por lo general no soportan el acceso a si mismos; es necesario enviar estos accesos a una base de datos para consultas. También se requiere otro servidor si se desea llevar a cabo la autenticación, aunque algunos dispositivos permiten añadir usuarios si así lo desea (Brown, 2001).

Una buena característica en algunos de ellos es que le permitirán utilizar una base de datos existente. Vienen con software de administración que por lo general está cargado en un equipo de escritorio. Se configura el dispositivo para usar autenticación y luego lo dirige al servidor de administrador que se instaló. Después se configura el servidor de administración para utilizar la base de datos de usuarios existente. Por ejemplo, si se tiene una base de datos NT, puede mantener una sola base de datos y hacer que el dispositivo VPN realice consultas para autorizaciones de usuarios, en lugar de tener varias bases de datos y tratar de mantenerlas sincronizadas.

En este punto, los proveedores deberían soportar los tres protocolos para establecimiento de túneles, PPTP, L2TP e IPSec, pero no es así. Los proveedores han dado grandes pasos para hacer que la implementación de los dispositivos dedicados al cifrado sea lo más sencilla posible. Como todo lo que sucede en la tecnología, si es fácil puede no ser tan flexible. Sin embargo, el desempeño puede ser bueno, lo cual es más que suficiente para una compañía.

Con la mayoría de las instalaciones de caja negra es posible que se requiera un cortafuego independiente, aunque algunos proveedores están comenzando a incorporar VPN de caja negra con capacidades de cortafuego. La Fig. 3.5 ilustra una solución de VPN de caja negra.

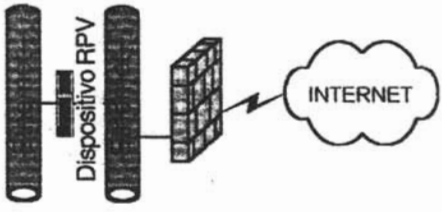


Fig. 3.5: VPN de Caja Negra.

El dispositivo VPN de caja negra se sitúa detrás del cortafuego. Aunque también puede situarse a un lado del mismo.

El cortafuego proporciona seguridad a la organización; pero no provee seguridad para sus datos. Asimismo, su dispositivo VPN le brindará seguridad a sus datos pero no a la organización. Los proveedores están trabajando para hacer que estos dispositivos sean sumamente fáciles de usar.

1.4. VPN Basadas en Enrutador.

Las VPN basadas en enrutador son adecuadas para una organización que ha hecho una gran inversión en enrutadores y cuyo personal de informática tiene experiencia en ellos. Muchos proveedores de enrutadores soportan esta configuración; una visita a sus páginas web le dará una muestra de lo que está disponible. Existen dos tipos de VPN basadas en enrutadores. En uno de ellos el software se añade al enrutador para permitir que el proceso de cifrado ocurra En el segundo método se inserta una tarjeta externa de otro proveedor en el mismo chasis que el enrutador. Este método está diseñado para en el proceso de cifrado del CPU del enrutador a la tarjeta adicional (Brown, 2001).

Algunos proveedores soportan intercambio en activo y redundancia, lo cual está integrado en sus productos VPN basados en enrutador. Esto puede ser necesario para las organizaciones que sólo pueden permitir un tiempo de inactividad corto. Téngase en cuenta que el desempeño puede ser un problema con las VPN basadas en enrutador. Debido a la adición de un proceso de cifrado al proceso de enrutamiento, se puede agregar una carga más pesada al enrutador, especialmente si éste está manejando una gran cantidad de rutas o implementando un algoritmo de enrutamiento intensivo.

Los proveedores de VPN basadas en enrutador pueden proporcionarle una lista de estadísticas de desempeño que podría mostrar que la carga de cifrado del producto es mínima. El enrutador deberá soportar todos los protocolos de seguridad de Internet y aquellos que son más probables se utilicen en el futuro, como PPTP, L2TP e IPSec. Estos protocolos para establecimiento de túneles son importantes para la interoperabilidad futura.

La figura 3.6 es una VPN típica basada en enrutador en la cual los paquetes se cifran desde el origen hacia el destino, por ejemplo, de las oficinas centrales a las oficinas remotas.

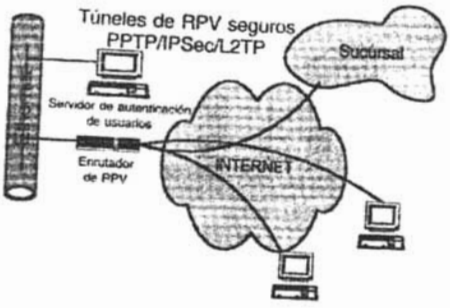


Fig. 3.6: VPN basada en enrutador.

Existen dos inquietudes con las VPN basadas en enrutador:

1. Interoperabilidad. Si se desea conectarse a las VPN de los proveedores, ¿su enrutador y el enrutador de los proveedores trabajan en conjunto y crean la VPN?

2.- Encapsulamiento ¿Se van a Transportar protocolos que no son IP, como IPX o SNA, a otro sitio? Algunos fabricantes de enrutadores cifran pero no encapsulan.

1.5. VPN Basadas en Acceso Remoto.

Hay muchas definiciones diferentes sobre qué es lo que conforma exactamente a una VPN de acceso remoto. Los fabricantes de enrutadores afirman una cosa, los distribuidores de software dicen otra y algunos proveedores dicen algo más. El acceso remoto como su nombre lo indica, significa que alguien de fuera está tratando de crear un flujo de paquetes cifrados hacia una organización. Así que, de manera más literal, tal vez el término se aplique al software que se ejecuta en las máquinas de los usuarios remotos, las cuales están tratando de crear un túnel hacia una organización y a un dispositivo en red que permita esa conexión.

Este túnel podría venir de Internet, pero también podría venir de una línea de marcación, una línea ISDN o una red X.25. En la Fig. 3.7 ilustra un escenario típico de acceso remoto.

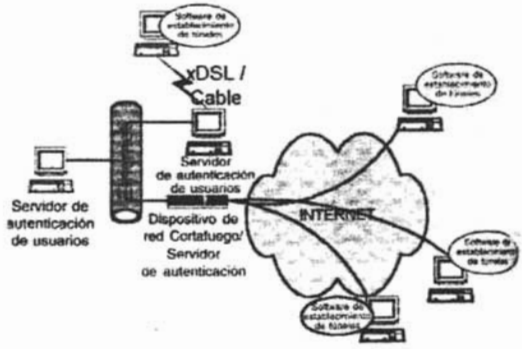


Fig. 3.7: Escenario de acceso remoto.

Este escenario tiene software que se ejecuta en una máquina remota en alguna parte y esa máquina intenta establecer una conexión a través de un túnel cifrado al servidor interno de la compañía o desde una línea de acceso por marcación como ISDN hacia un servidor de autenticación. Un servidor d acceso instalado en su red, ya sea un enrutador, un cortafuego, una caja negra o un servidor de autenticación independiente, concede el acceso. Este dispositivo de acceso remoto reduce la cantidad de los costosos equipos de líneas rentadas y de acceso por marcación remota.

1.6 VPN conscientes de Aplicaciones/kit de Herramientas Proxy.

Este tipo de VPN no es muy popular, pero cuando realmente se necesita es indispensable utilizarlo y en ese momento se tendrá que descubrir si ciertos productos la soportan. Esta situación en particular ocurre debido al enorme crecimiento de los servicios que se ofrecen en Internet. Observe la Fig. 3.8

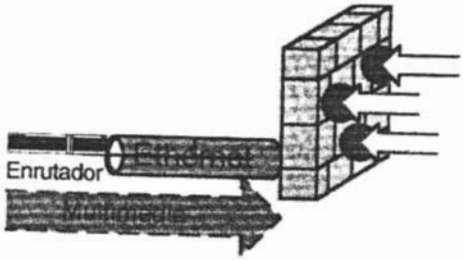


Fig. 3.8: VPN consciente de las aplicaciones.

Internet no es el impulsor de nuevas tecnologías de aplicaciones, pero es el mecanismo de transporte para trasladar estas aplicaciones más nuevas. Por lo general, en las comunicaciones cliente/servidor el cliente solicita un servicio específico a un servidor en un puerto específico. El servidor responde al cliente con la información necesaria y se lleva a cabo la comunicación. Ahora, con las aplicaciones más nuevas, como la telefonía IP y las teleconferencias, cuando se hace una conexión para una aplicación específica en un puerto determinado, la respuesta que el servidor envía de regreso llega a varios puertos. Así que, ¿cómo puede configurar la VPN para que maneje varias conexiones de entrada que se originan desde una solicitud de salida? No se pueden abrir puertos innecesarios debido a posibles violaciones en la seguridad, pero en las tecnologías más nuevas, es necesario. Si no puede abrir se, debe asegurar que la arquitectura de VPN soporte tecnologías nuevas como la telefonía IP, el envío de fax por Internet y los protocolos H.323 y T.120 (Brown, 2001).

Por ejemplo, se va a trabajar con un proveedor y a desarrollar aplicación nueva que necesitará soporte de cifrado sobre los puertos 23489 y 23678, y el puerto UDP 27834. ¿Cómo se implementará? Pueden los puertos individuales pero es una forma insegura.

Reacuérdese que los paquetes regresan cifrados, así que ¿cómo sabría el dispositivo VPN dónde se generaron? Una mejor forma es tener algún tipo de API que pueda escribirse en el dispositivo VPN, la cual permitirá escribir la funcionalidad que necesite a esto se le llama kit de herramientas de API para VPN. Algunos proveedores ofrecen productos para estas características.

1.7. VPN Basadas en Software.

Una VPN basada en software básicamente es un programa para establecer túneles o cifrado a otro anfitrión. Por lo general, se utiliza desde un cliente a un servidor. Por ejemplo, en una VPN de PPTP, el software cargado en el cliente se conecta al software cargado en el servidor y establece una sesión VPN. Existen otras versiones de VPN de software. Cuando se selecciona una VPN de software necesitará tener procesos de administración de claves adecuados posiblemente una autoridad emisora de certificados en las oficinas, con los otros tipos de VPN, por ejemplo, de cortafuego/VPN a cortafuego las únicas claves que se necesitan son de VPN a VPN. Esto significa que el tráfico en la red interna se descifra, así que sólo necesita las claves para los dispositivos VPN. Pero en caso de cliente a servidor, cada estación podría tener su propio par de claves privada/pública; sólo se requiere hacer planes para este tipo de instalación.

El tráfico inicia desde un anfitrión específico en la organización y establece una conexión a algún servidor en otra parte. El tráfico que sale del anfitrión se cifra o se encapsula, dependiendo de la VPN instalada, y se enruta a su destino.

Lo mismo ocurre para alguien que está tratando de conectarse a su red interna; una máquina cliente en alguna parte inicia una sesión de cliente VPN e instaura un diálogo de comunicación con el servidor VPN de su organización. Esta comunicación establece qué tipo de cifrado y cuáles algoritmos de autenicación deben utilizarse y otros datos importantes para iniciar la comunicación. Después de que la instalación inicial se ha completado, comienza el flujo de datos. Hay que asegurarse, si su cortafuego no es el dispositivo VPN, que está configurado para pasar el algoritmo de cifrado elegido.

1.8. Ventajas y Desventajas Asociadas con la Arquitectura de VPN.

Arquitectura de VPN	Ventajas	Desventajas
Hardware	Buen desempeño; Buena seguridad; Ampliable; carga de cifrado mínimo para paquetes grandes; un poco de soporte para balanceo de cargas	Flexibilidad limitada; precio alto; sin interfases ATM, FDDI o Token Ring; la mayoría son semidúplex; se necesita reiniciar para que los cambios tengan efecto; algunos tienen problemas de desempeño importantes con paquetes pequeños (64 bytes); funcionalidad de subred limitada; algunos carecen de NAT.
Software	Amplia variedad de plataformas; facilidad de instalación ; buena para una amplia gama de compañías.	Problemas de desempeño en el soporte NAT; algunos tienen tecnologías de cifrado viejas; propietario; algunos carecen de capacidad de administración remota; sin capacidades de supervisión.
Enrutador	Uso del hardware existente; seguridad sólida disponible; bajo costo si se utilizan los enrutadores existentes.	Algunos pueden necesitar tarjetas de cifrado adicionales; problemas de desempeño; pueden requerir una actualización a un enrutador más potente.
Cortafuego	Amplia variedad de plataformas; uso del hardware existente; soporte para balance de carga y cortafuegos redundantes; IPSec de bajo costo	Posibles problemas de seguridad debidos al sistema operativo; No todos son completamente interoperables con soporte RADIUS; algunos tienen problemas de licencias.
Marcación	Fácil establecimiento de VPN; el costo es bajo	Problemas con compresión de datos cifrados; el soporte para RADIUS es mínimo.

1.9. Certificación y Compatibilidad.

Cualquiera que sea la arquitectura de solución de VPN que una organización decida implementar, seria bueno verificar la certificación. También se podría confiar en la palabra del proveedor en el sentido de que sus productos están certificados para PPTP, L2TP o IPSec. Uno de estos será la Norma en el futuro.

Un punto importante sobre la compatibilidad: si estos productos no son normas ahora, ¿cómo se puede estar seguro de que su implementación será compatible con la norma aceptada? La respuesta real es que no es posible saberlo.

Nadie tiene la certeza sobre en qué dirección irá, pero lo mejor es apegarse a lo básico, probablemente podrá garantizar que el producto será compatible o podrá actualizarse a la Norma una vez que sea aceptada. Aun cuando se crea o no en las certificaciones, son un pequeño aspecto adicional para la prevención. ICSA certifica los productos de los proveedores de IPSec, los cuales son considerados por muchas personas como los que cuentan con el protocolo de seguridad de Internet del futuro.

2. Introducción a la Topología de VPN.

Hay muchas maneras para adquirir e implementar una arquitectura de VPN, también existen muchas formas de colocar esta arquita en una topología de VPN.

2.1 Topología de Cortafuego/VPN a Cliente.

La topología de cortafuego/VPN a cliente es el punto de partida para describir las topologías. La Topología de cortafuego/VPN a cliente será la primera debido a que es la topología de uso más común y prácticamente todas las organizaciones implementen una VPN utilizarán este tipo de configuración. Casi todas las organizaciones conectadas a Internet tienen un cortafuego instalado, y todo lo que necesitan es agregar software VPN al cortafuego.

Esto no implica que se trate de la mejor topología. Sin embargo, es la más común y posiblemente la más fácil para los quien tienen un cortafuego colocado y sólo desean la función VPN. La Fig. 3.9 ilustra este concepto (Clark, 2001).

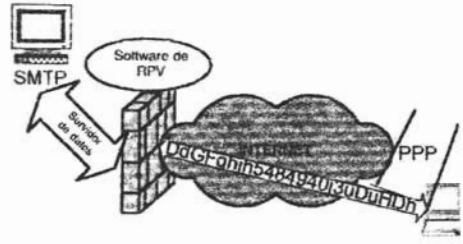


Fig. 3.9: Topología de cortafuego/VPN a cliente.

En la figura 3.9 un usuario en su equipo portátil remoto necesita el acceso a un servidor que se encuentra dentro de la red de la compañía, detrás de un cortafuego/VPN. El usuario desea conectarse al servidor de la compañía y obtener un reporte confidencial. Esta es la configuración cliente/VPN típica.

En ella hay dos componentes que deben habilitarse para establecer la comunicación:

- El dispositivo de cortafuego/VPN debe ejecutar algún tipo de código VPN. Existen muchas formas de realizar esto; algunos cortafuegos tienen incluida en su código la capacidad de crear una VPN, así que las reglas deberán agregarse al cortafuego. Con algunos fabricantes será necesario agregar más software, por ejemplo, si utiliza un cortafuego antiguo que no incluye el cifrado. En este caso, tendrá que encontrar un fabricante cuyo software pueda ser añadido al cortafuego existente.

- El equipo portátil tiene una pila de VPN instalada. Se trata de una pila de VPN puesto que una aplicación de VPN implicaría que el código corriera en el nivel 7 (aplicación) del Modelo OSI. La pila de VPN en realidad se encuentra entre los niveles 2 (enlace de datos) y 3 (red).

Los siguientes pasos describen el proceso de comunicación entre el equipo portátil y el servidor interno una vez que se han completado las configuraciones:

- El usuario con el equipo portátil marca a su ISP local y establece una conexión PPP
- El equipo portátil solicita las claves del dispositivo del cortafuego/VPN. Éste puede ser un paso manual realizado por el usuario o un paso automático configurado por el software.
- El cortafuego/VPN responde con la clave apropiada.
- El software de VPN instalado en el equipo portátil espera a que el usuario intente tener acceso al servidor interno (conocido como la dirección IP de destino). Si el usuario visita cualquier sitio distinto al de la red corporativa, no pasa nada. Ahora, el usuario quiere hacer una conexión con el servidor interno. El software que se ejecuta en el equipo portátil ve la solicitud (de nuevo, conocida como dirección IP), el paquete y lo envía a la dirección IP pública de la combinación cortafuego/VPN.
- El dispositivo de cortafuego/VPN le quita la dirección IP, descifra el paquete y lo envía al servidor dentro de la LAN local.
- El servidor interno responde la solicitud y envía el documento de regreso.
- El cortafuego/VPN examina el tráfico y por su tabla sabe que es una configuración de túnel de VPN. Así que toma el paquete, lo cifra y lo envía al equipo portátil.
- La pila de VPN en el equipo portátil ve el flujo de datos, sabe que viene del dispositivo de cortafuego/VPN, descifra el paquete y lo maneja en aplicaciones de niveles superiores.

Esta configuración es la que permite que la VPN tenga una gran flexibilidad; puede utilizar Internet como su propia red privada. Mientras que los fabricantes tienen discrepancias en la implementación y en las normas, siempre soportan algún tipo de comunicación de túnel cliente-VPN. Muchos ahorros en los costos vienen de esta configuración, así que cuando se examinen opciones de VPN, hay que asegurarse de que su fabricante soporta estas configuraciones.

Dos aspectos de este tipo de configuración que se deben vigilar son las siguientes:

- Las configuraciones del equipo portátil; este software tiene la tendencia a interactuar con otras aplicaciones y provoca problemas de interoperabilidad.
- Esta configuración añade una sobrecarga al proceso de cifrado/descifrado en el cortafuego. Es probable que se tenga que vigilar si existen problemas de desempeño en el cortafuego.

2.2 Topología de VPN/LAN a LAN.

Esta topología es la segunda más utilizada. Por lo general, las corporaciones han utilizado la topología de cortafuego/VPN a cliente ahora quieren extenderla a distintas oficinas remotas. Esta topología también se utiliza entre oficinas y distintos clientes/fabricantes, creando un túnel VPN, entre los dos sitios.

Teóricamente, si se utilizan tanto un cortafuego basado en NT como uno basado en UNIX®, ambos utilizarán cifrado DES y deberán ser capaces de comunicarse entre sí. Desde luego, es importante verificar esto para asegurarse (Clark, 2001).

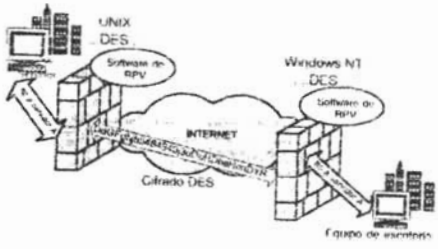


Fig. 3.10: Topología de LAN a LAN.

En la figura 3.10, aparece una organización con una oficina remota. Las dos tienen su cortafuego propio, una es una máquina basada en NT y la otra es una máquina basada en UNIX®. Ambas ejecutan software de VPN de distintos fabricantes y el algoritmo de cifrado utilizado en los productos VPN de los fabricantes es DES.

El ejemplo presenta a un usuario de la oficina remota que necesita conectarse al servidor de la otra oficina y hacer una transferencia FTP para transferir un archivo. Antes de realizar la comunicación, los componentes que deben habilitarse son los siguientes:

- El administrador de cada sitio está de acuerdo con el cifrado DES. El software de VPN de cada dispositivo crea una clave única.
- Si se trata de un producto de cortafuego/VPN, el administrador de cada oficina establece una regla, por ejemplo, que todo el tráfico destinado a la otra terminal debe cifrarse.
- El usuario final utiliza una aplicación FTP en su escritorio para intentar conectarse al servidor.
- El paquete abandona el escritorio en texto sencillo y llega al dispositivo de cortafuego/VPN.
- El paquete es cifrado y se envía a la dirección IP pública del dispositivo de cortafuego/VPN de la otra oficina.
- El cortafuego/VPN acepta y descifra el paquete y lo reenvía a su destino final.
- El servidor recibe el paquete y responde.
- Envía un paquete en texto sencillo a su dispositivo de cortafuego/VPN local.
- Después, el cortafuego/VPN lo cifra y lo envía al otro cortafuego/VPN.
- El cortafuego/VPN lo descifra y finalmente lo envía de regreso al usuario original.

El usuario no tiene idea de que el cifrado se realiza, no hay nada que el usuario final deba hacer para efectuar esta tarea. En lo que concierne al usuario, el servidor está en su red. El servidor no necesita una configuración especial, puesto que cree que está recibiendo una solicitud y una respuesta normales. Lo importante es la relación con el enrutamiento; tanto la máquina del usuario como la del servidor deben saber a qué direcciones enrutar el dispositivo de cortafuego/VPN.

2.3 Topología de VPN/cortafuego a Intranet/Extranet.

Hoy, las Intranets y Extranets son servicios de Internet comunes y de todos los días. En la tecnología VPN estos servicios no han cambiado, pero ahora tienen un nivel adicional de cifrado. Normalmente, las Intranets se utilizaban internamente por los empleados, y las Extranets se

utilizaban externamente por los clientes. La principal diferencia radicaba en la dirección en la que se tenía acceso a ellas. Ahora, con la tecnología VPN, se puede tener acceso internamente o externamente a cualquier servicio. Esto tiene dos condiciones.

Primero, se cuenta con flexibilidad para que una máquina se encargue de ambos y por lo tanto se reduce la redundancia. La segunda condición es la seguridad; ahora existe una forma para que los usuarios externos tengan acceso a estos servidores.

En el futuro, comenzará a desaparecer la diferencia entre Intranets y Extranets. Ahora debe preocuparse sobre lo lejos que se le permite viajar al tráfico externo. Para identificar a los empleados que requieren los servicios de Intranet pero que acceden a ellos externamente y a los clientes externos a quienes sólo se les permite el acceso a la Extranet en la figura 3.11 se ilustra este dilema.

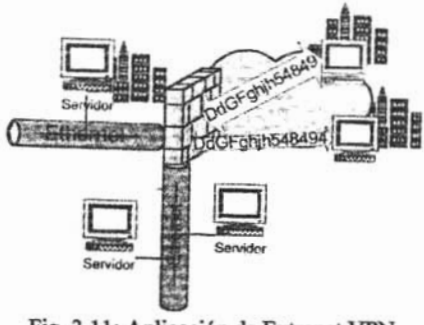


Fig. 3.11: Aplicación de Extranet VPN

Cualquiera de estos tres servidores puede cumplir el papel de servidor de la Extranet y de la Intranet. Cuando el equipo de escritorio remoto o el usuario de marcación remota intentan tener acceso a estos servidores, ¿a cuál se le permitirá accesar?

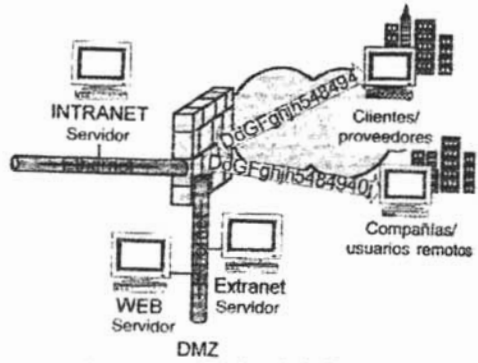


Fig. 3.12: Ubicación de la Extranet.

La figura 3.12 ilustra una posible ubicación para estos servidores. En esta figura, la Extranet se coloca en la DMZ, junto con el servidor web. Los clientes y los proveedores tienen permiso para conectarse al servidor de la Extranet. El servidor web sólo es para tráfico web normal y está disponible para todos. La Intranet se ubica detrás del dispositivo VPN y sólo los usuarios internos que llegan de Internet la usan.

Se colocará la Extranet en la misma zona que el servidor web. El servidor web tiene una seguridad mínima; el servidor de la Extranet por lo general tiene más seguridad. Este es un riesgo de seguridad. Si alguien intenta introducirse al servidor web, probablemente será para cambiar las páginas HTML. Así, desde el mundo exterior, hay algo extraño en la manera en que estas páginas se verán. Tal vez esto no sea un problema mayor para las compañías; sólo le afecta a los usuarios de estas páginas y la responsabilidad financiera no será mucha. Si alguien se introduce en la Extranet, ese alguien podría robar información sumamente importante. Esta información podría relacionarse con el dueño o con quienes tienen acceso al servidor. Normalmente, la compañía permite un acceso global al servidor web, por lo que no existen restricciones en esta fuente de comunicaciones. Así que necesita restringir el acceso a su Extranet.

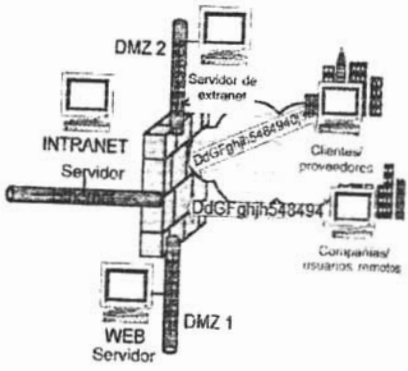


Fig. 3.13: Ubicación apropiada de una Extranet.

La figura 3.13 ilustra la ubicación adecuada para los distintos servidores. El servidor web se mantiene en una red poco confiable, permitiendo que todos tengan acceso a este enlace de red. No importa que el dispositivo del cortafuego o de la VPN permita que los paquetes fluyan al servidor web sin modificación.

La Extranet se coloca en la propia red por separado. La seguridad que se puede implementar aquí consiste en permitir que sólo aquellas direcciones de origen que considere necesarias pasen al dispositivo de cortafuego/VPN, La Extranet se estableció entre ciertas compañías y fabricantes; así que lo más probable es que lleguen desde sus propias redes internas, Por lo tanto, puede restringir el acceso sólo a esas redes. Desde luego, alguien puede burlar las direcciones de origen, pero cuando se estableció las comunicaciones, se creó utilizando una VPN. Desde el principio se cifraron todos los datos; y se está agregando una restricción adicional.

2.4 Topología de VPN/tramas o ATM.

Un gran atributo de Internet es su flexibilidad para habilitar comunicaciones instantáneas. Sin embargo, algunos negocios no creen en la eficacia de internet para transmitir información crítica-comercial debido a sus aspectos de seguridad.

Ésta es una razón de porqué las compañías construyen Intranets empleando sólo líneas rentadas o enlaces basados en retransmisión de tramas para conectarse a sus sitios. Por lo tanto, las redes privadas virtuales pueden configurarse sobre una infraestructura compartida tal como ATM o topologías de redes basadas en tramas. Los negocios que ejecutan sus propias Intranets sobre esta topología de VPN tienen la misma seguridad, facilidad de administración y confiabilidad que en sus propias redes privadas. Existen distintas formas para configurar esta topología, (Clark, 2001) como se ve en la Fig. 3.14

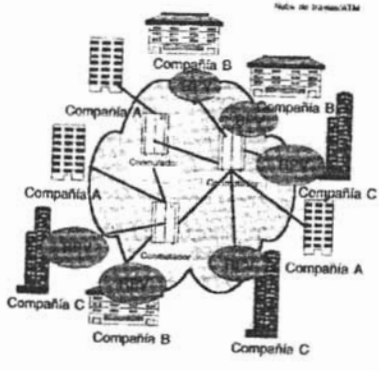


Fig. 3.14: VPN sobre un enlace ATM/Tramas.

Esta figura ilustra un ejemplo típico de una VPN sobre un enlace basado en tramas o ATM de algún ISP. Este tipo de topología generalmente se configura de dos maneras. La primera es IP sobre una infraestructura de red de tramas/ ATM. Esta configuración combina el nivel de aplicación de los servicios IP sobre la capacidad de una red ATM. Dependiendo de la configuración del equipo, los paquetes IP se convierten en celdas y se transfieren sobre una red ATM. El proceso de cifrado se ejecuta en estos paquetes antes de la conversión a celdas, y las celdas que contienen la carga IP cifrada se conmutan al destino final.

La segunda opción es la del grupo de trabajo de Conmutación de etiquetas multiprotocolo (MPLS) del Grupo de trabajo de ingeniería de Internet (IETF) Esto permite que los proveedores de servicios busquen la integración de ATM. En esta topología de red, los conmutadores inteligentes reenvían dinámicamente el tráfico IP en paralelo junto con el tráfico ATM en la misma red ATM. Al paquete se le aplica un campo que contiene un ID único identifica el destino final. Todos los conmutadores de esta red ATM examinan este campo y lo reenvían a su destino apropiado. El atributo de seguridad de esto es que el paquete sólo se reenvía a su destino, evitando así el espionaje. Cualquier proceso de cifrado que pueda utilizarse aquí sólo se aplica a la porción de datos, antes de enviarlo a la nube ATM. Debido a que esta configuración aplica un campo al paquete, no se pueden cifrar los encabezados del paquete; sin embargo, se podría cifrar la carga útil, lo que implica que la funcionalidad completa de IPSec no se implementará. Pero, al cifrar la carga y conmutarla sólo a su destino, sí existe seguridad.

2.5 Topología de VPN de hardware (caja negra)

Las VPN de hardware, o cajas negras, son dispositivos independientes implementan algoritmos de tecnología VPN. Algunas soportan normas de cifrado como DES de 40 bits (internacional) y 3DES (Estados Unidos y Canadá). Algunos autores (Brown S, L. Clark) creen que los dispositivos de hardware son capaces de completar más rápido el proceso de cifrado/descifrado que los dispositivos de software de las VPN.

Muchos fabricantes ofrecen soluciones tanto de cajas negras como de software para las VPN. Recientemente, los dispositivos de hardware comienzan a tener servicios adicionales como cortafuegos, antivirus y capacidad de enrutamiento.

Los dispositivos de hardware por lo general incluyen software adicional que se instala en el equipo de escritorio para permitir la configuración y el mantenimiento de ese dispositivo; además, un servidor web puede configurar algunos tipos. Los fabricantes de dispositivos ahora crean sus líneas de productos con un conjunto completo de servicios como los certificados digitales, el soporte LDAP, la vigilancia SNMP y capacidades completas para Internet y para la marcación a VPN.

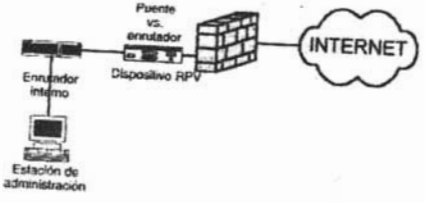


Fig. 3.15: VPN de caja negra detrás del cortafuegos.

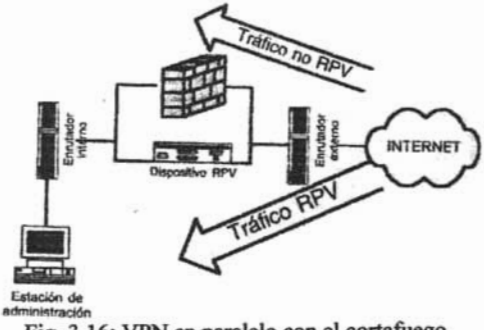


Fig. 3.16: VPN en paralelo con el cortafuego.

Las figuras 3.15 y 3.16 muestran un par de ubicaciones típicas para estos dispositivos. En la figura 3.15, el dispositivo VPN se ubica detrás del cortafuego de la red interna. Los paquetes de datos pasan por el cortafuego y por el dispositivo VPN. Conforme los paquetes de datos pasan por estos dispositivos, se mantienen intactos o se cifran, dependiendo de la configuración del dispositivo.

La estación de administración se ubica en algún lugar de la red interna utilizada para configurar el dispositivo; también existe la opción de utilizar un servidor web para configurar el dispositivo. Si tiene un conjunto de dispositivos VPN ubicados en distintos puntos geográficos, hay que asegurarse de contar con la capacidad para crear túneles de mantenimiento a estos dispositivos con el fin de modificarlos.

En esta configuración, el dispositivo VPN puede actuar como un puente o como un enrutador. Con el puente, los paquetes fluirán de una interfase a otra, y con el enrutamiento se asignarán espacios de direcciones IP y se deberá asegurar de que los otros dispositivos de la red puedan dirigirse a ellas.

En la figura 3.16 el dispositivo VPN tiene el cortafuego junto a él, o en paralelo. Esto se conoce como configuración de un brazo. Esta configuración permite al dispositivo VPN crecer a miles de túneles. El enrutador externo pasa el tráfico VPN al dispositivo VPN (por medio de la dirección VPN) y dirige todo el tráfico restante al cortafuego.

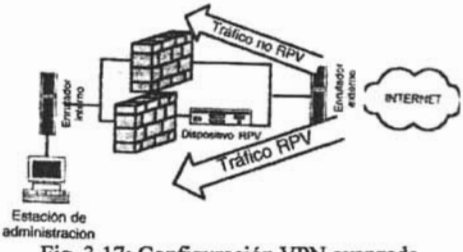


Fig. 3.17: Configuración VPN avanzada.

Como se ve en la figura 3.17, también es posible agregar un cortafuego detrás del dispositivo de cortafuego en una configuración más elaborada. Cuando se establecen túneles de VPN y se garantiza el acceso, éstos se crean para destinos específicos. Si se opta por hacerlo, después de que el dispositivo descifre el paquete, el cortafuego interno lo revisará para ver su destino y le permitirá o negará el acceso.

2.6 Topología de VPN/NAT.

Aunque la Traducción de direcciones de red (NAT) no es una VPN, se debe discutir puesto que muchas organizaciones la implementan, y los dispositivos VPN se ven afectados directamente por los procesos de NAT. La traducción de direcciones de red es el proceso de cambiar una dirección IP (por lo general la dirección privada de una compañía) a una dirección IP pública enrutable. NAT proporciona un mecanismo para ocultar la estructura de la dirección privada de una compañía. (Incluso, en algunos casos una compañía puede usar a NAT para ocultar su dirección pública.) Utilizar la traducción de direcciones de red no es complicado, pero la ubicación del dispositivo VPN es importante. Si se implementa a NAT en un paquete de VPN, ese paquete puede ser descartado; hay que tener en cuenta que una VPN es una configuración de IP a IP. La figura 3.18 ilustra el flujo de tráfico que tiene lugar en un cortafuego que implementa a NAT mientras que el dispositivo VPN se encarga de la autenticación de usuarios.

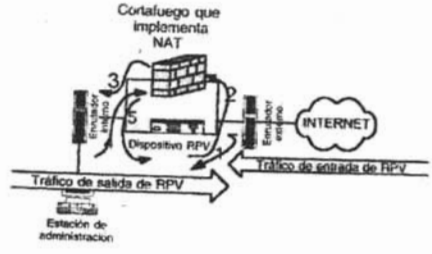


Fig. 3.18: Configuración VPN avanzada.

A continuación se presentan algunas notas sobre el tráfico de salida y entrada de la VPN:

Tráfico de salida de la VPN:

- Todo el tráfico que viene de un enrutador interno se dirige al dispositivo NAT para cambiar la dirección IP original del dispositivo que lo solicita a una dirección IP pública enrutable.

- Después, el dispositivo NAT reenvía el paquete al dispositivo VPN realiza el proceso de cifrado del paquete.

- El paquete se envía al enrutador externo y finalmente a su destino.

Tráfico de entrada de la VPN

- Primero, los paquetes de VPN entrantes deben dirigirse al dispositivo VPN; este dispositivo quita la carga de cifrado del paquete y privilegios de autenticación.

- El paquete se enruta al dispositivo de traducción de direcciones para remitirlo a su dirección IP original (interna). En este caso, el cortafuego está a cargo de NAT.

- El dispositivo NAT enruta el paquete (con su nueva dirección origen) al enrutador interno.

Protocolos Usados en una VPN.

Capítulo IV: Protocolos Utilizados en una VPN.

1. Túnel VPN.

Un túnel VPN funciona mediante la encapsulación de datos dentro de paquetes IP para transportar información que no cumple de ninguna forma con los estándares de direccionamiento en Internet. Posteriormente, estos paquetes encapsulados se transportan entre una red, o cliente único, y otra red sobre una red intermedia. A todo este proceso de encapsulación y transmisión de paquetes se le conoce como conexión por túnel, y a la conexión lógica por la que los paquetes viajan se le llama túnel. Un túnel es una conexión a través de Internet u otra red intermediaria. El resultado es que los usuarios remotos se convierten en nodos virtuales en la red a la que han sido conectados por túnel (Microsoft, 1999).

Desde la perspectiva del usuario, la naturaleza de la red física que ha sido conectada por túnel es irrelevante ya que aparece como si la información haya sido enviada sobre una red privada dedicada.

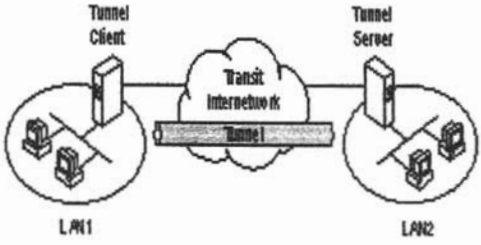


Fig. 4.1. Un modelo conceptual de una VPN.

La comunicación a través de Internet requiere que, tanto la encapsulación como la encriptación de flujo de datos, sea viable. PPTP y L2TP proporcionan servicios de encapsulación, a fin de facilitar las comunicaciones de protocolos múltiples mediante Internet.

La encapsulación permite que los paquetes de datos no basados en IP se comuniquen a través de Internet basada en IP desde un cliente remoto a una LAN corporativa privada, la cual permite que las redes no basadas en IP aprovechen al máximo el Internet.

2. Protocolo Punto a Punto (PPTP).

PPTP se diseñó para proporcionar comunicaciones autenticadas y cifradas entre un cliente y una puerta de enlace o entre dos puertas de enlace (sin necesitar una infraestructura de clave pública) utilizando un Id. de usuario y una contraseña. Apareció por primera vez en 1996, dos años antes de la disponibilidad de IPSec y L2TP. El objetivo del diseño era la simplicidad, la compatibilidad multiprotocolo y la capacidad de cruzar una amplia gama de redes IP (Brown, 2001).

PPTP es un estándar abierto en la industria. La especificación para PPTP es el resultado de la reunión de esfuerzos con un circulo de proveedores de operaciones de red reconocidos entre los que se incluyen Ascend Communications, 3Com/Primary Access, ECI Telematics, US Robotics, y Microsoft. Estas compañías constituyeron el foro PPTP, cuyos esfuerzos unidos se dieron a conocer públicamente y fueron presentados ante la organización de estándares y IETF en 1996.

El Protocolo Punto a Punto (PPTP) se diseñó para permitir que los usuarios remotos marcaran a su ISP local y establecieran un túnel al servidor de la compañía. En este caso puede ser un cliente PPTP Windows 98 que establece un túnel a un servidor PPTP en la red de una empresa. PPTP utiliza la infraestructura de protocolos existente para permitir una conexión por marcación, llamada PPP. Luego toma estos paquetes PPP y los encapsula dentro de un encabezado con Encapsulamiento para Enrutamiento Genérico (GRE). Debido a la dependencia en PPP, PPTP utiliza algoritmos de cifrado tales como PAP y CHAP para proporcionar el cifrado. Además, utiliza el Cifrado Punto a Punto de Microsoft (MPPE).

Debido a la disponibilidad del PPTP en NT y a la base de usuarios instalada, PPTP es un protocolo que viene en dos configuraciones: modo obligatorio y modo voluntario.

2.1 Modo Obligatorio.

Una sesión PPTP en modo obligatorio utiliza los servicios de un ISP junto con un procesador frontal PPTP, como lo muestra la figura 4.2. Los modos obligatorios están hechos con la ayuda de un NAS. No se necesita ningún software PPTP en el cliente. El protocolo PPP maneja cualquier problema de comunicación en una conexión por marcación al ISP; y , cualquier problema en el equipo portátil puede deberse a la configuración de marcación a la red. Puesto que los modos obligatorios se crean sin conocimiento del usuario cuando ocurre este tipo de problemas, es probable que se necesite ayuda del ISP que contrató. También restringen el acceso de los usuarios a otras partes de Internet.

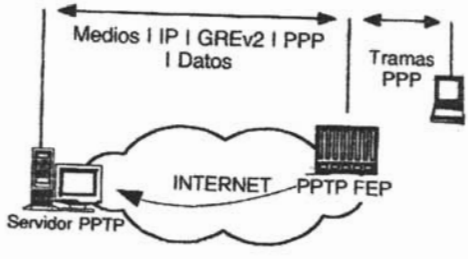


Fig. 4.2 modo obligatorio.

2.2 Modo Voluntario.

En el modo voluntario los clientes establecen una conexión PPTP directa con el servidor PPTP en el otro extremo de la red para crear un túnel, como se ve en la figura 4.3. En este caso el ISP no está involucrado. Para resolver el problema, lo primero que debe hacerse es asegurar el acceso a Internet.

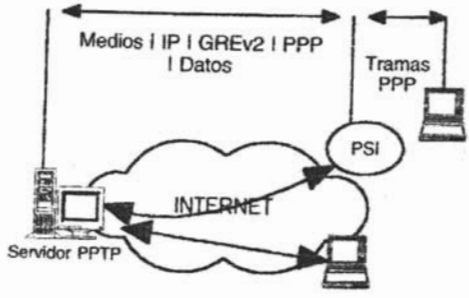


Fig. 4.3 modo voluntario.

En el PPTP de modo voluntario, no hay requisitos para el FEP de un ISP. Las conexiones se hacen directamente al servidor PPTP en la LAN de la empresa. Los problemas en el equipo portátil podrían ser aquellos derivados de las comunicaciones al configurar el PPP. Además, esta forma de PPTP permite que una máquina en Internet tenga acceso al servidor PPTP sin los servicios de una conexión PPP.

En cualquier configuración PPTP, se debe entender cómo PPTP establece una conexión para resolver los problemas de manera efectiva.

2.3 Escenario Típico de Conexión PPTP.

Una máquina cliente (Windows® 98 o NT 4.0) se conecta a un Proveedor de Servicios de Internet (ISP) utilizando una conexión de acceso telefónico a redes. En otro punto de Internet existe una máquina (NT 4.0 Server) con el servicio de servidor de acceso remoto (RAS) conectado a ella, bien directa y permanentemente, mediante un adaptador de Red o también mediante una conexión de acceso remoto, usando el adaptador de red privada virtual, a dicho servidor, creándose un túnel privado sobre Internet, que conecta ambas máquinas como si estuvieran en la misma red local, pudiendo así tener acceso a recursos compartidos tales como carpetas o impresoras. Este escenario puede variar según el tipo de conexión que tengan tanto el cliente como el servidor. Organizaciones con acceso permanente a Internet, pueden configurar servidores de acceso remoto para que soporten PPTP.

Esto permite que colaboradores en cualquier parte del mundo puedan conectarse a ellos, usando sus accesos a Internet habituales. Así, será posible participar de los recursos de la red corporativa, con seguridad garantizada, y sin los cortes habituales de las llamadas de larga distancia a estos servidores de acceso remoto (Collado et al. 2004).

2.4 Servidores PPTP.

Un servidor PPTP tiene dos reglas principales: actúa como el fin de punto de los túneles de PPTP y envía paquetes a y por el túnel. Los servidores PPTP envían paquetes a un ordenador destino para procesar en paquete PPTP obtenido de dirección o nombre de la red privada en el paquete PPP encapsulado. El servidor PPTP solo puede filtrar paquetes, usando filtros PPTP. Con los filtros PPTP puedes colocar el servidor para restringir quien puede conectarse a la red local o a Internet (Collado et al. 2004).

Estableciendo un servidor PPTP en un sitio corporativo se establecen unas pocas restricciones, especialmente si el servidor PPTP esta siendo colocado en el sitio privado del firewall. PPTP ha sido diseñado para que solo un número de puerto TCP/IP pueda usarse para transmitir datos a un firewall, número de puerto 1723. Esta escasez de configuraciones de números de puertos puede hacer al firewall más susceptible a ataques.

Solo se tiene el firewall para filtrar tráfico por el protocolo, se necesitará colocarlos permitiendo a GRE pasar por él.

Tipo de Hardware requerido en los servidores:

La máquina configurada como "PPTP Server" debe tener la configuración mínima requerida para correr Windows® 2000 Server. Además, debe tener dos adaptadores de red (NIC, módem, RDSI, X25), uno conectado a la red local LAN, y otro a Internet.

Una de las ventajas más palpables del PPTP es que reduce o elimina la necesidad de uso de complejas y caros equipos de telecomunicaciones para permitir las conexiones de equipos portátiles y remotos. PPTP puede usar redes telefónicas normales de forma totalmente segura.

2.5 Clientes PPTP.

Si el equipamiento ISP soporta PPTP, no requiere añadir software o hardware en el final del cliente; solo es necesaria una conexión estándar PPP. En la otra mano, si el ISP no soporta PPTP, un cliente Windows® NT puede utilizar PPTP y crear una conexión segura, primero utilizando ISP y estableciendo una conexión PPP, después a través de un puerto PPTP conectarse con el cliente.

2.5.1 Tipo de Hardware Requerido en los Clientes.

El cliente puede ser una máquina con Windows® 95 a 2000, tanto Server como Workstation. En ambos casos, se requiere de un módem o tarjeta RDSI, además de un equipo de conexión a una red telefónica (plaqueta en pared, teléfono móvil que soporte este tipo de conexiones, etcétera.) Por otro lado, si el cliente está accediendo al servidor PPTP a través de una red de área local (LAN), se precisa de un adaptador de red (NIC) que lo conecte físicamente a ella.

2.6 Comunicación de Datos PPP.

La comunicación de datos PPP es la comunicación inicial que necesita el equipo portátil para conectarse al ISP. El cliente remoto habilitado para PPTP se conecta al ISP utilizando datagramas PPTP cifrados y autentica al usuario. PPP encapsula todos los protocolos que no son TCP, tales como IPX y NetBEUI, dentro de estas tramas PPP.

2.7 Conexiones de Control PPTP.

Una vez que el protocolo PPP establece la conexión, el protocolo PPTP realiza la conexión entre el cliente PPTP y el servidor PPTP.

Emplea el protocolo TCP para establecer lo que se conoce como un túnel PPTP. Los mensajes de control, que se muestran en la tabla siguiente, son de ayuda para resolver problemas de conexiones PPTP.

Tipo de Mensaje	Significado
PPTP_START_SESSION_REQUEST	Inicia sesión
PPTP_START_SESSION_REPLY	Responde la solicitud
PPTP_ECHO_REQUEST	Mantiene la sesión
PPTP_ECHO_REPLY	Responder para mantener sesión
PPTP_WAN_ERROR_NOTIFY	En la conexión ha ocurrido un error en un enlace PPP
PPTP_SET_LINK_INFO	Configura la conexión entre cliente y servidor PPTP
PPTP_STOP_SESSION_REQUEST	Termina la sesión PPTP
PPTP_STOP_SESSION_REPLY	Responde
WAN_ERROR_NOTIFY	Errores en la interfaz PPP de la WAN.

Mensajes de control.

Dentro de estos mensajes de control hay códigos de errores adicionales que son útiles para resolver problemas. Por ejemplo, Start-O Connection-Reply tiene una lista de códigos que son resultado de agregar información adicional para resolver problemas, como se muestra enseguida.

1. Establecimiento exitoso del canal.
2. Error general, el código de errores indica el problema.
3. Ya existe el canal de comandos.
4. El solicitante no está autorizado para establecer el canal de comandos.
5. La versión del protocolo del solicitante no se soporta.

WAN-Error-Notify es una lista de mensajes de errores de control enviada desde el Concentrador de acceso PPTP (PAC) al Servidor de red PPTP (PNS) para indicar las condiciones de errores en el enlace WAN.

Las condiciones de error son las siguientes:

- Errores CRC El número de tramas PPP recibidas con CRC desde comienzo de la sesión.
- Errores de tramas El número de paquetes PPP entramados con formatos incorrectos.
- Desbordamiento del hardware El número de desbordamientos de la memoria intermedia (buffer) recibidos en el hardware desde el comienzo de la sesión.
- Desbordamiento de la memoria intermedia El número de desbordamientos de la memoria intermedia desde el comienzo de la sesión.
- Errores por tiempo agotado El número de periodos agotados desde el comienzo de la sesión.
- Errores de alineación. El número de errores de alineación.

2.7.1 Establecimiento de Túneles PPTP de datos.

Los túneles PPTP de datos son la etapa final de la transmisión, donde el protocolo PPTP forma los paquetes PPP que tienen paquetes PPTP cifrados y los envía al servidor PPTP. Entonces, el servidor PPTP descifra estos paquetes y los envía a los anfitriones respectivos.

Las comunicaciones PPTP dependen del tipo de modo que se emplee, ya sea voluntario u obligatorio, así que la solución de problemas dependerá de cómo se establecen las conexiones de control. En el caso del modo obligatorio, el FEP (procesador frontal) del ISP maneja las comunicaciones PPTP. En el caso del modo voluntario, el mismo equipo portátil maneja los mensajes de control PPTP (Brown, 2001) . El siguiente es un conjunto de pasos típicos para manejar las comunicaciones PPTP:

1. El equipo portátil crea una cuenta PPP de marcación a un ISP o a un ISP con FTP.

2. El FEP podría enviarle una señal al servidor PPTP con una PPTP_Start_Session_Request, y el servidor podría responder con una PPTP_Start_Session_Reply.

3. Entonces, el FEP hace una solicitud al servidor PPTP.

4. El servidor envía la respuesta al FEP.

5. Comienza la comunicación de datos.

6. Finalmente, se envía un PPTP_Stop_Session_Request y se recibe un PPTP_Stop_Session_Reply (vea la Fig. 4.4).

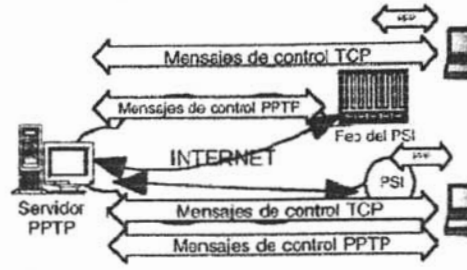


Fig. 4.4 mensajes de control.

El servidor PPTP esta detrás del cortafuego, como lo muestra la figura 4.5. En esta figura se emplea la comunicación PPTP a través del cortafuego; sin embargo, si no se configura el cortafuego para que pase los paquetes correctos, la comunicación PPTP nunca se efectuará. PPTP utiliza el protocolo IP 47, el cual es el protocolo GRE, y los puertos TCP 1723 ó 5678. El puerto 1723 es para el servicio PPTP de Microsoft.

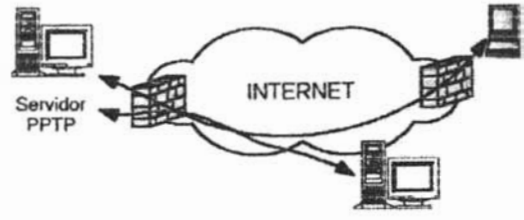


Fig. 4.5 PPTP a través de un cortafuego.

2.8 Análisis a PPTP.

Se realizo un análisis el 1 de junio de 1998 sobre el criptoanálisis de la implantación de Microsoft Corp. del PPTP por el afamado especialista y criptólogo Bruce Schneier y el destacado intruso Peter Mudge de LOpht Heavy Industries en la revista *Phrack Magazine* se escribió sobre este análisis técnico de algunos de los hallazgos incluidos en AlephOne . Aleph One saca a la luz más información sobre inseguridades PPTP.

Estas dos personas estudiaron la interacción de un cliente servidor y llegaron a los siguientes puntos:

1.- Algoritmos débiles que permiten que los escuchas furtivos puedan descubrir las contraseñas.

2.- El diseño imperfecto que permite a un atacante adueñarse y luego enmascararse como un servidor legitimo.

3.-Errores de implantación que permiten la recuperación de datos encriptados.

4.- Mensajes no autenticados que permitirían a los intrusos derrumbar la puerta de enlace de activación de túneles de PPTP.

2.8.1 La Posición de Microsoft.

Microsoft, sigue mejorando su tecnología de operación de red y comunicaciones Windows® y lanza una actualización de rendimiento y seguridad PPTP para clientes y servidores basados en Windows®.

La solución VPN habilitada por PPTP de Microsoft combina los siguientes beneficios: una plataforma ampliamente disponible, una operación de red con todas las funciones, la integración activa de Windows® y la facilidad de uso para entregar una plataforma de comunicaciones altamente programable y flexible. Un sistema basado en Windows® configurado adecuadamente, que utilice herramientas Windows® y PPTP para reforzar la política de seguridad de contraseña responsable, proporciona una solución VPN económica, confiable y segura que permite ahorros en los costos relacionados con las comunicaciones basadas en Internet (Microsoft, 1999).

2.8.1.1 Avance de la Tecnología.

Como resultado de una continua revisión experimentada y de los rápidos avances tecnológicos.

La vanguardia de la encriptación y seguridad de red cambia constantemente. Por esta razón, Microsoft proporciona periódicamente actualizaciones oportunas para sus servicios de seguridad y productos. Los clientes que pagan la política de seguridad siempre deberán estar al tanto sobre los más recientes avances de seguridad disponibles en Microsoft, y deberán monitorear regularmente el sitio Web de seguridad de Microsoft en http://www.microsoft.com/security

Los desarrollos recientes con la tecnología VPN PPTP de Microsoft incluyen:

- Mejora de autenticación con MS-CHAP versión 2
- Opción para solicitar autenticación de contraseña más sólida
- Mejora de encriptación con la Encriptación de punto a punto de Microsoft (MPPE)

Mejora de Autenticación con MS-CHAP versión 2.

El Protocolo de autenticación *Handshake* de Microsoft (MS-CHAP) es un mecanismo de autenticación que se utiliza para validar las credenciales del usuario contra los dominios Windows® NT, mientras que las claves de sesión resultantes se utilizan para encriptar los datos del usuario (Microsoft, 1999).

La Encriptación es el proceso de codificación de datos que sirve para prevenir el acceso no autorizado, especialmente durante la transmisión. La Encriptación se lleva acabo utilizando un algoritmo especial junto con uno confidencial (también conocido como *clave*) para transformar datos, como puede ser una contraseña, de manera tal que los datos no puedan ser entendidos por ninguna persona que no conozca la clave correcta. La contraseña *hashed* sólo puede ser decriptada por un ordenador que tenga la misma clave.

La versión 2 MS-CHAP incluye una función de una salida de la contraseña del usuario, un reto generado por el servidor y el cliente, además de datos adicionales en el mensaje *Satisfactorio* de la versión 2 MS-CHAP. El cliente de la versión 2 MS-CHAP se desconecta si no puede autentificar el servidor.

Cuando el servidor de acceso de red recibe una solicitud de autenticación MS-CHAP versión 2, por parte de un cliente remoto, éste envía un reto, el cual consiste en una ID de sesión y una cadena de retos arbitrarios, para el cliente remoto. El cliente remoto debe confirmar el nombre del usuario, el *hash* de la cadena de retos, la ID de sesión y la contraseña *hashed* . Este diseño, el cual manipula un *hash* del *hash* de contraseña, proporciona un nivel adicional de seguridad ya que permite que el servidor almacene contraseñas *hashed* en lugar de contraseñas de texto.

La versión 2 MS-CHAP también proporciona códigos de error adicionales incluyendo un código expirado de contraseña, mensajes encriptados adicionales de cliente-servidor permiten a los usuarios cambiar sus contraseñas(Microsoft, 1999). En la implementación de la versión 2 de MS-CHAP de Microsoft, tanto el cliente como el servidor generan una clave inicial de manera independiente para la encriptación de datos subsecuentes por MPPE.

2.8.1.2 Opción para Requerir Autenticación de una Contraseña más Sólida.

Cuando los clientes basados en Windows® se conectan a un servidor PPTP basado en Windows® NT, realizan una autenticación de respuesta a retos mediante el uso de una técnica denominada MS-CHAP. Esta técnica utiliza una función *hashing* para obscurecer la contraseña Windows® NT en la respuesta. (Una contraseña Windows® NT debe ir en minúsculas y puede tener hasta 14 caracteres de longitud y utiliza el conjunto de caracteres Unicode de 16 bits).

Debido a que la autenticación se basa, en parte en el *hashing* de la contraseña del usuario para generar claves de encriptación inicial, los administradores de red deben reforzar el uso de una estructura de contraseña Windows® NT más compleja..

Aunque se pueden utilizar las contraseñas anteriores del Administrador LAN (LM), las contraseñas LM no son tan complejas como las contraseñas Windows® NT, y por lo tanto son más susceptibles a la fuerza bruta o ataques de diccionario, en la que un intruso trata de adivinar la contraseña del usuario.

2.8.1.3 Solicitud del uso de Contraseña Windows® NT.

Microsoft ha lanzado una actualización para los componentes de cliente y servidor PPTP para Windows® NT que le da a los administradores la habilidad de configurar el servidor PPTP de manera tal que sólo puedan aceptar la autenticación de una contraseña más sólida de Windows® NT. Esta actualización también permite que el administrador configure clientes PPTP basados en Windows® NT para que nunca puedan utilizar la autenticación LM. Microsoft liberó una actualización para el cliente PPTP basado en Windows® 98 que le permitirá ser configurado de manera tal que nunca tenga que utilizar la autenticación LM al conectarse a los servidores PPTP.

2.8.1.4 Reforzamiento de la Política de Contraseña.

Microsoft recomienda que los clientes refuercen el uso de contraseñas sólidas (complejas) en sus redes mediante el uso de las herramientas de Windows® que le permiten al administrador hacerlo. Las contraseñas podrían mezclar letras minúsculas y mayúsculas, números y puntuación.

Una política de contraseñas adecuada que especifique la longitud mínima de contraseña, la diversidad de caracteres y la actualización regular es una parte importante en el mantenimiento de la seguridad de la red. Windows® NT puede reforzar fácilmente esta política de contraseñas.

2.8.1.5 Principios Básicos de la Política de Contraseñas Adecuadas.

Las contraseñas sólidas solicitan por lo menos un número mínimo de caracteres y una diversidad de tipos de caracteres. Las buenas contraseñas deberán ser indescifrables por otros. Esto es importante ya que las contraseñas mal elegidas atentan contra la seguridad.

Las contraseñas mal elegidas incluyen aquellas que:

- Se forman únicamente de palabras de diccionario.
- Son de un solo tipo (mayúsculas o minúsculas).
- Se crean de nombres de personas o cosas que podrían descifrarse por otros, tal como el nombre de un hijo de usuario, mascota, o incluso el nombre de soltera de la madre.

Las claves bien elegidas incluyen aquellas que:

- Contiene por lo menos un número y un símbolo (tales como un ?) en medio.
- Aparecen ser "gobbledygook" al observador casual.
- No contiene palabras del diccionario o nombres propios.

La administración adecuada de la política de contraseñas hace que cualquier solución basada en una contraseña sea más difícil de comprometer. Las contraseñas complejas, la tecnología adecuada, y las restricciones físicas, todas en conjunto hacen que Windows® sea una solución muy segura de VPN en el mundo real.

La encriptación de 128 bits de Microsoft, la clave de encriptación no sólo es una función de una contraseña compleja si no también incluye una función en el reto. Este algoritmo hace que un ataque sea mucho más difícil.

2.8.1.6 Mejora de Encriptación con MPPE.

El uso de encriptación proporciona un nivel adicional de seguridad para redes privadas virtuales basadas en PPTP. Aunque esto es poco común, si alguna vez se ve en el mundo real es posible que una persona intercepte paquetes VPN. Si un agresor pudiera colocar una máquina entre el cliente y su servidor de destino, la máquina en el medio podría intentar suplantar el servidor PPTP sujeto y aceptar el tráfico del cliente. La vulnerabilidad a intromisiones de un intruso existe con cualquier protocolo de autenticación de respuestas de reto no mutuo y por lo tanto no es específico para productos de Microsoft. Además, la versión 2 MS-CHAP proporciona autenticación mutua y se diseñó específicamente para vencer dicho ataque.

Al utilizar la encriptación basada en software de 128/40 bits, todo usuario comunicado con datos entre el cliente y el servidor está totalmente protegido y no puede ser leído por la máquina intrusa, la cual no cuenta con la clave necesaria para desencriptar la información transmitida.

PPTP utiliza el algoritmo de encriptación RSA RC4, que opera en el nivel de encriptación más sólido permitido por el gobierno de los Estados Unidos–utilizando claves de 128 bits en Norteamérica y claves de 40 bits en otras partes. Cuando se utiliza la versión 2 MS-CHAP, las claves separadas de encriptación de RC4 se derivan para cada dirección, y por predeterminación, las claves de encriptación se cambian en cada paquete. Estos hechos hacen que las intromisiones sean extremadamente difíciles (Microsoft, 1999).

2.8.1.7 Protección de canal de control

Este programa proporciona una más amplia verificación de parámetros en los datos que se transfieren al canal de control para asegurarse de que los datos en el canal de control no puedan bloquear el servidor PPTP. Este programa de reparación también se incluye en las actualizaciones de PPTP para Windows® NT y posteriores.

Después de esta reparación, el peor resultado de un ataque de este tipo sería abandonar la sesión activo de PPTP.

2.9 Recomendaciones para fortalecer a PPTP.

Microsoft publica parches para servidores y clientes en todas sus plataformas periódicamente se recomienda utilizar los más actuales consultando el Microsoft Security en el sitio (http://www.microsoft.com/security)

Además PPTP ha mejorado de manera importante en Windows® 2000 y cuentan con la capacidad de utilizar el protocolo L2TP basado en IPSec. Los clientes PPTP de Win 9x se deben actualizar a la versión 1.3 de acceso telefónico a redes para ser compatibles con las medidas de seguridad más exigentes del lado del servidor.

Microsoft sigue evolucionando su operación de red privada virtual a fin de proporcionar a los usuarios soluciones seguras VPN y bien integradas.

2.10 Diferencias entre protocolos.

Comparativa entre PPTP y L2TP

- Con PPTP, el cifrado de datos comienza después de que la conexión se procese (y, por supuesto, después de la autentificación PPP). Con L2TP/IPSec, el cifrado de datos empieza antes de la conexión PPP negociando una asociación de seguridad IPSec.

- Las conexiones PPTP usan MPPE, un método de cifrado basado en el algoritmo de encriptación Rivest-Shamir-Aldeman (RSA) RC-4, y usa llaves de 40, 56 o 128 bits. Las conexiones L2TP/IPSec usan Data Encryption Standard (DES), con llaves de 56 bits para DES o tres llaves de 56 bits para 3-DES. Los datos se cifran en bloques (bloques de 64 bits para el caso de DES).

- Las conexiones PPTP requieren sólo autentificación a nivel de usuario a través de un protocolo de autentificación basado en PPP. Las conexiones L2TP/IPSec requieren el mismo nivel de autentificación a nivel de usuario y, además nivel de autentificación de máquina usando certificados digitales.

- PPTP requiere una capa de transporte basada IP de la red mientras que L2TP requiere solamente que los medios proporcionen el punto a la conectividad del punto. El protocolo de L2TP se puede utilizar tan directamente sobre el relay del capítulo del IP, X.25 y ATM. PPTP no puede apoyar los medios no-IP directamente.

- PPTP apoya solamente un solo túnel entre el servidor de VPN y el cliente. Con L2TP, los túneles múltiples se pueden apoyar para transportar las cargas útiles end-to-end. Por lo tanto, las operaciones del multi-túnel son posibles con L2TP que corresponde a los varios niveles de la calidad del servicio (QoS) y de la seguridad.

[1]La siguiente tabla muestra las diferencias entre protocolos:

Características	Descripción	PPTP/PPP	L2TP/PPP	L2TP/IPSec
Autenticación de usuario	Puede autenticar al usuario que esta iniciando las comunicaciones.	SI	SI	SI
Autenticación de equipo	Permite autenticar los equipos implicados en las comunicaciones.	SI	SI	SI
Compatible con NAT	Puede pasar por traductores de direcciones de red para ocultar uno o ambos extremos de las comunicaciones.	SI	SI	NO
Compatibilidad con multiprotocolo	Define un método estándar para trasmitir tráfico Ip y no Ip.	SI	SI	SI
Asignación dinámica de direcciones ip de túnel	Define una forma estándar para definir una dirección Ip para la parte de túnel de las comunicaciones. Es importante para que los paquetes devueltos se enluten de vuelta en la misma sesión en ves de a través de una ruta sin túnel e insegura para eliminar la configuración manual estática del equipo final.	SI	SI	SI
Cifrado	Puede cifrar el tráfico que trasmite.	SI	SI	SI
Utiliza PKI	Puede utilizar PKI para implementar el cifrado y/o la autenticación	SI	SI	SI
Autenticidad de paquetes	Proporciona un método de autenticidad para asegurarse de que el contenido del paquete no se modifica mientras se trasmite.	NO	NO	SI
Compatibilidad multidifución	Puede trasmitir trafico multidifución además de trafico Ip de difusión simple.	SI	SI	SI

[1] Fuente: http: //www. microsoft.com/ latam/ technet/ articulos/ Windows2k/ msppna/ default.asp.2004)

2.11 Túneles de VPN Anidados.

Los túneles de VPN anidados pueden considerarse como un túnel dentro de otro túnel. Existen muchas formas para hacer túneles anidados; una manera de emplearlos es cuando la organización quiere implantar seguridad punto a punto (Brown, 2001). La Fig. 4.6 ilustra un túnel anidado.

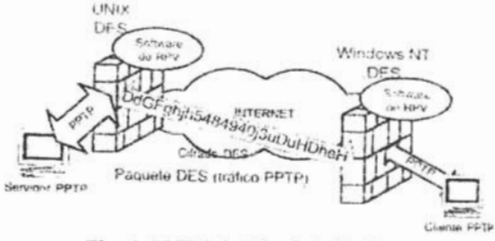


Fig. 4.6 VPN de Túnel Anidado.

En la figura 4.6, aparece un cliente PPTP que espera conectarse con el servidor PPTP, El proceso es el siguiente:

1. El cliente PPTP realiza el proceso de cifrado en los datos desde la aplicación.

2. Después, reenvía el flujo de datos cifrados al dispositivo de cortafuego/VPN, el cual añade cifrado DES al paquete. El cifrado DES puede implementarse como parte de la norma IPSec.

3. El paquete es recibido por el dispositivo remoto de la VPN, el cual revisa la autenticación, quita el cifrado DES y lo envía a su destino final que es el servidor PPTP.

4. El servidor PPTP descifra el paquete PPTP y lo reenvía a las aplicaciones de nivel superior.

Otra forma para realizar un túnel anidado podría ser con el uso de un algoritmo de clave pública como PGP. En este caso, el proceso es el siguiente:

1. El cliente podría utilizar la clave pública del servidor para cifrar un archivo de texto simple.

2. Los datos cifrados se enrutan al primer dispositivo de cortafuego/VPN para ser cifrados de nuevo con DES.

3. Se reenvía al dispositivo VPN remoto.

4. El dispositivo de cortafuego/VPN receptor ejecuta el proceso de descifrado y lo envía al servidor.

5. Un usuario en el servidor puede utilizar su clave privada para descifrar el mensaje.

Estas dos formas muestran cómo se puede crear un túnel anidado. Desde luego, siempre es posible utilizar otro algoritmo para realizar el cifrado, como el proceso de cifrado llamado Triple DES (3DES).

3.- Protocolos para Establecimiento de Túneles de Nivel 2 (L2TP).

El protocolo de túneles L2TP, ha nacido de la combinación de las características del protocolo PPTP y L2F (Layer 2 Forwarding). L2TP es un protocolo de red que facilita la creación de túneles para enviar tramas PPP. Encapsula las tramas PPP para que puedan ser enviadas sobre redes IP, X.25, Frame Relay o ATM. La carga útil de las tramas PPP, puede ser encriptada y/o comprimida. Se puede usar L2TP directamente sobre diferentes tipos de WAN, por ejemplo, Frame Relay, sin una capa de transporte IP. L2TP usa UDP y una serie de mensajes de L2TP para los mantenimientos de túneles sobre redes IP. L2TP permite múltiples túneles entre los dos puntos finales (Clark, 2001).

L2TP está compuesto de dos partes, el concentrador de acceso L2TP (LAC) y el servidor de red L2TP (LNS). El LAC se sitúa entre un LNS y un sistema remoto, manda paquetes a cada uno de los dos. El LNS es el par del LAC, y es un punto de terminación lógica de una sesión PPP que a la cual se le esta siendo aplicado el túnel desde el sistema remoto por el LAC. El L2TP soporta dos modos de túneles, el modo Obligatorio y el Voluntario.

L2TP usa el Protocolo de Control de Red (Network Control Protocol NCP) para asignar la IP y autentificar en PPP, llama comúnmente, PAP o CHAP. La seguridad en L2TP requiere para el transporte seguro es necesario que estén disponibles los servicios de encriptación, integridad y autentificación para todo el tráfico L2TP. Este transporte seguro opera en todo el paquete L2TP y es funcionalmente independiente de PPP y del protocolo que éste transporta.

Túnel Obligatorio L2TP:

- El usuario remoto inicializa una conexión PPP a un ISP.
- El ISP acepta la conexión y el enlace PPP se establece.
- El ISP solicita la autentificación parcial para saber el nombre de usuario.
- El ISP mantiene una lista de todos los usuarios admitidos, para servir el final del túnel.
- LNS.
- El LAC inicializa el túnel L2TP al LNS.
- Si el LNS acepta la conexión, el LAC encapsulara el PPP con el L2TP, y entonces.
- enviara a través del túnel.
- El LNS acepta estas tramas, y las procesa como si fueran tramas PPP.
- El LNS la autentificación PPP para validar al usuario y entonces asigna una dirección
- IP.

Túnel Voluntario L2TP:

- El usuario remoto tiene una conexión a un ISP ya establecida.
- El cliente L2TP (LAC), inicializa el túnel L2TP al LNS.
- Si el LNS acepta la conexión, LAC encapsula con PPP y L2TP, y lo manda a través del
- túnel.
- El LNS acepta estas tramas, y las procesa como si fueran tramas normales de entrada.
- el LNS entonces usa la autentificación PPP para validar al usuario y asignarle una IP.

4 -Protocolo de Seguridad en Internet.

IPSec está diseñado para proporcionar seguridad basada en encriptación para datagramas o paquetes IP (véase la Fig. 4.7). Para brindar seguridad, el estándar IPSec especifica dos protocolos de seguridad: El protocolo Encabezado de autenticación y el protocolo Encapsulamiento de carga de seguridad (Clark, 2001).

Fig. 4.7 formatos típicos de formato ip.

El protocolo Encabezado de autenticación (AH, Authentication Protocol) de IP proporciona autenticación de origen de datos, integridad sin conexión y un servicio antirrepetición opcional.

El protocolo Encapsulamiento de carga de seguridad (ESP, Encapsulating Security Payload) suministra encriptación y autenticación limitada, en comparación con AH, para datagramas de IP. Al igual que AH, ESP proporciona integridad sin conexión, autenticación de origen de datos y servicio de antirrepetición. Esta es una característica importante para protocolos sin conexión. Esta característica proporciona una barrera para rechazar ataques al servicio.

AH y ESP son los mecanismos que utiliza IPSec para proporcionar servicios de seguridad a datagramas de IP vinculados a Internet. En general, los dos protocolos de seguridad ofrecen tres clases de servicios:

1. Autenticación de encabezado (AH) y encapsulamiento de carga (datos transportados por paquete de IP) para proteger campos de información "en riesgo" en encabezados IP y cargas de paquete,

2. Autenticación y encriptación para protocolos sin conexión de más alto nivel como TCP y UDP. Por lo general, los protocolos sin conexión 1 proporcionan retroalimentación de "conexión con éxito" entre el emisor y el receptor. En una transmisión *sin conexión,* el protocolo del emisor sólo deposita la transmisión en la línea de comunicaciones. Si el sistema del receptor responde, la conexión tiene éxito. Si el receptor está desconectado y no se establece la conexión o, en el extremo, si la sesión es secuestrada, el emisor original del mensaje no recibirá respuesta, de ahí el nombre de protocolos sin conexión.

3. Autoprotección de los agentes de seguridad reales (parámetros);es decir, claves de encriptación, que negocian conexiones de IPSec.

4.1 Asociación de Seguridad del Modo de Transporte en IPSec.

En IPSEc cuando se habilita una conexión mediante AHo ESP, a la conexión resultante se le llama *asociación de seguridad* (AS). Bajo los estándares IPSec, las ASs son tipos específicos de modos de transmisión para paquetes de IP. A los dos modos de transmisión que utiliza IPSec para transferencia de seguridad se les llama *modo de transporte* y *modo de túnel.*

En modo de transporte, los servicios de seguridad se transmiten directamente al paquete mediante un encabezado de protocolo de seguridad de AH o ESP.

Durante la transmisión, el encabezado de protocolo de seguridad se coloca o anida después del encabezado IP original y de las opciones de destino, pero antes de la carga o los datos de IP. En el caso de AH, se proporciona protección al encabezado IP, las opciones seleccionadas y la carga de IP. En el caso de protección de ESP, sólo se encapsula la carga con servicios de seguridad (véase la Fig. 4.8). A veces los paquetes de IP también contienen encabezados de *extensión,* que por lo general aparecen después del encabezado IP de base pero antes de las opciones de destino. Cuando se incluyen encabezados de extensión, también se utilizará AH para autenticar esta parte del paquete.

Fig. 4.8 Seguridad Ip de modo transporte.

4.2 Asociación de Seguridad del Modo de Túnel en IPSec.

En el caso de modo de túnel, IPSec anexa un encabezado IP externo. Este suele incluir el destino del procesamiento o puerta de enlace de seguridad de IPSec. En el modo de túnel, hay dos casos en que ocurre transmisión de punto a punto entre dos puertas de enlace de seguridad o entre un host (cliente o servidor) y una puerta de enlace de seguridad. En contraste, IPSec no agrega un encabezado IP externo en modo de transporte, porque las asociaciones de seguridad a menudo se establecen entre dos anfitriones (para distinguir entre anfitriones y puertas de enlace de seguridad, los primeros suelen originar o terminar mensajes, mientras que las segundas transfieren mensajes).

En la transmisión, el encabezado de protocolo de seguridad se localiza detrás del encabezado IP externo pero antes del encabezado IP original y la carga de paquete asociada. La protección que proporciona AH es similar a la que se proporciona en el modo de transporte. La protección se extiende al encabezado IP externo y a todo el paquete de IP en túnel (encabezado IP interno/externo y carga de paquete). ESP, por otro lado, extiende servicios de seguridad sólo al paquete de IP en túnel, no al encabezado IP externo (véase la Fig. 4.9).

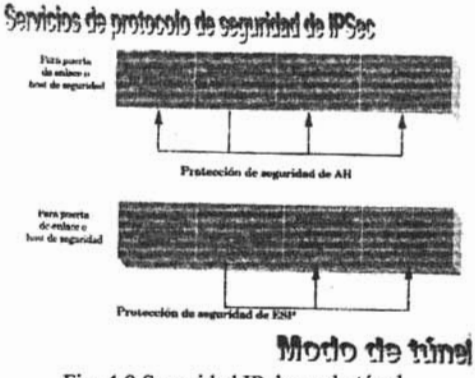


Fig. 4.9 Seguridad IP de modo túnel.

La estructura de paquete estandarizada y las asociaciones de seguridad son de los principales beneficios de las iniciativas de IPSec. Una estructura de paquete estandarizada facilita la interoperación de soluciones de VPN de terceros hacia abajo, al nivel de datagrama de IP o de transmisión. IPSec extiende servicios de seguridad a la capa de IP, lo que da como resultado protección para protocolos IP y de capa superior, como TCP y UDP, mientras viajan por Internet.

4.3 Intercambio y Administración de Claves de IPSec.

El sistema de administración predeterminado de IPSec para claves de encriptación es ISAKMP/IKE (Internet Security Association and Key Management Protocol/Internet Key Exchange, Protocolo de Asociación de Seguridad de Internet y Administración de claves/intercambio de clave de Internet). La administración de clave simple para IP (SKIP, Simple Key Management for Internet Protocol) es opcional. Entre otras cosas, los protocolos de administración de claves IPSec aseguran que ambos extremos de la VPN utilicen y desplieguen las mismas claves para autenticación y encriptación de paquetes IP. También aseguran que se intercambien las claves a intervalos regulares para reforzar integridad de transmisiones VPN de manera continua. Con claves de 40 bits, más débiles, el cambio de la clave a intervalos regulares es crítico, porque si se le brinda el tiempo suficiente, un intruso romperá el código encriptado.

La Seguridad de las VPN.

Capítulo V.- La Seguridad de las VPN.

1. Seguridad

Una VPN completa, normalmente incluye un componente crítico: la seguridad. Esto lo logra incluyendo tecnología en controles de acceso, autenticación y encripción, para poder garantizar la seguridad de las conexiones a los usuarios, principales aspectos de la privacidad e integridad de los datos (Scott et al. 1999).

En muchos artículos y documentos, se habla sobre la criptografía y cifrado al mismo tiempo. De hecho, se usan juntos con tanta frecuencia que es difícil hablar de ellos por separado. Criptografía es el arte de mantener las cosas en secreto, el algoritmo matemático. Cifrado, por su parte, es el marco de referencia. Pretty Good Privacy es el marco de referencia (el Algoritmo de cifrado de datos internacional (IDEA) es la criptografía. Aunque IDEA contiene la palabra cifrado, es un algoritmo de criptografía matemático.

2. ¿Qué es la criptografía?

"En términos simples, un proceso criptográfico toma un texto archivo de texto simple y lo convierte en un texto "cifrado" por un proceso de cifrado." (Brown. 2001).

El cifrado no es nada más que tomar un mensaje, por ejemplo "Llegaré tarde" convertirlo en argot, algo como "2deR56Gtr2345 hj5UieO4". El otro extremo de este proceso se llama descifrado y es el reverso del cifrado; por ejemplo al tomar "2deR56Gtr2345 hj5UieO4" y convertirlo de nuevo en "llegare tarde".

Al restablecer el texto cifrado a su forma original, éste sufre un proceso llamado descifrado, como se explicó anteriormente. El uso de la clave facilita ese proceso y el proceso de descifrado sólo puede ocurrir con el uso de la clave.

Todos los algoritmos de cifrado dependen de las funciones criptográficas.

2.1 Criptografía de Clave Privada Contra Pública.

Con la criptografía histórica, el emisor y el receptor de un texto utilizan la misma clave (la "clave secreta"). El emisor utiliza la clave secreta para cifrar el mensaje, mientras que el receptor utiliza la misma clave para descifrarlo. Este método se conoce como criptografía de clave secreta o criptografía simétrica. El principal problema aquí es la clave; el emisor y el receptor no sólo deben estar de acuerdo en usar la misma clave, sino que también deben idear una manera de intercambiarla. Si están en diferentes áreas geográficas, el intercambio de las claves se vuelve un gran problema. ¿El emisor y el receptor querrán confiar en una línea telefónica o en el correo para intercambiar las claves? ¿Pueden confiar en una compañía de correo? Ya que en la criptografía de clave secreta las claves son de extrema importancia, ¿puede confiarse en la seguridad, especialmente dentro de una organización grande?

Esta creación, distribución y seguridad se llama Administración de Claves. Para resolver el problema de la administración de claves, Whitfield Diffie y Martin Hellman introdujeron el concepto de criptografía de clave pública en 1976. En la criptografía de clave pública, cada parte obtiene un par de claves, una pública y una privada. La clave pública está hecha para que todos la conozcan mientras que la privada no. En la criptografía de clave pública se elimina la necesidad de un canal de seguridad. Además, los criptosistemas de clave pública permiten el uso de firmas digitales y de autenticación de datos.

La ventaja de utilizar criptografía de clave pública es la seguridad y la conveniencia. La clave privada nunca necesita transmitirse o confiarse a alguien más (por ejemplo, a un servicio de correo). Por lo tanto, no hay posibilidad de que la clave se comprometa ni de que la transmisión sea interceptada o decodificada.

Otra ventaja de los sistemas de clave pública es que proporcionan firmas digitales que no se pueden rechazar.

La desventaja de utilizar criptografía de clave pública es la velocidad, muchos algoritmos de cifrado de clave secreta son considerablemente más rápidos que los algoritmos de cifrado de clave pública. Sin embargo, la criptografía de clave pública se puede utilizar en conjunción con la criptografía de clave secreta para obtener los beneficios de ambos. Al trabajar con el cifrado la solución es combinar sistemas de clave pública y secreta para obtener seguridad de los sistemas de clave pública y las ventajas de velocidad de los sistemas de clave secreta.

2.2 Cifras de Bloque.

Una cifra de bloque es un cifrado que repite varias operaciones de sustitución, transposición, adición modular, multiplicación y transformación lineal en un algoritmo mucho más sólido. Este algoritmo de cifrado se efectúa con la clave del usuario especificada. El proceso de descifrado es lo opuesto a este algoritmo (Brown, 2001).

Existen muchas variantes de estos algoritmos. A una clase se le llama "Cifra Feistel". Ésta opera sobre una mitad del texto cifrado en cada repetición y luego intercambia las mitades del texto cifrado después de cada ciclo.

2.2.1 Norma de Cifrado de Datos (DES).

La Norma de Cifrado de Datos (DES), también es conocida como Algoritmo de Cifrado de Datos fue desarrollada por IBM (que originalmente la llamó "Lucifer"). El algoritmo DES utiliza un tamaño de 64 bits y una clave de 56 bits durante la ejecución (los 8 bits de paridad se quitan de la clave de 64 bits completa) (Mason, 2002). DEA es un criptosistema simétrico, específicamente una cifra Feistel de 16 ciclos. En una cifra de ciclo se aplica el algoritmo varias veces; en este caso, el algoritmo se completa 16 veces. Durante cada ciclo (también llamado transformación) se utiliza una subclave con el proceso de repetición.

Esta subclave es un derivado de la clave principal que el usuario suministró mediante una función especial en el algoritmo. El término "agenda de claves" se utiliza para indicar el juego de subclaves empleado en cada repetición.

El número de ciclos incrementa la seguridad, pero el contrapeso es el desempeño.

2.2.2 DES 3, TRIPLE DES y 3DES.

Triple DES es un conjunto de algoritmos para incrementar la fuerza del DES normal. Esto se lleva acabo al ejecutarse el algoritmo DES con una o más claves, como por ejemplo existen varios modos para 3 DES, tales como:

- DES-EEE3. Este es el algoritmo DES que se ejecuta 3 veces, cada una con una clave de cifrado diferente.
- DES-EDE3. Este algoritmo DES utiliza 3 claves de cifrado distintas, pero el proceso de cifrado es cifrar-descifrar-cifrar.
- DES-EEE2. Es similar a DES-EEE3 pero tanto el primer como el tercer proceso del cifrado utilizan la misma clave.
- DES-EDE2. Similar a DES-EDE3 pero la primera y la tercera repetición utilizan la misma clave.

Existen otras versiones de este proceso: repetición individual, doble o triple utilizando una o mas claves para cada proceso. La mayor solidez radica en el uso del algoritmo DES con tres claves distintas.

2.2.3 Algoritmo Internacional de Cifrado de Datos (IDEA).

El algoritmo IDEA es un cifra de bloque que se creó en 1990 por una compañía suiza. Utiliza 64 bits con ocho ciclos, en comparación con la cifra Feistel de 16 ciclos.

Como en las cifras de bloque, el descifrado es el mismo proceso que el cifrado una vez que todas las subclaves de descifrado se calcularon a partir de las claves de cifrado. Este cifrado se diseñó para una implementación fácil en hardware y software. La seguridad de IDEA se

basa en la utilización de tres tipos incompatibles de operaciones aritméticas en palabras de 16 bits. En este algoritmo, las operaciones de tres grupos algebraicos diferentes se mezclan (XOR, módulo de adición 216 y módulo de multiplicación 216+1). IDEA utiliza 52 subclaves, cada una comienza con una longitud de 16 bits. La generación de subclaves es como sigue: la clave de 128 bits de IDEA se utiliza como las primeras ocho subclaves K1 a K8. Las ocho siguientes se obtienen de la misma manera, después de un una rotación circular a la izquierda de 25 bits. Este proceso se repite hasta que todas las subclaves de cifrado se hayan calculado (Brown, 2001).

IDEA es un cifrado sólido que ha enfrentado muchos retos en su contra. Se considera inmune al criptoanálisis diferencial y no se han reportado ataques criptoanaliticos lineales. Aunque, existe una gran clase de claves débiles, 2 a la 51, que en el proceso de cifrado podrían permitir que se recuperara la clave. Sin embargo, IDEA todavía tiene 2 a la 128 claves posibles, lo cual hace que sea seguro.

2.2.4 RC2.

RC2 es una cifra de bloque con un tamaño de clave variable. "RC" son las siglas en inglés de "Código de Rivest", lo que hace referencia al autor Ron Rivest de RSA Data Security. El tamaño del bloque es de 64 bits y es aproximadamente 2 o 3 veces más rápido que DES cuando se implementa en software.

Debido a que el gobierno de los Estados Unidos restringió la exportación a 40 bits, el creador utilizo otro método que permite la exportación.

RC2 tiene una característica especial gracias a la cual una cadena especial (de 40 a 88 bits) puede adjuntarse a la clave de cifrado, esta cadena es llamada "sal", esta diseñada para detener a los atacantes y utiliza una clave de cifrado más larga. Después del cifrado, la sal se envía sin cifrar con el permitiendo así la exportación sin romper la Ley.

2.2.5 Cifra de Bloque RC5.

RC5 es diferente a los otros algoritmos RC debido a que utiliza un tamaño de bloque variable, un tamaño de clave diferente y un número de ciclos distinto. RC5 utiliza tamaños de bloque de 32, 64y 128 bits. La clave variable abarca de 0 a 2048 bits y el número de ciclos puede ir de 0 a 255. Es una cifra rápida y puede utilizarse con un tamaño de bloque de 64 bits que puede ser un reemplazo para DES. Esta flexibilidad de tamaño le da al RC5 una gran seguridad. La generación de subclaves se calcula con la clave definida por el usuario y el número total de subclaves depende del número de ciclos implementados. Después, la tabla se utiliza para cifrado y descifrado. La rutina consiste en tres operaciones algebraicas: adición de enteros, modo en bits OR exclusivo y rotación variable. Estas operaciones hacen que el RC5 sea fácil de probar e implementar. RC5 se ha probado contra ataques de criptoanálisis diferencial y lineal (Bronw, 2002).

2.3 Cifras de Flujo.

Las cifras de flujo son algoritmos de cifrado simétricos que normalmente son más rápidos que los de bloque. Mientras que las cifras de bloque trabajan con partes de datos (64 bits), las de flujo trabajan sobre bits individuales. Una buena característica de seguridad con las cifras de flujo es que aunque se utilicen el mismo algoritmo y la misma clave, tal vez no aparezca el mismo texto cifrado; eso depende del momento en que los bits se encuentran en el proceso de cifrado. Comparando con las cifras de bloque, en las cuales el uso del mismo algoritmo y la misma clave generan el mismo texto cifrado que se puede utilizar como un ataque de análisis de datos sostenido.

En lugar de texto cifrado como en el caso de cifras de bloque, las cifras de flujo producen lo que se conoce como flujo de claves. El proceso de cifrado utiliza tanto el texto simple como la clave de flujo (Brown, 2001).

2.3.1 RC4.

Es otra cifra de flujo, también desarrollada por Ronn Rivest de RSA Data Security, Inc. Utiliza una cifra de flujo de tamaño de clave variable con operaciones algebraicas orientadas a bytes. El algoritmo se basa en la utilización de permutación aleatoria. El cifrado se diseñó para ejecutarse rápidamente en el software y utiliza de 8 a 16 operaciones por byte. Junto con RC2, tiene un estatus de exportación especial por parte del gobierno de Estados Unidos.

2.3.2 Generador de Números Pseudoaleatorios Congruentes Mezclados.

El generador de números pseudoaleatorios congruentes mezclados por lo general se implementa en software. Es una técnica básica que produce bits aparentemente aleatorios. Es la misma técnica que se utiliza para producir los números que regresan cuando se usa la función aleatoria en la mayoría de los lenguajes que utilizan BASIC: módulo "a" constante, reemplazar n por "a" veces n más "b", donde "a" y "b" son constantes. Si a y b son lo suficientemente grandes, el comportamiento de n, sus bits más importantes, parecerá aleatorio. Un uso común para el generador de números pseudoaleatorios es utilizarse como parte del generador de números aleatorios MacLaren-Marsaglia.

2.3.3 Cifra Vernam

Una cifra Vernam, a menudo llamada "descartable", utiliza una cadena de bits que se genera de manera totalmente aleatoria. El flujo de claves tiene la misma longitud que el mensaje de texto simple y la cadena aleatoria se combina utilizando XOR en modo de bits con el texto simple para producir el texto cifrado.

Todo el flujo de claves es aleatorio, por consiguiente, aun con recursos computacionales de alto nivel, sólo se puede adivinar el texto solo si se dispone del texto cifrado. Estas cifras ofrecen confidencialidad las descartables son los mejores mecanismos de seguridad hoy en día. Ya que la clave secreta es tan grande como el mensaje puede causar problemas serios de administración de claves y, por tanto, la cifra descartable no es práctica. Las cifras de flujo se desarrollaron como alternativa frente a las descartables (Clark, 2001).

2.4. Message Digest 2 (MD2), 4 (MD4), 5 (MD5).

Ron Rivest de los Laboratorios RSA creó Message Digest 2, 4, 5. Son todas las funciones de transformación del código que toman una cadena de una longitud arbitraria y producen una salida de longitud fija de 128 bits.

MD2 se diseñó en 1989 y se mejoró para las máquinas microprocesadoras de 8 bits, se han descubierto algunos puntos débiles en el campo de mensaje de MD2 si algunos cálculos se dejaron incompletos durante la transformación del código. Por consiguiente, la implementación de MD2 ya no es recomendable.

MD4 se diseño en los años noventa y utiliza un bloque de 512 bits con el mensaje. Esta función de transformación de código utiliza 3 ciclos en su implementación.

MD5 se desarrolló en 1991 y aunque es más lento que MD4 se considera más seguro. Este algoritmo consiste en cuatro ciclos. Algunas personas reportaron puntos débiles en él, pero aun así se considera seguro y se usa ampliamente.

2.4.1 Algoritmo de Transformación del Código Seguro (SHA y SHA-1).

El gobierno de Estados Unidos desarrolló el Algoritmo de Transformación del Código seguro (SHA). SHA-1, una modificación del SHA, se lanzó en 1994 (Mason, 2002); este algoritmo toma una longitud de cadena y produce un compendio de de 160 bits. Aun cuando es más lento que otras funciones de transformación del código, se considera más seguro ya que tiene mayor longitud.

2.5 Sellos Digitales.

Cuando alguien recibe un documento, es importante estar seguro de la firma digital que verifica al emisor original y el sello que muestra la fecha y la hora en que se creó o se modificó el documento. Juntos, las firmas digitales y los sellos pueden actuar como notaría pública en un documento electrónico. Todos los documentos legales y las patentes necesitan que se les asigne un sello. Un ejemplo simple de sello es enviarse una carta a uno mismo y no abrirla. Dentro, los contenidos están a salvo de la manipulación y el sello que pone el servicio postal en el sobre es como el de una notaría pública (Clark, 2001).

Los documentos electrónicos almacenados en el disco duro de un servidor necesitan otro modo de documentar la fecha y la hora. Hasta ahora, al cambiar la fecha en la máquina no se afecta la fecha del documento. Por consiguiente, se necesita un modo de asignar sellos al texto electrónico y no al medio en el cual está almacenado. Una solución para el problema de los sellos es una autoridad confiable emisora de sellos, similar a una autoridad emisora de certificados. Un individuo enviaría el documento a una autoridad de sellos que sellaría el documento con la fecha y la hora, y lo regresaría. La autoridad conservaría una copia; si alguna vez hubiera una duda respecto a la fecha del documento, se podría consultar a la autoridad. Existen problemas con esta implementación; el documento puede ser interceptado o la autoridad de sellos tal vez no sea digna de confianza.

Una mejor manera de implementar sellos es en conjunto con las firmas digitales. Un individuo podría calcular una función de transformación del código, marcarla con su firma digital y enviarla a la autoridad de sellos. La autoridad adjuntaría la fecha y la hora, firmaría el mensaje y lo enviaría de regreso al individuo.

Esta es una forma simple pero exacta de considerar la asignación de sellos a un documento. Existen algoritmos adicionales disponibles que protegen contra las autoridades de sellos poco confiables y contra las autoridades que envían fechas y horas equivocadas.

2.6 Firmas Digitales con Autoridades Emisoras de Certificados.

Las firmas digitales funcionan de manera inversa al proceso de cifrado normal. La firma digital utiliza la clave privada en algunos bloques de datos (y sólo un individuo tiene acceso a su clave privada) y el receptor descifra esos datos con la clave pública que está disponible y es conocida. Cuando utilizamos firmas digitales, queremos tener certeza en la identificación del emisor; de otro modo, la firma se podría invalidar y no habría rechazo. Las firmas digitales también pueden utilizarse de otras maneras. Ya mencionamos su uso en la de sellos a documentos, donde la otra parte firma digitalmente los datos que vienen de un emisor con su clave secreta (Brown, 2001).

2.6.1 Cómo Funcionan los Certificados.

Un documento pasa a través de un compendio de (mecanismo de transformación del código). Este valor se cifra con la clave privada del individuo. La información resultante es la firma digital que se envía y almacena en una autoridad emisora de certificados. Después, reenvía el mensaje junto con su firma digital al receptor, quien descifra esta transformación del código con la clave pública del emisor. El receptor solicita la clave del emisor a la autoridad emisora de certificados, y te descifra el compendio.

Si la firma descifra adecuadamente y la transformación del código coinciden, la firma se acepta como valida. Las funciones de transformación del código criptográficas (como MD5 y SHA) se utilizan para calcular lo más importante del mensaje cuando se crea la firma digital (Clark.2001).

2.7 Clipper Chip.

Clipper Chip fue la respuesta del gobierno de Estados Unidos al cifrado de custodia de claves. Es un microchip que en el interior contiene hardware a prueba de falsificaciones que utiliza el algoritmo Skipjack. Cada chjp contiene una clave de unidad única de 80 bits que se deposita en dos partes en dos agencias de custodia, ambas partes se deben conocer para recuperar la clave. El chip se fabricó de tal manera que no pueda aplicársele ingeniería inversa, esto significa que el algoritmo Skipjack y las claves de cifrado no se pueden recuperar desde el chip. Utiliza tres tipos de clave de cifrado: una clave de sesión, una clave de unidad y una clave de familia.

Cuando dos dispositivos quieren iniciar una comunicación, primero, acuerdan una clave de sesión de 80 bits. El método usado se determina por la implementación; se pueden emplear métodos de clave pública como RAS o Diffie-Hellman. El mensaje se cifra con la clave de sesión y otra pieza de datos llamada campo de acceso de aplicación de la ley. En todo esto se incluye la clave de sesión, la clave de unidad y algunos otros datos, que se cifran con la clave de familia.

Durante una comunicación normal el emisor y el receptor cifran y descifran sus respectivos mensajes con las claves de sesión. Si una agencia de aplicación de la ley quiere escuchar la comunicación, puede utilizar la clave de familia para escuchar en secreto. Después podrá obtener un número de serie y una clave de sesión de cifrado. Con una garantía, la agencia puede obtener las dos partes de la clave de unidad y descifrar la clave de sesión, y por último emplear la clave de sesión para descifrar el mensaje.

Sin embargo, los investigadores de AT&T han mostrado que es posible modificar un campo en el algoritmo Skipjack, el Campo de acceso de aplicación de la ley (LEAF), lo que impediría que las agencias de aplicación de la ley determinaran la fuente original del mensaje.

3. Cifrado.

3.1 Cifrado de Clave Privada.

En el sistema de cifrado de clave privada (simétrico), se emplea la misma clave tanto para cifrar como para descifrar. La prioridad en la seguridad es darle al receptor esa clave en una forma segura. La Fig. 5-1 ilustra el clave privada.

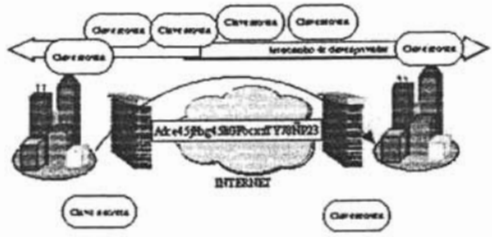


Fig. 5-1 proceso de cifrado de clave privada

En los sistemas de cifrado de clave privada, por ejemplo, DES la clave secreta cifra el mensaje. En este ejemplo el mensaje es "Mañana a las 9 a.m." Una vez cifrado, el mensaje se transporta a través de la red donde se emplea de nuevo la clave secreta para obtener el mensaje original se muestra en la figura 5-1, la clave privada debería ir por otro medio y debería transportarse por separado.

En un sistema de clave privada, la integridad de la clave es importante. Por lo tanto, es imperativo reemplazar periódicamente. El concepto denominado "secreto perfecto", donde las claves son renovadas frecuentemente, ayuda a limitar el daño debido a que sólo proporciona una pequeña oportunidad para ataques.

El problema con este tipo de sistemas es el número de claves que es necesario administrar.

En sistemas con pocas claves esto puede ser aceptable. Mientras más claves se necesiten, la administración y la distribución de claves se vuelve imposible. Por ejemplo, una organización que tiene 100 usuarios en una VPN podría significar que hay que manejar 4950 claves.

3.2 Cifrado de Clave Pública.

Los criptosistemas de clave pública utilizan una combinación de privada que el individuo mantiene en secreto y una clave pública disponible. Esta clave privada no es la mencionada anterioriormente en los criptosistemas de clave privada; la clave privada sólo descifra los mensajes que han sido cifrados con la clave pública asociada. Rivest Shamir Adleman y Diffie-Hellman (D-H) son dos sistemas de clave pública conocidos que se emplean actualmente en las VPN. La Fig. 5-2 ilustra un esquema de cifrado de clave pública Diffie-Hellman.

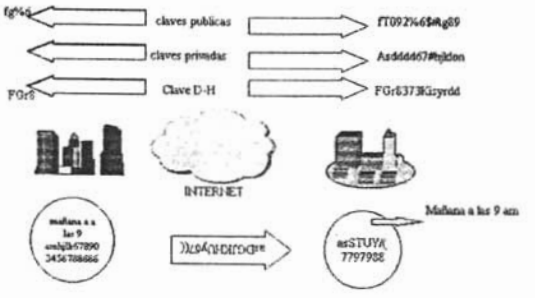


Fig. 5-2: Algoritmo de cifrado de clave publica Diffie-Hellman

En la figura 5-2 tanto el receptor como el emisor tienen claves Diffie-Hellman. El emisor obtiene la clave pública del receptor desde varias fuentes y cifra el mensaje "Mañana a las 9:00 a.m." con esta clave pública. Mensaje es enviado al receptor a través de una red pública. Entonces el receptor utiliza su clave privada en este mensaje y lo descifra. Nótese que se requieren tanto la clave privada como la pública para generar una clave D-H, así que si alguien le envía al receptor una clave pública diferente, la clave D-H tal vez no se genere y el receptor sabrá que algo ha pasado.

Esto no significa que fuera interceptada intencionalmente la causa puede deberse a ruido en la línea.

3.3 Claves Secretas Compartidas.

También es posible utilizar los criptosistemas de clave secreta puesto que son más rápidos, pero primero es necesario encontrar una forma para establecer una clave segura que sólo conozcan las dos partes. No se desea darle a la otra parte la clave secreta, pero es conveniente no depender sólo de las claves públicas. Ésta también es una característica de los criptosistemas de clave pública Diffie-Hellman. La Fig. 5-3 muestra cómo funciona este proceso.

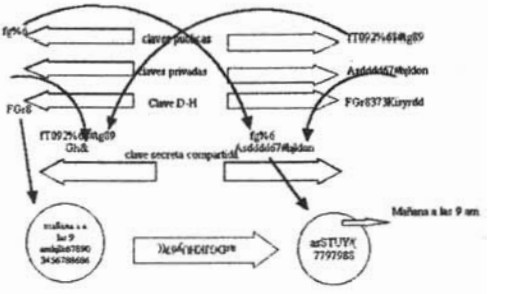


Fig. 5-3: Clave secreta compartida Diffie-Hellman

En la figura 5-3, el usuario A y el usuario B quieren comunicarse con un sistema de cifrado de clave secreta empleando primero el esquema de cifrado de clave pública Diffie-Hellman. Una propiedad del esquema de cifrado de clave pública Diffie-Hellman es que cualquiera de las dos partes que utilice la clave pública del otro generará los mismos resultados. En este ejemplo, el usuario A obtuvo la clave pública del usuario B y el usuario B obtuvo la clave pública del usuario A. Cuando realizan la función de cálculo de sus claves privadas individuales y de la clave pública del otro, obtienen el mismo resultado; en este caso, la clave secreta compartida fue lDfrT6543asdui&65678f. Esta es la clave secreta que emplearán las partes en comunicaciones seguras posteriores.

Sin embargo, continúa el problema de la primera comunicación entre los dos usuarios: compartir las claves públicas hace que la configuración sea vulnerable frente a lo que se conoce como el ataque de "intermediario" que se muestra en la figura 5-4. En este escenario, el usuario A intenta conseguir la clave pública del usuario B. El "intermediario" envía al usuario A su clave pública, afirmando que es el usuario B. Después, le envía su clave pública al usuario B, afirmando que es el usuario A. Conforme el tráfico pasa de un lado a otro entre el usuario A y el B, el intermediario intercepta y después los reenvía sin que los usuarios A y B sepan lo que sucede. Para evitar este tipo de violaciones de seguridad se requiere el uso de firmas digitales.

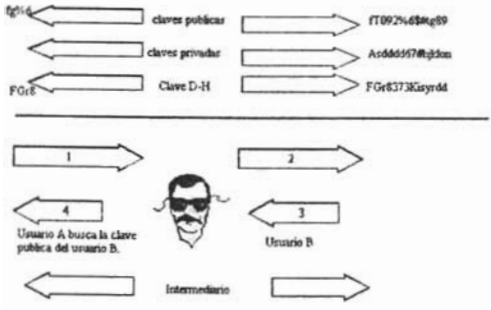


Fig. 5-4 : Ataque de intermediario.

3.4 Firmas Digitales.

Las firmas digitales son una forma de cifrado, pero que funcionan de una manera opuesta a como se piensa que funciona el cifrado. En el cifrado, sólo el receptor tiene la capacidad para descifrar el mensaje que está dirigido a él. También sucede lo inverso. Si un usuario cifra un mensaje con su clave privada, entonces el receptor puede descifrar el mensaje con la clave pública del emisor. Aun cuando el emisor no necesariamente cifre un mensaje, cifra un valor de transformación del código que se basa en el mensaje enviado. Si el receptor recalcula el mismo valor de transformación del código, sabrá que viene de ese emisor.

Cualquiera que tenga la clave pública del emisor, la cual está disponible, puede descifrarlo; sin embargo, sólo podrán descifrar el valor de transformación del código y no el mensaje en sí. Por lo tanto, si alguien escucha furtivamente, podrá estar seguro de que el emisor original envió un mensaje pero, debido a que el mensaje no se cifró con la clave pública, no podrá descifrarlo. En este caso, no hay que preocuparse por la seguridad de los datos, sino por quién los envió (Clark, 2001).

3.5 Autoridades Emisoras de Certificados (CA).

Siempre existe la posibilidad de un fraude en cualquier infraestructura de clave pública. En algunos casos, el atacante pretende ser alguien más como en el ataque de intermediario. Con el uso de las firmas digitales, se puede estar seguro de que alguien firmó el documento pero se necesita un tercero para asegurarse de que la firma es legítima. Ese es el papel de la autoridad emisora de certificados: asegurar quien dice ser (Brown, 2001).

Para obtener un certificado, esa persona presenta su clave a una autoridad emisora de certificados, junto con alguna pieza única de identificación de usuario. La clave pública, la pieza única de identificación y una identificación particular de la CA forman el certificado sin firma. Después la autoridad emisora de certificados tiene que firmar esta información.

Esto se realiza como sigue: la autoridad emisora de certificados transforma el código del certificado sin firma. Después, la CA toma el código transformado y lo cifra junto con su clave privada. Entonces, la CA adjunta esta firma al certificado original para crear el certificado firmado. Ahora, el usuario puede dar este certificado a cualquiera que lo necesite o puede adjuntarlo a su clave pública. Para que el receptor verifique esto, debe descifrar la autoridad emisora de certificados y con la clave pública para recuperar el código transformado original. Después, el usuario recalcula el código transformado de la firma, junto con el código recuperado en el primer paso.

Si ambos coinciden, entonces el receptor puede estar seguro que el certificado coincide con el emisor original. Este proceso ocurre durante la primera comunicación antes de una fecha de expiración o si el emisor revoca su clave pública. Una vez que el receptor almacena esta firma digital que ha sido verificada por la autoridad emisora de certificados, puede aceptar cualquier comunicación futura por parte del emisor que tenga su firma digital.

La Norma X.509 está recibiendo una aceptación universal para formatos de certificados con clave pública. Un certificado X.509 consiste en la clave pública del usuario y la firma de un tercero para la identificación en el bloque de información de ese usuario. Este tercero (autoridad emisora de certificados) puede ser una agencia gubernamental, una institución financiera o incluso un servidor confiable dentro de la oficina. El usuario le da a la autoridad emisora de certificados su clave pública y ésta responde con un certificado. Ahora el usuario puede publicar este certificado, junto con su clave pública, y cualquiera puede verificarlo con la autoridad emisora de certificados. La Norma X.509 también incluye otros elementos como un identificador que indica el algoritmo empleado para firmar el documento, la fecha de expiración del certificado y, en la última versión del X.509v3, es posible añadir información en circunstancias especiales. La Norma X.509 incluso permite revocar la clave antes de que expire. Algunas de las aplicaciones utilizadas por X.509 son IPSec, SSL, Transacciones Electrónicas Seguras (SET) y Extensión Segura de Correo Internet de Propósitos Múltiples (SIMIME).

3.6 Algoritmo de Clave Pública Diffie-Hellman.

En 1976, Whitfield Diffie y Martin Hellman publicaron un artículo titulado "New directions in Cryptography" (Nuevas tendencias en criptografía). Desde entonces se ha empleado su algoritmo de clave pública en todo el mundo. El protocolo de acuerdo de claves Diffie-Hellman (también llamado acuerdo exponencial de claves) es una generación de claves negociada.

Su fortaleza radica en el campo matemático finito de exponenciación de los logaritmos. El protocolo permite que dos usuarios intercambien una clave secreta en un medio inseguro sin secreto previo alguno. El algoritmo D-H también ha establecido la función de seguridad de un acuerdo de claves secretas, por lo tanto aunque sea un algoritmo asimétrico (clave-pública), tanto el emisor como el receptor pueden utilizar un algoritmo de cifrado simétrico. La figura 5-3 ilustra el concepto del acuerdo de clave secreta. Diffie-Hellman fue el primer algoritmo de clave pública desarrollado y continúa siendo muy popular (Brown, 2001).

Existen dos valores globales en el intercambio de claves Diffie-Hellman: P (que es un número primo) y G (comúnmente llamado generador). G tiene una propiedad especial: es un entero menor que P y puede generar todos los números entre 1 y P-1 al multiplicarse por sí mismo. Se hace referencia a G como módulo de P. Antes de que los usuarios puedan comunicarse entre si utilizando el intercambio de claves D-H necesitan acordar las mediante este procedimiento:

1. El usuario 1 genera un número privado X y el usuario 2 genera un numero privado Y.

2. Ambos generan valores públicos basándose en los valores privado y global que han elegido, P y G. La clave privada del usuario 1 es Gx mod P, y la clave privada del usuario 2 es Gy mod P.

3. Ahora intercambian sus claves públicas.

4. Después calculan sus claves secretas: el usuario 1 calcula Kxy= (Gy)x mod p, y el usuario 2 calcula Kyx = (Gx)y mod p. La operación logarítmica tiene la propiedad de que la clave secreta K a su vez tiene la propiedad Kxy=Kyx= K (la clave secreta); por lo tanto, ambos podrían tener la misma clave secreta.

La seguridad detrás de esto es tal que nadie más puede generar esta clave secreta. Sólo las partes que conocen los valores X y Y pueden generarla.

Muchos expertos en seguridad están de acuerdo en que es necesario un modulo sumamente grande en el intercambio de claves D-H de P y G; en la actualidad se recomienda un módulo de 1024 bits.

El intercambio de claves es vulnerable al ataque de intermediario. Este punto vulnerable existe debido a que el intercambio de claves D-H no autentica a los usuarios. Por lo tanto, se necesitan otros pasos para evitar estos ataques, tales como el de firmas digitales y las autoridades emisoras de certificados.

3.7 Algoritmo de Clave Pública RSA.

En 1977, Rivest Shamir Adelman (RSA) desarrolló lo que probablemente es el criptosistema de clave pública de uso más común en la actualidad. Se puede utilizar para cifrado y autorización, y tiene extensiones de 768, 1024 y mayores. La solidez de RSA proviene de la dificultad para factorizar primos grandes. RSA se utiliza ampliamente en aplicaciones de Internet como PGP y S/MIME (Mason, 2002).

RSA utiliza dos fórmulas matemáticas: la función de cifrado, la cual es CT =PTpub mod N, y una función de descifrado, PT=CTpriv mod N, donde PT el texto sencillo, CT es el texto cifrado, Pub es la clave publica y Priv es clave privada mod N. El módulo es el resto de una operación matemática modular por ejemplo, 125/6= 20.83, 125 mod 6 = 5.

Los pasos involucrados en los cálculos de RSA son los siguientes:

1. Se toman dos números primos grandes, por ejemplo, Pl y P2, y se multiplican para determinar su producto. En RSA se llama a este número M, o el módulo M = P1*P2.

2. Enseguida se elige un número, llamado Pub, el cual es menor que M, pero relativamente primo a (P1-1) (P2-1), lo cual significa que los números (Pub) y (P1-1) (P2-1) no tienen denominadores comunes para ellos mismos excepto 1.

3. Se encuentra otro número, por ejemplo Priv, con la propiedad de que (PubPriv-1) es divisible entre (P1-1) (P2-1).

4. Priv es el exponente privado de la clave privada (M, Priv) y Pub es el exponente público de la clave pública (M, Pub).

5. Los dos números primos grandes ya no son necesarios y pueden destruirse.

La seguridad de RSA está relacionada con las propiedades de factorización de números primos grandes y con la determinación de un conjunto de claves tales que la clave pública "Pub" es la inversa de la clave privada "Priv" con respecto a la exponenciación en el módulo M. Esto significa que (PTpub mod M)priv mod M= PTpubpriv mod M = PT. En otras palabras, el texto sencillo elevado a la potencia de la clave pública, módulo M, es igual al texto sencillo elevado a la potencia de la multiplicación de las claves pública y privada del módulo M, lo cual es igual a texto sencillo. El Totient de Euler (ET) ayuda a determinar el conjunto de claves de modo que se cumplan las condiciones anteriores; el totient es el conjunto de números entre 1 y M-1 que son relativamente primos a M; por lo tanto, para determinar ET(M) es necesario conocer los factores primos de M.

El totient de Euler toma en cuenta dos teoremas de la aritmética:

- Teorema fundamental de la aritmética. Este teorema establece que cada número no primo (números que son divisibles entre 1 y entre sí mismos) puede representarse como el producto de un conjunto único de números primos.

- Primos relativos. Dos números son relativamente primos si existe la condición de que no tengan factores primos comunes.

Por lo tanto debe encontrarse este conjunto único de factores primos de N para calcular el cociente de Euler ET(M). Encontrar estos primos es prácticamente imposible para un valor de M muy grande lo cual hace que RSA sea tan seguro. El objetivo principal detrás de esto es que con un módulo M (que un ordenador puede generar) y Pub (la clave pública ya disponible) no puede determinarse Priv (la clave privada) y por lo tanto descifrar un mensaje.

RSA es extremadamente seguro, no sólo porque ha probado serlo, sino porque aún no se inventan algoritmos matemáticos para resolverlo. Existe otro tipo de especulaciones en el sentido de que utilizar un algoritmo pudieran encontrar la raíz pública de mod M sería más fácil que factorizar pero de nuevo aún no existe tal algoritmo y RSA ha resistido a miles de intentos por descifrarlo (Mason, 2002).

3.8 Pretty Good Privacy (PGP).

Pretty Good Privacy (PGP) de Philip Zimmermann se ha empleado por todo el mundo. Pretty Good Privacy criptosistema híbrido, con todas las ventajas. Combina un algoritmo privado con uno de clave pública. Esto le da tanto la rapidez de un simétrico como las ventajas de un sistema asimétrico. Por lo que concierne a los usuarios, PGP actúa como cualquier otro criptosistema de clave publica; utiliza el algoritmo de clave pública RSA e IDEA para el cifrado. Se emplea una sola clave IDEA para cifrar el mensaje, y se utiliza la misma para descifrarlo (cifrado simétrico). Después se utiliza RSA para cifrar la clave IDEA usada para el cifrado con la clave pública del emisor (asimétrico). El receptor emplea su clave privada para descifrar la clave IDEA cifrada con RSA posteriormente esta clave IDEA descifrada se emplea para descifrar del mensaje. Junto con PGP, Zimmermann creó un conjunto de utilerías para administrar un anillo de claves públicas donde los usuarios pueden manejar distintas claves públicas (Clark, 2001).

La figura 5-5 ilustra un ejemplo de una comunicación PGP para los usuarios A y B. El mensaje es "Mañana a las 9:00 a.m". El proceso E sigue:

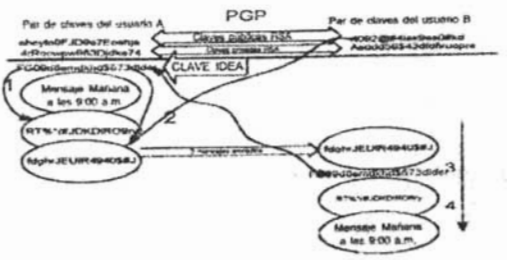


Fig. 5.5: comunicación PGP.

1. El usuario A cifra el mensaje "Mañana a las 9:00 a.m". con la clave de cifrado IDEA.

2. El usuario A cifra la clave IDEA con la clave pública RSA del usuario B.

3. El mensaje, que consiste en el mensaje cifrado IDEA y en la clave IDEA cifrada con RSA, se envía al usuario B.

4. El usuario B utiliza su clave privada RSA para descifrar la clave cifrada.

5. Finalmente, el usuario B descifra el mensaje original con la clave descifrada.

PGP se ha desarrollado con una aplicación de interfaz amigable que existe actualmente en muchos equipos de escritorio con todo tipo de aplicaciones. Su popularidad y facilidad de uso, junto con la solidez de la seguridad RSA, lo convierten en una herramienta de seguridad muy valiosa.

3.9 Infraestructura de Claves Públicas (PKI).

La Infraestructura de claves públicas (PKI) es un sistema de certificados digitales, autoridades emisoras de certificados (tanto comerciales como gubernamentales), servicios de administración de certificados y directorio (LDAP, X.500) que verifica la identidad y la autoridad de cada parte involucrada en cualquier transacción a través de Internet. PKI es la estructura que proporciona servicios de firmas digitales y privacidad como apoyo al comercio internacional, equilibrando las necesidades gubernamentales y asegurando la privacidad (Brow,2001).

Algunos usos de PKI incluyen:

- Autenticación y autorización.
- Privacidad y confidencialidad.
- Integridad de los datos.
- Sin rechazos.
- Servicios de directorio tales como X.500 y LDAP.
- Transmisión de documentos.
- Transacciones legales y financieras.
- Recuperación y almacenamiento de documentos.

PKI se está integrando en aplicaciones que soportan la seguridad en una amplia gama de servicios de Internet, por ejemplo, el correo electrónico, los documentos WWW y LDAP. Los certificados que unen al usuario con sus claves públicas (y que por lo tanto pueden revelar la identidad del usuario) juegan un papel importante en PKI. Con PKI y el uso de certificados, se efectuarán electrónicamente acciones tales como el otorgamiento de permisos para firmar cheques electrónicos, para que los bancos hagan efectivos los cheques electrónicos y para probar la identidad. Para que esto ocurra, el certificado que une al usuario con su clave pública deberá contener información acerca de dicho usuario. La información contenida en PKI incluirá:

- Identificación de quién ostenta el certificado
- Número de serie del certificado.
- Fecha de expiración del certificado.
- Copia de la clave pública del usuario y de su firma digital.
- El nombre de la autoridad que certifica y su firma digital.

Aun cuando PKI promete mucho, existen temas sin solución en el empleo cotidiano de PKI a gran escala que afectan la interoperabilidad, la facilidad de manejo y la capacidad de crecimiento. El primero es que aún existen varias normas, incluyendo las Normas criptográficas de clave pública (PKCS) de ESA Data Security y los certificados digitales que proporciona X.509. Los formatos de los certificados difieren: existen certificados X.509, certificados X.509 de Transacción electrónica segura (SET), claves PGP firmadas y certificados SPM. Así que, ¿cuáles soportarán los proveedores? Un aspecto relevante de los grupos PKI involucra a la administración y la anulación de certificados.
En general, una infraestructura PKI tiene la seguridad y flexibilidad para aprovechar las aplicaciones que se desarrollan actualmente, por ejemplo, VPN de Extranet, comercio electrónico y LDAP.

4. Comunicación y Autenticación Seguras.

La autenticación es un factor importante en la configuración de una VPN. Aunque , así como existen distintas arquitecturas, topologías y esquemas de cifrado en las VPN, también hay muchos esquemas de autenticación. Decidirse por alguno depende de la necesidad. Existen dos aspectos: la autenticación ("¿quien tiene el permiso?") y la autorización ("¿a qué tiene acceso?") (Clark, 2001).

4.1 Protocolos de Autenticación.

En cualquier infraestructura de comunicaciones en red existe la un proceso de autenticación que permita que el usuario acceda a de red y que impida, al mismo tiempo, el acceso no garantizado de los usuarios sin autorización.

Esto requiere de una configuración de confianza de dos sentidos: el sistema debe confiar en el usuario y el usuario debe confiar en otros usuarios del sistema (por ejemplo, al emplear alguna clave pública). Para que el sistema gane la confianza del usuario, el usuario deberá ser capaz de probar que es quien dice ser. Esto requiere algún tipo de proceso de autenticación.

El sistema que permite que estas comunicaciones se realicen utilizan los protocolos de autenticación, muchos de los cuales ya están disponibles actualmente. Se pueden encontrar al iniciar una sesión en su ordenador, en una red, utilizar un cajero automático para retirar dinero, etcétera. Estos protocolos son de distintos tipos, pero muchos utilizan el viejo principio de verificación con una o varias contraseñas. Lo que es distinto es quién tiene la contraseña y cómo se transfiere la información del cliente al servidor. En los sistemas de contraseñas normales, tanto el sistema como el usuario conocen la contraseña. Generalmente, si alguien se registra en el sistema del ordenador, éste tiene almacenada la contraseña de la persona junto con su identidad dentro de una base de datos. La persona proporciona su contraseña y, si coincide con la contraseña que se encuentra en la base de datos del ordenador, se inicia la sesión.

Sin embargo, esto obliga a que las contraseñas se almacenen en algún lugar, en este caso, en un archivo del servidor. Ahora no sólo tiene que preocuparse por la seguridad del servidor, sino también por el archivo en ese servidor. En los sistemas más recientes se utiliza una función de transformación del código de un sentido, en lugar del archivo. Una función de transformación del código de un sentido es un algoritmo criptográfico que permite crear un valor de transformación del código en una dirección, pero ir en la dirección inversa (por ejemplo, al encontrar la contraseña de texto sencillo a partir del valor de transformación del código) es imposible en términos de computación.

Incluso estas funciones de transformación del código de un sentido no tienen garantía de ser 100 por ciento invulnerables.

Al ejecutar un programa que compute miles de valores de transformación del código basados en las contraseñas y al comparar estos valores, es posible adivinar cuáles son algunos de esos valores. Las contraseñas no son cadenas muy extensas, por lo que no se necesita un sistema de ordenadores muy poderoso para lograrlo. Algunas de estas funciones de transformación del código también agregan el valor de una sal (se habló de las sales en el RC2) a las cadenas para hacerlas mas complejas. Si esta sal es lo suficientemente extensa, entonces se considera que el potencial de un ataque tipo diccionario está casi eliminado.

Después de las contraseñas, los servicios de autenticación se orientan hacia el modelo cliente/servidor de autenticación empleando un Servidor de acceso a red (NAS). Este NAS es el ejecutor (intermediario) de la autenticación y de la autorización del cliente; el servidor de seguridad sólo se encarga de la configuración de los usuarios. Por consiguiente, debe haber un conjunto de reglas que indiquen la forma en que el NAS y el servidor de seguridad pueden comunicarse entre si, en beneficio del cliente. Por lo general, este conjunto de reglas de comunicación se llama protocolo de autenticación. Existen muchos protocolos de autenticación de distintos tipos de proveedores.

Los servidores de red y los servidores de seguridad son diferentes; por lo tanto, las elecciones que se hagan dependerán de los aspectos de interoperabilidad y del compromiso con las normas abiertas.

4.2 Contraseñas del Sistema Operativo.

Las contraseñas continúan siendo la forma más común en los procesos de autenticación de usuarios en la actualidad. Se emplean para controlar el acceso a la información, desde sencillos registros de red hasta números de identificación personal (NIP) que se usan en los cajeros automáticos. No importa que se escriba sobre la falta de seguridad en los archivos de contraseñas se emplean mucho porque su instalación y su implementación son sencillas, económicas y convenientes.

Al mismo tiempo, las contraseñas son famosas por que se trata de una forma de protección sumamente pobre. Los consejeros de seguridad que cerca de un 80 por ciento de los incidentes de seguridad reportados se relacionan con contraseñas elegidas pobremente. Las fallas de la seguridad de las contraseñas son muy peligrosas debido a que un solo ordenador puede tener cientos o miles de cuentas protegidas con contraseñas. En las redes interconectadas de la actualidad, las consecuencias pueden ser devastadoras. Un intruso hábil podría irrumpir en el sistema no para destruirlo sino para usarlo como punto de partida para ataques a otros objetivos.

Por lo tanto, si se insiste en utilizar un archivo de contraseñas, ya sea como opción o debido a la carencia de recursos, al menos tome las precauciones necesarias para proteger a su servidor de los ataques.

Lo que no debe hacer:

- NO utilice su nombre de registro de ninguna forma (escrito como esta invertido, en mayúsculas, duplicado, etcétera).
- NO utilice su nombre ni sus apellidos de ninguna forma.
- NO emplee el nombre de su esposa ni los de sus hijos.
- NO emplee ninguna información que se pueda obtener fácilmente acerca de usted. Esto incluye su número de licencia, número telefónico, número del seguro social, la marca de su automóvil, el nombre de la calle donde vive.
- NO utilice una contraseña que sólo tenga números o letras.
- NO utilice una palabra contenida en diccionarios de ningún idioma ni en otro tipo de lista de palabras.
- NO utilice una contraseña con menos de seis caracteres.

Lo que sí se debe hacer

- Utilice una contraseña con mayúsculas y minúsculas.
- Utilice una contraseña con caracteres no alfabéticos (dígitos o puntuación).
- Utilice una contraseña que sea fácil de recordar, de modo que no tenga que escribirla.
- Utilice una contraseña que pueda escribir rápidamente, sin que tenga que mirar el teclado.

Al seleccionar las contraseñas, es importante recordar que debe haber un intercambio: elija una que sea fácil de memorizar para que no tenga que anotaría en algún lado, pero lo suficientemente restrictiva como para mantener alejados a los intrusos potenciales. El objetivo es hacerla lo más difícil posible para que el intruso no pueda adivinar qué contraseña eligió. Esto deja al intruso potencial sin otra opción más que la búsqueda por fuerza bruta, probando con todas las combinaciones posibles de caracteres ASCII. Una búsqueda de este tipo puede consumir mucho tiempo, y eso le proporcionará la oportunidad para detectar si alguien quiere irrumpir en su sistema.

4.3 S/KEY.

S/KEY es un algoritmo de software que fue desarrollado por Bellcore Laboratories y se describe en el RFC-1760, una parte del cual se cita a continuación:

Las contraseñas descartables del sistema S/KEY tienen una extensión de 64 bits. Esto se basa en la creencia de que son lo suficientemente extensas como para ser seguras y lo suficientemente cortas como para introducirlas manualmente... cuando sea necesario. El sistema S/KEY aplica funciones de transformación del código varias veces, produciendo una salida final de 64 bits.

MD4 acepta un número arbitrario de bits como entrada y produce una salida de 128 bits. Las funciones de transformación del código seguras de S/KEY consisten en aplicar MD4 a una entrada de 64 bits y plegar la salida de MD4 con la función O exclusiva (XOR) para producir otra salida de 64 bits.

4.4 Servicio de Marcación para Autenticación de Usuarios Remotos (RADIUS).

El Servicio de marcación para autenticación de usuarios remotos, o es un sistema de seguridad distribuida que garantiza el acceso remoto y servicios de redes frente al acceso no autorizado, al emplear el protocolo UDP. La autenticación RADIUS incluye dos componentes: un servidor de autenticación y protocolos de cliente. El servidor se instala en una maquina en el sitio del cliente. Toda la información sobre la autenticación de usuarios y acceso a los servicios de la red se localiza en el servidor RADIUS. RADIUS permite distintos formatos que pueden adaptarse a los requisitos de un cliente individual. Un servidor RADIUS autenticará a los usuarios utilizando un archivo de contraseñas UNIX®, el Servicio de Información de Red (NIS) de Sun Microsystems o una base de datos RADIUS administrada en forma independiente. El modelo RADIUS trabaja en el cliente enviando solicitudes de autenticación al servidor RADIUS, además de que actúa en los reconocimientos que envía el servidor (Goralski-Waclowski, 1999).

RADIUS autentica a los usuarios a través de una serie de comunicaciones entre el cliente y el servidor. A continuación se muestran los pasos involucrados en una comunicación RADIUS típica que emplea un servidor de comunicación RADIUS:

1. Desde un equipo portátil, un usuario marca a un módem conectado al servidor RADIUS de comunicaciones por marcación. Una vez que se completa la configuración de la conexión, la marcación le solicita al usuario su nombre y su contraseña.

2. El servidor de marcación crea un paquete de datos a partir de información, conocido como solicitud de autenticación. Los datos incluyen información para identificar la marcación específica que envía la solicitud de autenticación, el puerto de donde proviene la comunicación el nombre del usuario y su contraseña. Para ofrecer seguridad adicional el servidor de marcación, que actúa como un cliente RADIUS, cifra la contraseña antes de enviarla al servidor RADIUS.

3. La solicitud de autenticación se envía desde el cliente RADIUS hasta el servidor RADIUS. RADIUS permite varios servidores y, dependiendo de la topología de la red, los clientes pueden enrutar sus solicitudes de distintos servidores.

4. Cuando el servidor RADIUS recibe la solicitud, el servidor valida y descifra el paquete de datos para tener acceso a la información del nombre de usuario y de la contraseña. Esta información se pasa a los sistemas apropiados que manejan la seguridad, como puede ser una base de datos de usuarios controlada localmente.

5. Una vez que se verifican el nombre de usuario y la contraseña, el servidor envía un reconocimiento (llamado "reconocimiento de autenticación") que incluye información sobre el sistema de red del usuario y los requisitos del servicio. Esto quiere decir que el servidor RADIUS puede decirle al servidor de marcación que el usuario sólo tiene permiso para acceder a un anfitrión específico de la red.

6. Si el nombre de usuario y la contraseña son incorrectos, el servidor RADIUS le envía un "rechazo de autenticación" al dispositivo de marcación, por lo que se le niega el acceso a la red a ese usuario.

7. Para protegerse contra intrusos, especialmente del ataque de intermediario, el servidor RADIUS envía una clave de autenticación, o firma, que los identifica con el cliente RADIUS.

8. Con esta información, el servidor de marcación le permitirá o rechazará los servicios de red al cliente.

El servicio RADIUS no está limitado a servicios de marcación. Muchos proveedores de cortafuegos soportan el uso de servidores RADIUS. Por lo tanto, si se decide por éste, puede tener a sus usuarios de marcación y a sus usuarios de VPN autenticados en el servidor RADIUS.

4.5 Kerberos.

Kerberos V5 es un protocolo de autenticación confiable fabricado por un tercero que permite que un proceso se ejecute en un cliente para demostrar su identidad frente a un servidor Kerberos, sin tener que enviar los datos a través de la red, lo cual permitiría que un atacante o un verificador, se hicieran pasar por un director. Se desarrolló a mediados de la década de los 80 como parte del proyecto Athena del MIT y se describe en el RFC-1510. El protocolo Kerberos se basa en el protocolo de autenticación de Nedham y Schroeder, pero se modificó para soportar distintas funciones en entornos diferentes .El nombre Kerberos viene de la mitología griega, del perro guardián de tres cabezas llamado Cancerbero que pertenecía a Hades (Brown, 2001).

Kerberos es un sistema de cifrado DES simétrico. Utiliza una función de clave privada centralizada y en el núcleo del sistema se encuentra el centro de distribución de claves (KDC). El sistema de autenticación Kerberos utiliza una serie de mensajes cifrados para demostrarle a un verificador que el cliente se ejecuta en beneficio de un usuario. KDC maneja centralmente a los usuarios y los servicios, los cuales se llaman directores Kerberos no utilizan contraseñas en el sentido normal en lugar de eso emplea credenciales y claves de sesión.

Los directores contactan al KDC para conseguir credenciales de manera que puedan tener acceso a los servicios de red.

4.6 Certificados.

Los certificados son simples estructuras de datos que contienen información. En los certificados no sólo nos preocupa la información, sino el hecho de identificar positivamente algo, ya sea un usuario o un dispositivo. Cuando se habla de identificar positivamente algo, se hace referencia al concepto de sin rechazos y, en este contexto, también al concepto de relacionar una clave pública con un sujeto. Puede pensar en los certificados digitales como en un pasaporte que se emplea para comprobar una identidad (Goralski-Waclowski, 1999).

El contenido de los certificados digitales es el siguiente:

- La identidad de quien ostenta el certificado.
- El número de serie del certificado.
- Una fecha válida e inamovible para la transacción.
- La fecha de expiración del certificado.
- Una copia de la clave pública de quien ostenta el certificado para cifrar y/o firmar.
- La identidad de la autoridad emisora de certificados y su firma digital.
- Nombre del grupo.
- Estado, ciudad.

4.6.1 Normas de los Certificados.

Los certificados digitales se basan en las recomendaciones de la Serie X de la Unión Internacional de Telecomunicaciones, en las normas ITU-X.509 y en "PKCS #7, Norma de sintaxis criptográfica de mensajes" de RSA. Actualmente, los certificados digitales X.509 han sido revisados en la versión propuesta X.509v3. Algunas de las modificaciones a las normas X.509 han sido:

- X5O9v1. La versión 1 definió un conjunto muy sencillo de atributos, llamado información de clave pública. Sin embargo, todavía había aspectos relacionados con la seguridad en la versión 1. Muy pocas plataformas soportaban la versión 1 y ésta no crecía muy bien.

- X.509v2. Se añadió algo más de información acerca del tema y de la autoridad emisora de certificados, pero seguía sin tener gran aceptación.

- X.509v3. La versión agregó extensiones de prioridad; por lo tanto se podían añadir información de la clave pública y atributos adicionales, si era necesario. Las listas de revocación de certificados también se agregaron. La versión 3 es aceptada por el gobierno y empresas comerciales de los Estados Unidos.

Actualmente, con la aceptación de X.509v3 y la Infraestructura de Clave Pública (PKI), los negocios serán capaces de conducir sus transacciones comerciales empleando certificados digitales dentro del sistema PKI desde sus estaciones de trabajo, mediante el uso de navegadores web y de una aplicación LDAP (por ejemplo, una base de datos).

4.6.2 Obtención de un Certificado.

En la mayoría de los casos, no es necesario obtener un certificado; es posible utilizar el certificado de firma digital que se incluye en el servidor seguro. Los certificados digitales incluyen información sobre el propietario del certificado por lo tanto, cuando los usuarios visitan un sitio web seguro, el navegador revisa la información en el certificado para ver si coincide con la información del sitio que se incluye en el URL. A veces aparece un cuadro advirtiendo que hay un problema y alguien puede estar tratando de interceptar las comunicaciones.

Es posible que esto sea cierto, pero generalmente es más probable que el nombre del sitio sea incorrecto, o el nombre de dominio esté equivocado y, cosas por el estilo.

Suponiendo que se quiere conseguir un certificado propio. Todo lo que se debe hacer es ir a uno de los muchos sitios que expiden certificados (éstas son autoridades emisoras de certificados) y comprar uno. Los certificados tienen precios distintos dependiendo del tipo de certificado que quiera. A continuación aparece una pequeña muestra de los certificados disponibles:

- Clase A, 1, Premium, Avanzado. Estos certificados digitales tienen un alto nivel de seguridad. Por lo general se usan para sitios habilitados para SSL y SOCKS, ofrecen seguridad de alto nivel para aplicaciones MIME, transacciones financieras, comercio electrónico mejorado y otras aplicaciones seguras.

- Clase B, 2, Medium, Básico. Éstos son certificados digitales con seguridad de nivel medio. Se utilizan para acceder a sitios habilitados para SSL, proporcionan seguridad de nivel medio para aplicaciones S/MIME comercio electrónico mejorado, compras en línea, periódicos, etcétera.

- Clase C, 3, Basic, correo gratuito. Estos certificados digitales ofrecen seguridad básica. Se usan para pedidos por correo electrónico y para correo personal seguro.

- Clase D o 4 (encadenada). Este tipo se utiliza en organizaciones de propósitos múltiples y es muy parecido a la licencia multiusuario.

La razón por la que hay nombres muy diferentes se debe a que las distintas CA nombran de diferente manera sus certificados y algunos se traslapan. La Clase A en una CA es lo mismo que la Clase 1 para otra CA.

En un sitio, una Clase B es comparable a la Básica de otro sitio, incluso la Básica de una CA es similar a la Clase C de otra CA. Además, los precios varían considerablemente. Van desde gratis hasta $100 USD por certificado, con ciertas rebajas cuando se compran varios certificados (esto se conoce como Encadenada o Clase D). Mientras más alto sea el nivel del certificado que requiera, más pruebas tendrá que proporcionarle a la CA, lo cual significa un costo mayor. Por ejemplo, si quiere un certificado Clase A, o Premium, porque va a realizar transacciones financieras en Internet, la CA debe asegurarse que el usuario es quien dice ser, lo cual involucra un escrutinio mayor en distintas bases de datos para corroborar la información que el usuario proporcionó y, por lo tanto, costos más altos y tal vez una mayor responsabilidad legal. Se ha hablado de la revocación de certificados; la CA se asegurará de revocarle el certificado una vez que se indique o en el caso de una falla de seguridad.

Las autoridades emisoras de certificados son compañías independientes y no conceptos ni algoritmos de software. Esto significa que un intruso puede penetrar y forzar el sistema de una CA igual que cualquier otro sitio. Mientras más sólida sea la infraestructura de la CA, más sólida será la protección.

4.7 Tarjetas Inteligentes.

Una tarjeta inteligente es muy parecida a la tarjeta de crédito que se lleva en la billetera. Es una tarjeta de plástico del tamaño de una tarjeta de crédito que tiene un pequeño chip incrustado. Las tarjetas inteligentes proporcionan portabilidad de datos, seguridad y conveniencia. Con ellas se emplean tres términos:

1. Una tarjeta IC con interfase ISO 7816.
2. Procesador de tarjeta IC.
3. Señal de identificación personal que contiene IC.

El término tarjeta inteligente viene del francés. Aunque investigadores en Estados Unidos, Japón y Austria trabajaban en las tarjetas inteligentes, fueron los franceses quienes hicieron una fuerte inversión en esta tecnología. El francés Roland Moreno causó un gran impacto en la tecnología de tarjetas inteligentes en los setenta, durante un periodo de inversión nacional importante para la modernización de la infraestructura tecnológica de su nación. Una compañía llamada Bull obtuvo cerca de 60 patentes relacionadas con las tarjetas MP; se llamaban "carte a memoire" o tarjetas de memoria. Francia comenzó a exportar esta tecnología a mediados de los 80, Roy Bright de la organización mercantil Intelimatique del gobierno francés creó el término "tarjeta inteligente" (Brown, 2001).

Una tarjeta inteligente es un dispositivo de control de acceso que soporta distintas aplicaciones. Permite que los usuarios tengan acceso a datos personales y empresariales, que realicen adquisiciones, y que ayuden a los negocios a evolucionar y expandir sus productos y servicios en un mercado global en constante cambio. Los bancos, las instituciones financieras, las empresas de telecomunicaciones, las compañías de software y las aerolíneas son algunas de las empresas que tienen la oportunidad de adaptar las tarjetas inteligentes a sus productos y servicios individuales. Actualmente, existen más de mil millones de tarjetas inteligentes y los pronósticos indican que pronto habrá más de dos mil millones. Anualmente el número de estas tarjetas crece a una tasa del 30 por ciento, principalmente fuera de Estados Unidos. El crecimiento de servicios se concentra en áreas como servicios telefónicos digitales inalámbricos, teléfonos de paga, telefonía inalámbrica, acceso a Internet servicios bancarios asistencia médica y televisión de pago por evento.

4.8 Protocolo Ligero para Acceso a Directorio (LDAP).

El Protocolo Ligero para Acceso a Directorio (LDAP) es un protocolo extensible que sirve para acceder a la información dentro de un directorio: sin embargo, la estructura del directorio dentro de LDAP no es la misma que un directorio normal. En un directorio normal, por lo general se tiene una vista estática del contenido del directorio, donde el contenido se crea, modifica y elimina con el tiempo. Al comparar esto con un directorio LDAP donde es posible almacenar fotos, certificados, URL y cosas por el estilo) se puede ver que la estructura de LDAP está viva con todo tipo de datos que pueden almacenarse dentro de ella. LDAP puede definirse para grupos de personas, por lo tanto es posible tener un punto de acceso para los distintos tipos Algunas de las normas de LDAP definen:

- El protocolo de red para tener acceso a esta información
- Un espacio de nombre, que determina cómo se hace referencia a información
- Cómo está organizada la información dentro del directorio
- Un modelo distribuido (en LDAPv3)

LDAP nació del Protocolo para Acceso a Directorio (DAP) de X.500, comenzó en 1988. El DAP de X.500 definía un conjunto de protocolos en un sistema abierto que le proporcionaba a los usuarios y las máquinas acceso a los servicios de directorio en toda la organización X.500 usaba un conjunto de servidores de directorio (DAS), y cada uno tenía una porción del total del servicio de directorio en una compañía. Se buscaba que X.500 fuese una norma abierta. Desafortunadamente, esto significaba que los datos tenían muy seguros en su tránsito por la red (modelos posteriores al protocolo X.500 soportaban funciones de seguridad adicionales). LDAP ha sufrido varias modificaciones. LDAPv2 fue una norma de Internet en el RFC-18777.

Sin embargo debido a varias limitaciones con esta versión, no se consideró como una opción viable para la comunidad de Internet. Hoy en día, LDAPv2 se guía por la misma norma del RFC; no puede funcionar con las redes actuales .LDAPv3 es la norma opcional que se describe en los RFC 2222, 2251, 2252 y otros (Clark, 2001).

LDAPv3 utiliza un modelo de seguridad que se basa en el Nivel de seguridad y autenticación simple (SASL), descrito en el RFC-2222. Esto permite cifrado y comunicaciones seguras entre el servidor y el cliente. SASL es un sistema, mientras que el Nivel de conexión segura (SSL) y Kerberos pueden utilizarse como servicios de seguridad. LDAP permite el uso de certificados, con la norma X.509, y se continúa trabajando en él para soportar a la última norma de certificado X.509v3.

LDAPv3 ha mejorado el desempeño de su predecesor, LDAPv2. En LDAPv2, los clientes que deseaban tener acceso al servicio de directorio X.500 primero debían pasar por el servidor LDAP y hacer una solicitud de enlace. Una vez autenticados, el servidor LDAP solicitaba la base de datos X.500 en beneficio del cliente. En LDAPv3, un cliente puede solicitar búsquedas al servidor LDAPv3 sin enlazarse primero con él. Esto representa una mejora, puesto que muchas de las solicitudes eran anónimas y primero debían ser permitidas. Si la base de datos X.500 debe establecer la seguridad, el LDAPv3 rechazará la solicitud del cliente, publicará un error de enlace y el cliente intentará de nuevo, pero esta vez enlazándose primero al servidor LDAP (Clark, 2001).

LDAP viene de la comunidad de Internet y tiene un amplio soporte por parte de los principales proveedores que emplean a X.500. Al igual que el World Wide Web, LDAP le proporciona al usuario una gran flexibilidad. Con LDAPv3 y su soporte para X.509v3, es posible que continúe su crecimiento como otros servicios que existen en Internet. Los navegadores web, los clientes de correo, las aplicaciones basadas en LDAP y las redes privadas virtuales aprovecharán las ventajas de LDAP.

5. Protocolo de Túnel Punto a Punto.

El Protocolo de Túnel Punto a Punto (Point-to-Point Tunneling Protocol, PPTP) encapsula los paquetes (frames) del Protocolo Punto a Punto (Point-to-Point Protocol, PPP) con datagramas IP para transmitirlos por una red IP como Internet o una Intranet privada.

El PPTP utiliza una conexión TCP conocida como la conexión de control de PPTP para crear, mantener y terminar el túnel, y una versión modificada de la Encapsulación de Enrutamiento Genérico (Generic Routing Encapsulation, GRE) para encapsular los paquetes (frames) PPP como datos para el túnel. Las cargas de los paquetes encapsulados pueden estar encriptadas o comprimidas o ambas cosas.

El PPTP supone la disponibilidad de una red IP entre un cliente PPTP (un cliente de túnel que utiliza el protocolo PPTP) y un servidor PPTP (un servidor de túnel que utiliza el protocolo PPTP). El cliente PPTP podría estar ya conectado a una red IP por la que puede tener acceso al servidor PPTP, o el cliente PPTP podría tener que llamar telefónicamente a un servidor de acceso de red (Network Access Server, NAS) para establecer la conectividad IP como en el caso de los usuarios de accesos telefónicos para Internet.

La autentificación que ocurre durante la creación de una conexión VPN con PPTP utiliza los mismos mecanismos de autentificación que las conexiones PPP, tales como el Protocolo de Autentificación Extendible (Extensible Authentication Protocol, EAP), el Protocolo de Autentificación con Reto/Negociación de Microsoft (Microsoft Challenge-Handshake Authentication Protocol, MS-CHAP), el CHAP, el Protocolo de Autentificación de Claves Shiva (Shiva Password Authentication Protocol, SPAP) y el Protocolo de Autentificación de Claves (Password Authentication Protocol, PAP). El PPTP hereda la encriptación, la compresión o ambas de las cargas PPP del PPP.

Para Windows® NT 4.0, debe de utilizarse Seguridad de Nivel de Transporte EAP (EAP-Transport Level Security, EAP-TLS) o MS-CHAP para que las cargas PPP sean encriptadas utilizando la Encriptación Punto a Punto de Microsoft (Microsoft Point to Point Encryption, MPPE) (Goralski-Waclowski, 1999).

5.2 Encriptación con MPPE.

PPTP hereda la encriptación MPPE, la cual utiliza el cifrador de flujos (streams) RSA RC4. El MPPE está disponible solamente cuando se utiliza el protocolo de autentificación MS-CHAP (versión 1 o versión 2).

5.3 Generic Routing Encapsulation (GRE).

Es el protocolo de Encapsulación de Enrutamiento Genérico. Se emplea en combinación con otros protocolos de túnel para crear redes virtuales privadas

El GRE fue diseñado para proporcionar mecanismos de propósito general, ligeros y simples, para encapsular datos sobre redes IP. El GRE es un protocolo cliente de IP que usa el protocolo IP 47.

Este protocolo es normalmente usado con VPN de Microsoft entre servidores con acceso remoto (RRAS) configurados para el enrutamiento entre redes de área local.

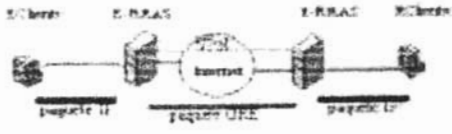


Fig. 5.6 Esquema General de GRE.

GRE se encarga del encapsulamiento de los datos para enviarlos por un túnel, pero él no crea los túneles, de eso de encarga el protocolo PPTP u otro protocolo utilizado para este fin.

El proceso de encapsulamiento tienen los siguientes pasos:

- El paquete IP con los datos se transmite desde el Ecliente al servidor E-RRAS.
- Se le añade la cabecera del PPP y se cifra todo junto obteniendo un 'fragmento PPP'.
- Los datos cifrados se colocan dentro de un paquete GRE con su correspondiente cabecera.
- Se envía el paquete GRE del servidor E-RRAS al servidor R-RRAS a través de Internet.
- Este envía se realiza por una conexión VPN creada anteriormente.
- El servidor R-RRAS elimina el encabezados GRE, descifra, elimina el encabezado PPP y transmite los datos (paquete IP) a el Rcliente.
- Los datos cifrados se colocan dentro de un paquete GRE con su correspondiente cabecera.

Esquema: Formato de un paquete GRE

Encabezado de vínculo de datos (DLL)	Encabezado IP	Encabezado GRE	Encabezado PPP	Carga de PPP cifrada	Finalizador de vínculo de datos

5.4 Servidor del Acceso de Red (NAS).

Un servidor del Acceso de Red (NAS) es un servidor del ordenador que permite a un abastecedor de servicio independiente (ISP) proveer de clientes conectados el acceso del Internet. Un servidor del acceso de red tiene interfases al abastecedor de servicio local de telecomunicación tal como la compañía del teléfono y a la espina dorsal de Internet (http://www.argo.es/~jcea/artic/vpn1.htm.2005)

El servidor autentica la petición de los usuarios conexión. Recibe entre llamada de marcado manual de cada usuario que el anfitrión (tal como su ordenador) que desea tener acceso al Internet, realiza los pasos necesarios para autenticar y para autorizar a cada usuario, generalmente verificando después permite un nombre del usuario y contraseña, y peticiones de comenzar a fluir una el anfitrión del usuario y los anfitriones (ordenadores) a otra parte en el Internet.

5.5 El Protocolo de Autenticación Ampliable (EAP).

El Protocolo de Autenticación Ampliable (EAP) es una extensión de PPP, que proporciona un mecanismo de soporte estándar para los esquemas de autenticación como las tarjetas token, Kerberos, Clave pública y clave/S, y está totalmente soportado tanto en Windows® NT Dial-Up Server como en Dial-Up Networking Client. EAP es un componente de tecnología crítica para las VPN seguras, protegiéndolas de la fuerza bruta de un ataque de diccionario o de que las contraseñas sean adivinadas (Microsoft, 1999).

EAP permite que los módulos de autenticación de terceros interactúen con la implementación de una VPN de Servicio de acceso remoto (RAS) Microsoft Windows® NT. La disponibilidad de EAP en Windows® NT es una respuesta a la creciente demanda para aumentar la autenticación RAS con dispositivos de seguridad de terceros.

EAP es una extensión propuesta por IETF para PPP que permite que los mecanismos

arbitrarios de autenticación se empleen para la validación de una conexión PPP.

EAP se diseñó para permitir la adición dinámica de módulos de conexión de autenticación tanto del lado del cliente como del servidor en una conexión. Esto permite que los proveedores suministren un nuevo esquema de autenticación en cualquier momento. EAP proporciona la máxima flexibilidad en variedad y singularidad de autenticación. EAP se pondrá en marcha en Microsoft Windows® 2000.

5.6 Seguridad de Nivel de Transacción (TLS).

Las tarjetas inteligentes y tarjetas token pueden ofrecer seguridad absoluta para las VPN.

Las tarjetas inteligentes son pequeños dispositivos casi del tamaño de una tarjeta de crédito, la cual contiene una CPU y una pequeña memoria. Se usan comúnmente para almacenar credenciales de autenticación (tales como certificados de clave pública) claves de encriptación, e información de una cuenta. Algunos también implementan algoritmos de encriptación en la tarjeta, para que las claves de encriptación nunca se borren de la tarjeta inteligente. En la actualidad, las tarjetas inteligentes no son comúnmente utilizadas para la seguridad de acceso remoto, ya que son pocos los paquetes de acceso remoto que las soportan. Windows® 2000 soporta el uso de tarjetas inteligentes en todas las variedades de autenticación, incluyendo RAS, L2TP, y PPTP (Microsoft, 1999).

Las tarjetas token de diferentes proveedores funcionan en diferentes formas, pero básicamente todas son generadoras de contraseñas de hardware. Por ejemplo, algunas tarjetas tienen una pequeña pantalla LCD y un teclado como el de una calculadora. El usuario introduce un PIN numérico y la tarjeta muestra un código de pase numérico, el cual a su vez se utiliza como contraseña.

Normalmente, las tarjetas token están diseñadas de manera tal que sólo produzcan un código de pase determinado.

Las tarjetas token funcionan muy bien para las aplicaciones de marcación (RAS) o autenticación del ordenador. Debido a que las aplicaciones de red de tarjetas token por lo regular se basan en cliente-servidor, las tarjetas inteligentes pueden ser vulnerables a ser descubiertas casualmente. (Y otras veces en esquemas de contraseña).

Estas tarjetas y certificados de usuario de clave pública recibirán soporte por medio del uso del Protocolo de autenticación ampliable Seguridad de nivel de transacción (EAP-TLS), el cual se ha sometido a IETF como una propuesta preliminar para un método sólido de autenticación basado en certificados de clave pública. Con EAP-TLS, un cliente presenta un certificado de usuario al servidor de marcación, al mismo tiempo que el servidor presenta un certificado de servidor al cliente. El primero proporciona autenticación sólida de usuario al servidor; el segundo asegura al usuario que ha alcanzado el servidor que esperaba. Ambos sistemas llegan a la cadena de autoridades confiables para verificar la validez del certificado que se ofrece.

El certificado del usuario podría almacenarse en la PC de cliente de marcación, o almacenarse en una tarjeta inteligente externa. En cualquiera de los casos, el certificado no puede accederse sin alguna forma de identificación de usuario (número PIN o intercambio de contraseña/nombre) entre el usuario y la PC del cliente. Este enfoque cumple con "algo de lo que el usuario sabe más algo que se tiene", los cuales son criterios recomendados por la mayoría de los expertos en la seguridad.

EAP-TLS es el método específico EAP que se implementa en Windows® 2000. Como MS-CHAP, EAP-TLS regresará una clave de encriptación que permitirá que MPPE encripte los datos subsecuentes.

5.7 Mejora de Autenticación con MS-CHAP versión 2.

El Protocolo de autenticación Handshake de Microsoft (MS-CHAP) es un mecanismo de autenticación que se utiliza para validar las credenciales del usuario contra los dominios Windows® NT, mientras que las claves de sesión resultantes se utilizan para encriptar los datos del usuario.

La Encriptación es el proceso de codificación de datos que sirve para prevenir el acceso no autorizado, especialmente durante la transmisión. La Encriptación se lleva acabo utilizando un algoritmo especial junto con uno confidencial (también conocido como clave) para transformar datos, como puede ser una contraseña, de manera tal que los datos no puedan ser entendidos por ninguna persona que no conozca la clave correcta. La contraseña hashed sólo puede ser decriptada por un ordenador que tenga la misma clave.

La versión 2 MS-CHAP incluye una función de una salida de la contraseña del usuario, un reto generado por el servidor y el cliente, además de datos adicionales en el mensaje Satisfactorio de la versión 2 MS-CHAP. El cliente de la versión 2 MS-CHAP se desconecta si no puede autentificar el servidor

Windows® 2000 incluye compatibilidad con la versión 2 del Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP v2, Microsoft Challenge Handshake Authentication Protocol), que proporciona seguridad de alto nivel para las conexiones de acceso remoto. MS-CHAP v2 resuelve algunos problemas de MS-CHAP versión 1.

MS-CHAP v2 es un proceso unidireccional con contraseña cifrada y autenticación mutua que funciona de la manera siguiente:

- El autenticador (el servidor de acceso remoto o el servidor IAS) envía un desafío al cliente de acceso remoto que consta de un identificador de sesión y una cadena de desafío arbitraria.

- El cliente de acceso remoto envía una respuesta que contiene:
- El nombre del usuario.
- Una cadena de desafío arbitraria del mismo nivel.
- Una codificación unidireccional de la cadena de desafío recibida, la cadena de desafío del mismo nivel, el identificador de sesión y la contraseña del usuario.

1. El autenticador comprueba la respuesta del cliente y devuelve una respuesta que contiene:

- Una indicación del éxito o fracaso del intento de conexión.

- Una respuesta autenticada basada en la cadena de desafío enviada, la cadena de desafío del mismo nivel, la respuesta codificada del cliente y la contraseña del usuario.

2. El cliente de acceso remoto comprueba la respuesta de autenticación y, si es correcta, utiliza la conexión. Si la respuesta de autenticación no es correcta, el cliente de acceso remoto termina la conexión.

5.8 El Challenge Handshake Authentication Protocol.

CHAP, MS-CHAP, PAP: El Challenge Handshake Authentication Protocol es un estándar IETF usado comúnmente para la autentificación de usuarios a través de conexiones PPP.

El Microsoft CHAP es una variación del CHAP usado para autentificar usuarios contra un Módulo de Acceso de Seguridad (SAM) Windows® 2000 Server, e incluye soporte para cambios de contraseñas. MS-CHAP ofrece una encriptación y un intercambio de claves transparente y automático (http: // www .microsoft .com/ windows2000/ es /server/ help /sag_ RASS _MSCHAPv2 .htm. 2005)

5.8.1 El Password Authentication Protocol.

El Password Authentication Protocol ofrece autentificación de contraseña de texto limpio. Este protocolo es completamente soportado, pero no se recomienda su uso por cuestiones de seguridad. Los sistemas funcionan así sin necesidad de alteraciones con los protocolos de autentificación más frecuentemente usados por ISPs.

5.9. Cifrado Punto a Punto de Microsoft (MPPE).

Cifrado punto a punto de Microsoft (MPPE, Microsoft Point-to-Point Encryption) cifra los datos de las conexiones PPP de acceso telefónico o de las conexiones VPN basadas en PPTP. Los esquemas de cifrado MPPE compatibles son: de alto nivel (clave de 128 bits) y estándar (clave de 40 bits). MPPE proporciona seguridad a los datos entre la conexión PPTP y el servidor de túnel. La versión de 40 bits se puede utilizar en todo el mundo; está integrada en todos los equipos que ejecutan Windows® 2000. El nivel de cifrado de 128 bits sólo está disponible en EE.UU. y Canadá. Puede habilitar la versión de 128 bits si instala una versión de software específica en el cliente y en el servidor (http://www.microsoft.com/windows2000/es/advanced/help/default.asp?url=/windows2000/es/advanced/help/data_encryption.htm.2005).

Conexiones de red y de acceso telefonico acepta cinco tipos de cifrado: Microsoft MPPE, que utiliza el cifrado RSA RC4 y una implementacion de protocolo de seguridad de protocolo Internet (IPSec) que utiliza el cifrado Estándar de cifrado de datos (DES).

MPPE e IPSec aceptan varios niveles de cifrado, como se muestra en la tabla siguiente.

Implementación de cifrado	Uso
MPPE estándar (40 bits, 56 bits)	Uso internacional
MPPE reforzado (128 bits)	Norteamérica
IPSec DES (56 bits)	Uso internacional
IPSec Triple DES (3DES)	Entornos de alta seguridad de Norteamérica

- Los controles del servidor son flexibles y se pueden configurar para denegar el uso del cifrado, requerir un método de cifrado específico o permitir que el equipo seleccione un método de cifrado. De forma predeterminada, la mayor parte de los servidores permiten el cifrado y permiten que los clientes seleccionen los métodos de cifrado. Esto funciona en la mayor parte de los equipos. El administrador del sistema establece los requisitos de cifrado. Para conocer las opciones disponibles, póngase en contacto con el administrador del sistema.
- Para habilitar el cifrado de datos basado en MPPE en conexiones de acceso telefónico o de red privada virtual (VPN), debe seleccionar los métodos de autenticación MS-CHAP, MS-CHAP v2 o EAP-TLS. Estos métodos de autenticación generan las claves utilizadas en el proceso de cifrado.

- Las redes privadas virtuales (VPN) utilizan el cifrado en función del tipo de servidor al que se conecten. Si la conexión VPN está configurada para conectar con un servidor PPTP, se utiliza el cifrado MPPE. Si la conexión VPN está configurada para conectar con un servidor L2TP, se utilizan los métodos de cifrado IPSec. Si la conexión VPN está configurada para un tipo de servidor Automático, que es la opción predeterminada, primero se intenta con L2TP y el cifrado IPSec asociado y, después, se intenta con PPTP y el cifrado MPPE asociado.

- MPPE requiere claves comunes en el cliente y en el servidor, como las generadas por la autenticación MS-CHAP o EAP.

Conclusiones.

Conclusiones:

La red privada virtual es una forma de compartir y transmitir información dentro de un círculo cerrado de usuarios , sitiados en diferentes zonas geográficas, utilizando un canal público como Internet y añadiéndole tecnología de encriptamiento, encapsulamiento y autenticación.

Las redes privadas virtuales se han constituido como un importante avance tecnológico, y como punto de crecimiento para que Internet cambie la manera en que las empresas hagan negocios.

La maduración de los estándares tecnológicos de VPN como son (PPTP, L2TP, IPsec), harán que la tasa de adopción por parte de las empresas aumente y al mismo tiempo establezca la VPN a la vanguardia del despliegue WAN.

Las VPN vienen a ser una solución, para las empresas que necesitan una fuerza de trabajo móvil, y no puedan costear los gastos de tener una red privada propia.

La VPN propuesta en el presente trabajo esta ubicada en el área de acceso remoto, que es el acceso a través de Internet que se crea entre oficinas centrales y usuarios móviles.
La VPN, de este trabajo se ubica en la arquitectura de VPN basada en acceso remoto, que es software que se ejecuta en los usuarios remotos, y crean un túnel, proveniente de Internet hacia una empresa.

En cuanto a la topología, se ubica en VPN/LAN a LAN, que es la que contempla la comunicación de una red interna con usuarios remotos.

Las plataformas de Sistemas Operativos que se utilizan tanto en los clientes, como en el servidor, son de la familia Windows® debito a que los Sistemas Operativos de Microsoft gozan de gran presencia en el mercado nacional, asiendo esto, que al implantar una solución VPN sean los costos mínimos, ya que desde el sistema Windows® 98 hasta Windows® XP, viene incluido el cliente PPTP para crear redes privadas virtuales.

El protocolo PPTP se eligió porque es un protocolo diseñado para proporcionar comunicaciones autenticadas, cifradas y al mismo tiempo cuenta con simplicidad, compatibilidad y gran capacidad de cruzar redes IP.

PPTP se vale de GRE para encapsular de PAP, CHAP, MS-CHAPv2, y MPPE para cifrar y autenticar. En Windows® 2000 Server se dan las ultimas mejoras de PPTP y los clientes deben contar mínimo con la versión 1.3 de acceso telefónico a redes, para ser compatibles con las medidas de seguridad que exigirá el servidor.

Microsoft sigue mejorando su tecnología de operación de red y comunicaciones, y aunque PPTP no es el mejor protocolo para establecer VPN, sigue siendo una alternativa para mejorar la seguridad y el acceso a redes, y posicionándose como una alternativa realmente baja en costo y al alcance principalmente de las PYMES.

Propuestas:

La red privada virtual basada el PPTP es una alternativa viable para las pequeñas y medianas empresas interesadas en expandir sus negocios , a través de trabajadores móviles.

Particularmente en el caso de México la AMECE (Asociación Mexicana estándares para el Comercio Electrónico) dio a conocer que el crecimiento del uso de Interne para diversas transacciones o transferencias de datos, a crecido en el orden del 400% en los últimos años, situando a México en el segundo lugar en América Latina, solo por debajo de Brasil.

Para poder llevar a cabo una solución VPN particularmente, la propuesta en este presente trabajo , seria conveniente tomar en cuanta los siguientes aspectos:

Tener un proveedor de servicios de Internet que tenga la mayor disponibilidad posible es decir que se pueda tener una conexión hacia el las 24 horas del día y dentro del territorio nacional.

Tener una conexión a Internet de banda ancha, recomendada para no comprometer la transferencia de datos. Y al mismo tiempo dejar atrás algunos obstáculos que se tienen con una conexión normal .

Contar con un servidor acorde con las necesidades de usuarios móviles que manejara, es decir un servidor lo suficiente mente rápido y con el Hardware necesario para hacer la conexión con Internet y con la red interna.

Contar con ordenadores móviles preferentemente con un procesador a 350 Mhz. Y 64 Mb en RAM.y un MODEM para poder conectarse a la red telefónica básica .

Las contraseñas de acceso a la red interna, preferentemente que sean puestas por el administrador de la red para asegurar el uso: de letras , números y signos.

Debido al elevado uso de Internet por las empresas para la expansión de sus negocios, es recomendable al utilizar a PPTP como protocolo para VPN, se consulta periódicamente las mejoras en materia de seguridad que lance Microsoft.

El presente trabajo solo toma en cuenta el análisis y funcionamiento del protocolo Punto a Punto (PPTP) y su uso en los sistemas operativos de Microsoft.

Anexos.

Procedimientos de Configuración de Windows 2000 Server.

Procedimiento A. Configuración TCP/IP en los adaptadores LAN y WAN.

1.- Se hará click en la opción "conexiones de red y acceso telefónico", con el botón secundario del ratón dar click en la "conexión de red" y enseguida en "propiedades", se vera la pantalla siguiente, seleccione la opción "protocolo de internet (TCP/IP)" y a continuación en configurar.

2.- Al ver la siguiente pantalla ingrese los valores de 192.168.0.1 en la dirección ip, en la mascara de subred 255.255.255.0 , y click en aceptar.

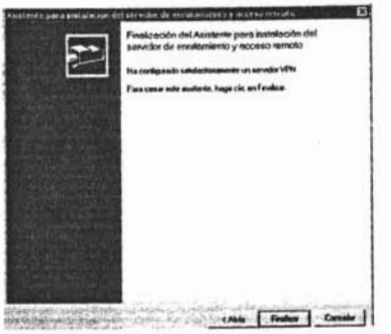
3.- Se hará click en la opción "conexiones de red y acceso telefónico", con el botón secundario del mause dar click en la "conexión a internet" y enseguida en "propiedades", se vera la pantalla siguiente, seleccione la opción "protocolo de internet (TCP/IP)" y a continuación en configurar.

4.- Introduzca el valor de 207.46.130.1 que es un ip estático y valido en internet y click aceptar.

5. Seleccione la opción "asignar direcciones ip automáticamente", mas adelante veremos como crear un conjunto de direcciones estáticas, y click en siguiente.

7.- Seleccionar la opción "No quiero configurar una sesión radius" y click en siguiente.

8. Dar click en finalizar y la configuración estará completada.



Procedimiento B. Habilitar el Servicio de Enrutamiento y Acceso Remoto.

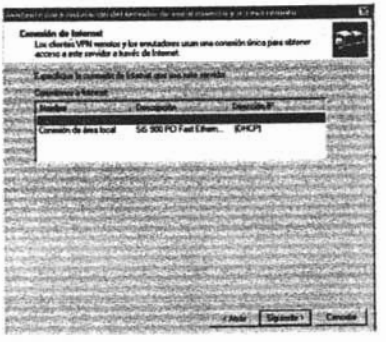
1. En el menú "Herramientas adminisdtrativas", abra Enrutamiento y acceso remoto", haga click con el botón secundario del ratón en el nombre del servidor y, después, haga click en "Configurar y habilitar el enrutamiento y el acceso remoto".

2. Se ejecutara el asistente "para la instalación del servidor", se podrá comenzar, con un click en siguiente.

3. Seleccione la opción "Servidor de red privada virtual", y click en siguiente.

4. Seleccione el protocolo "TCP/IP", marque la opción "si, todos los protocolos están en la lista", y click en siguiente.

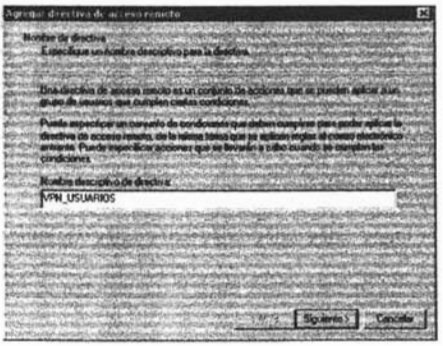
5. Seleccione el modem con el que el servidor se conecta a internet, y dar click en siguiente.



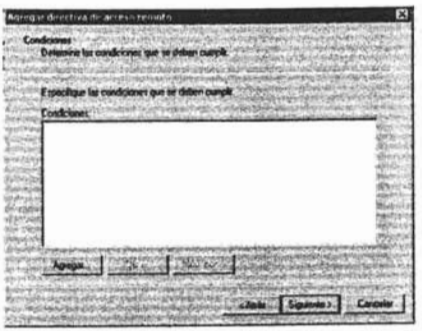
Procedimiento C: Directivas de acceso remoto.

1. En la opción directivas de acceso remoto, seleccione el grupo al cual se le aplicaran las directivas, en este caso el grupo es: GRUPO_VPN. Con el botón derecho del ratón sobre el grupo, desplegar el menú, seleccionar propiedades, y seleccionar la opción "agregar directiva de acceso remoto".

2. Se ejecutara el asistente para "agregar directiva de acceso remoto", en nombre de la directiva poner VPN_USUARIOS, y click en siguiente.

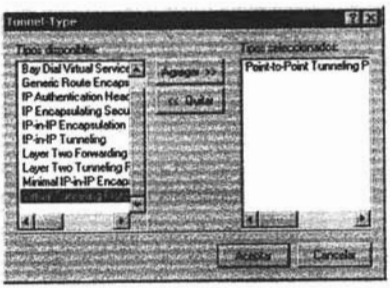


3. A continuación definiremos las condiciones que se deben cumplir, dar click en agregar, y nos mandara a los atributos.



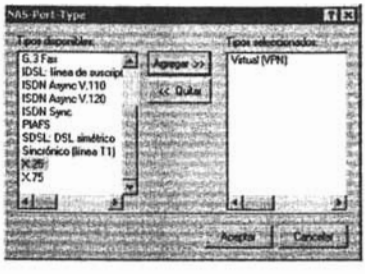
3.- En atributos seleccionar Tunnel-Type (Tipo de túnel), y click en agregar.

4. En tipo de túnel seleccionar "PPTP", click en agregar y aceptar.



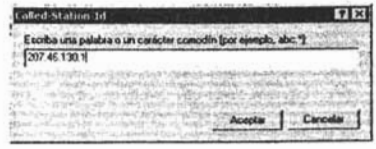
5. De nuevo en atributos seleccionar NAS-Port-Type (Tipo de puerto físico usado por el NAS), y click en agregar.

6. Seleccionar "Virtual VPN", click en agregar y aceptar.



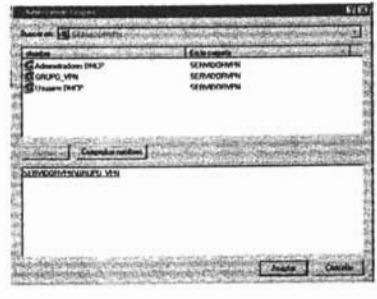
7. Seleccionar Called-Station-Id (Numero de teléfono marcado por el usuario), y click en agregar.

8.- Aquí se pide un carácter comodín y pondremos la dirección ip del servidor 207.46.130.1, y click en aceptar.



9. Seleccionar Windows-Groups (Grupos de windows), y click en agregar.

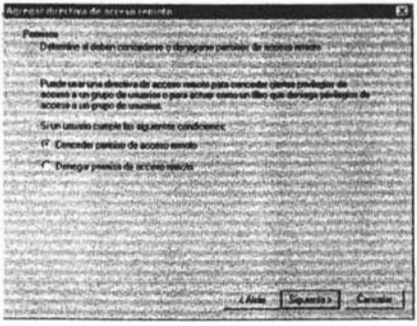
10. Se seleccionara el grupo: GRUPO_VPN, y click en aceptar.



11. Se muestra cuales son los grupos que serán incluidos en la directiva, en este caso GRUPO_VPN, que pertenece al SERVIDOR VPN.

12. Aquí se muestra cuales son las directivas ya agregadas, para la directiva VPN_USUARIOS, y click en aceptar.

13. Se seleccionara la opción "Conceder permiso de acceso remoto", y click en siguiente.

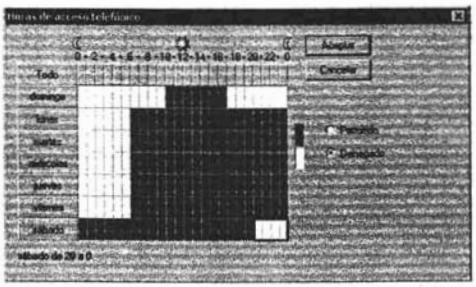


Procedimiento D: Autentificación y Cifrado.

1.- En la directiva de acceso remoto configuraremos al perfil de usuario, dando click en "modificar perfil".

2. En restricciones de marcado, se hará click en "modificar".

3. Se configura de la siguiente manera, la parte oscura son las horas y días de la semana donde se permite el acceso a los usuarios y, la parte clara son los horarios que no esta permitido el acceso, esto es en función de cómo se quiera configurar.



4. En la pestaña ip se marcara la opción "la configuración del servidor define la directiva".

5. En la pestaña autenticación, se marcaran las siguientes opciones:

- MS-CHAP v2
- MS-CHAP

6. En la pestaña cifrado, se marcaran las opciones: Básica y fuerte. La autenticación y cifrado estarán completas al dar click en aceptar.

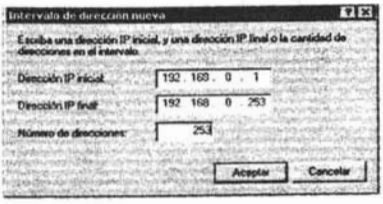
Procedimiento E: Crear un Grupo de Direcciones Ip Estáticas.

1. Se seleccionará "Programas", "Herramientas administrativas" y, a continuación, se hará click en "Enrutamiento y acceso remoto".

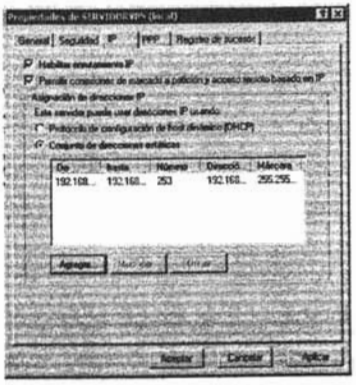
En el servidor de la consola, se hará click con el botón secundario del ratón en el servidor para el que desea crear un grupo de direcciones IP estáticas y, a continuación, se hará click en "Propiedades".

2. En la ficha "IP", se hará click en "Conjunto de direcciones estáticas" y, a continuación, se hará click en "Agregar".

3. En "Dirección IP inicial", se escribirá una dirección IP inicial 192.168.0.1 y, a continuación, se escribirá una dirección IP final 192.168.0.254 para el intervalo en "Dirección IP final" o el número de direcciones IP en el intervalo de "Número de direcciones" 253.



4. Se hará click en Aceptar y, a continuación, se vera la pantalla siguiente y las ip estáticas estarán creadas.



<u>Nota.-</u> Si el conjunto de direcciones IP estáticas se compone de intervalos de direcciones IP de una subred independiente, se tendrá que habilitar un protocolo de enrutamiento IP en el equipo servidor de acceso remoto o agregar rutas IP estáticas que están formadas por {Dirección IP, Máscara} de cada intervalo de las rutas de la intranet. Si no se agregan las rutas, los clientes de acceso remoto no podrán recibir el tráfico de los recursos de la intranet.

PROCEDIMIENTO F: Creación de una Ruta Estática.

1.- En rutas estáticas, que esta contenida en enrutamiento ip, con el botón derecho del ratón, se despliega el menú, y se selecciona "ruta estática nueva".

2. En interfaz se selecciona al modem con el que se tiene acceso a internet, en destino se pondrá: 0.0.0.0, lo mismo en mascara de red. En puerta de enlace, en métrica 1, y click en aceptar.

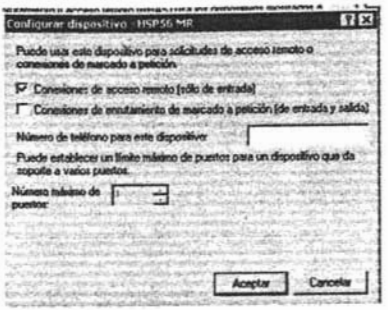
3. Se vera la pantalla siguiente, y estará lista la ruta estática.

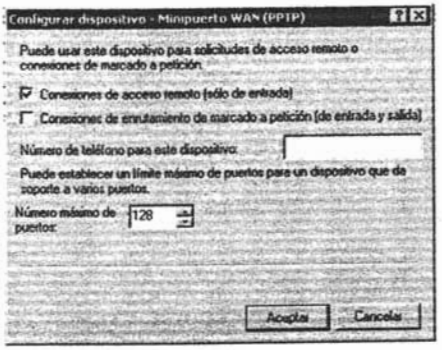
PROCEDIMIENTO G: Configuración de Puertos PPTP.

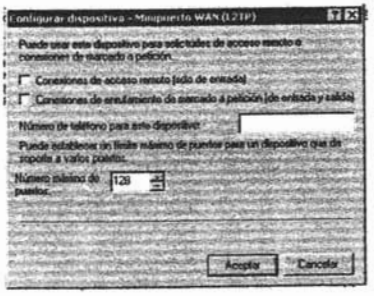
1. En Enrutamiento y acceso remoto, abra el cuadro de diálogo Propiedades de Puertos.

2. En el cuadro de diálogo Propiedades de Puertos, seleccione un dispositivo (para los puertos VPN, son Minipuerto WAN (PPTP) y Minipuerto WAN (L2TP) y haga click en Configurar.

3. En el cuadro de diálogo Configurar dispositivo, active la casilla de verificación Conexiones de acceso remoto (sólo de entrada) para habilitar las conexiones VPN entrantes.







4. Opcionalmente puede aumentar o reducir el número de puertos virtuales disponibles en el servidor.

Haga clic en Aceptar en los cuadros de dialogo Configurar dispositivos y propiedades de puertos.

PROCEDIMIENTO H: Agregar Filtros de Paquetes PPTP.

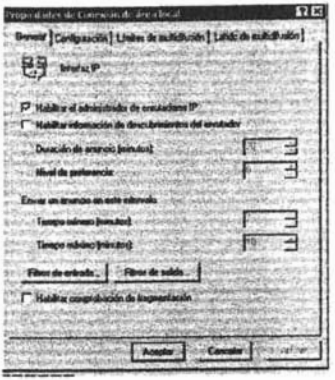
Se hará click en "Inicio", se seleccionará "Programas", "Herramientas administrativas" y, a continuación, se hará click en "Enrutamiento y acceso remoto".

En el árbol de la consola, se hará doble click en el servidor para el que se desea configurar el filtrado de paquetes PPTP.

Se hará doble click en "Enrutamiento IP".

Se hará click en "General".

En el panel de detalles, se hará click con el botón secundario del ratón en la interfaz que esté conectada a Internet y, a continuación, se hará click en "Propiedades".



En la ficha "General", se hará click en "Filtros de entrada".

En el cuadro de diálogo "Filtros de entrada", se hará click en "Agregar".

En el cuadro de diálogo "Agregar filtro IP", se activará la casilla de verificación "Red de destino". En "Dirección IP" se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en "Máscara de subred" se escribirá "255.255.255.255". En "Protocolo", se hará click en Otros. En "Número de protocolo" se escribirá 47 y, a continuación, se hará click en Aceptar.

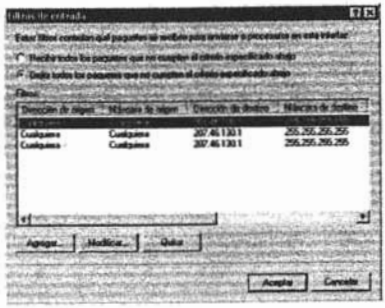
En el cuadro de diálogo "Filtros de entrada", se hará click en "Agregar".

En el cuadro de diálogo "Agregar filtro IP", se activará la casilla de verificación "Red de destino". En "Dirección IP" se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en "Máscara de subred" se escribirá "255.255.255.255". En "Protocolo", se hará click en "TCP". En "Puerto de destino" se escribirá 1723 y, a continuación, se hará click en Aceptar.

En el cuadro de diálogo "Filtros de entrada", se hará click en "Agregar".

En el cuadro de diálogo "Agregar filtro IP", se activará la casilla de verificación "Red de destino". En "Dirección IP" se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en "Máscara de subred" se escribirá "255.255.255.255". En "Protocolo", se hará click en TCP [establecido]. En "Puerto de origen" se escribirá 1723 y, a continuación, se hará click en Aceptar.

En el cuadro de diálogo "Filtros de entrada", se hará click en "Omitir todos los paquetes que no cumplen el criterio especificado abajo" y, después, se hará click en Aceptar.



En la ficha "General", se hará click en "Filtros de salida".

En el cuadro de diálogo "Filtros de salida", se hará click en "Agregar".

En el cuadro de diálogo "Agregar filtro IP" se activará la casilla de verificación "Red de origen". En "Dirección IP" se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en "Máscara de subred" se escribirá "255.255.255.255". En "Protocolo", se hará click en "Otros". En "Número de protocolo" se escribirá 47 y, a continuación, se hará click en Aceptar.

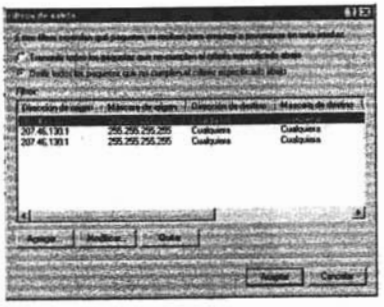
En el cuadro de diálogo "Filtros de salida", se hará click en "Agregar".

En el cuadro de diálogo "Agregar filtro IP" se activará la casilla de verificación "Red de origen". En "Dirección IP" se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en "Máscara de subred" se escribirá "255.255.255.255". En "Protocolo", se hará click en "TCP". En "Puerto de origen" se escribirá 1723 y, a continuación, se hará click en Aceptar.

En el cuadro de diálogo "Filtros de salida", se hará click en "Agregar".

En el cuadro de diálogo "Agregar filtro IP" se activará la casilla de verificación "Red de origen". En "Dirección IP" se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en "Máscara de subred" escribirá "255.255.255.255". En "Protocolo", se hará click en "TCP [establecido]". En "Puerto de destino" se escribirá 1723 y, a continuación, se hará click en Aceptar.

En el cuadro de diálogo "Filtros de salida", se hará click en "Omitir todos los paquetes que no cumplen el criterio especificado abajo" y, después, se hará click en Aceptar.



Se hará click en "Aceptar" para guardar los cambios efectuados en la interfaz.

PROCEDIMIENTO I: Configurar un Número de Teléfono en un Dispositivo.

Se hará click en "Inicio", seleccione "Programas", "Herramientas administrativas" y, a continuación, se hará click en "Enrutamiento y acceso remoto".

En el árbol de consola, se hará click en el servidor para el que desea configurar un número de teléfono.

En el panel de detalles, se hará click con el botón secundario del ratón en "Puertos" y, a continuación, se hará click en "Propiedades".

En el cuadro de diálogo "Propiedades de puertos" se hará click en el dispositivo que corresponde al equipo VPN o de acceso telefónico y, a continuación, se hará click en "Configurar".

En "Número de teléfono para este dispositivo" se escribirá el número de teléfono para el puerto. Para los puertos VPN, se escribirá la dirección IP de la interfaz de Internet del servidor VPN.

Se hará click en Aceptar.

Procedimiento J: Configuración del Dominio.

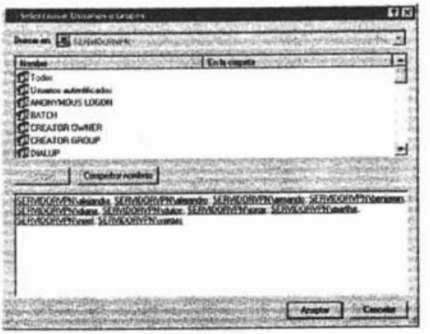
1. En la opción administración de equipos.

2. Se seleccionara la opción usuarios locales y grupos.

3. Los usuarios se crean ingresando el nombre del usuario, nombre completo, descripción, contraseña y confirmando contraseña.

3. Una vez ingresado los usuarios se creara, el grupo nuevo, ingresando el nombre de grupo y su descripción.

4. En seguida se seleccionaran los usuarios para este grupo, escogiéndolos de una lista de usuarios que proporcionara el servidor, y click en aceptar.



4. Aquí se puede ver cuales son los usuarios y el grupo al que pertenecen.

VPN de Windows 2000: Pruebas de Rendimiento Empresarial.

A petición de Microsoft Corporation, NSTL comprobó el rendimiento de la característica Red privada virtual (VPN) incluida en el sistema operativo Windows 2000 Server. Las redes privadas virtuales (o VPN) utilizan Internet como medio para permitir a los usuarios autorizados el acceso a datos ubicados en entornos de redes corporativas. Las VPN utilizan diversos tipos de mecanismos de cifrado y seguridad para asegurar que no se pueden interceptar los datos. La tecnología VPN no sólo permite que los recursos de red estén disponibles para los usuarios externos, sino que también ofrece un medio seguro de redes conectadas en distintas ubicaciones geográficas sin el elevado costo que suponen las líneas telefónicas dedicadas.

Metodologías de las Pruebas.

NSTL realizó las pruebas de VPN en diciembre de 1999. Ocho proveedores configuraron sus dispositivos VPN (que eran una combinación de hardware y software) en el laboratorio de NSTL. La prueba utilizada para evaluar VPN de Windows 2000 . Todos los dispositivos VPN se probaron en un segmento de LAN Ethernet estándar a 100 Mbits/segundo utilizando seguridad IP (IPSec). Este informe se centra en el rendimiento del reenvío de paquetes a través de un túnel desde una puerta de enlace a otra, una prueba de tráfico máximo del túnel desde el cliente a una puerta de enlace y una prueba de tráfico sostenido del túnel. NSTL probó el rendimiento de VPN en Windows 2000 mediante el Protocolo de túnel punto a punto (PPTP) y, después, con el Protocolo de túnel de nivel 2 (L2TP) cifrado por IPSec.

Para la prueba de reenvío de paquetes, NSTL instaló Windows 2000 Advanced Server en dos sistemas servidores avanzados. Los servidores tenían cuatro procesadores Intel Xeon a 550 MHz y más de 1 GB de memoria RAM. Cada servidor tenía instalados 4 adaptadores de servidor Intel Pro/100 S con compatibilidad para descarga de Seguridad IP (IPSec). El rendimiento de la red es máximo cuando se utiliza la NIC de descarga al reducir la carga en el procesador de los sistemas host descargando el cifrado desde el equipo al adaptador de red. Se estableció un túnel desde una puerta de enlace a otra. NSTL utilizó un generador de tráfico de Shomiti Systems, Inc para ofrecer tráfico unidireccional del Protocolo de datagramas de usuario (UDP) en el segmento de LAN de 100 Mbits con una utilización de la red del 100%.

Entonces, NSTL redujo el porcentaje de uso de la red hasta que no se perdió ningún paquete. Se midió el rendimiento máximo para PPTP y después para L2TP sobre IPSec (L2TP/IPSec). Para poder hacer comparaciones, NSTL representó gráficamente los tres mejores resultados obtenidos en la prueba anterior de VPN y el dispositivo que presentó el menor rendimiento.

La segunda prueba, la prueba de túneles máximos, evaluó el número máximo de túneles que podían establecerse y el rendimiento de cada túnel. El banco de pruebas consistió en dos servidores con cuatro procesadores Xeon donde se había instalado Windows 2000 Advanced Server. El primer servidor (de aplicaciones para el usuario) tenía instalados seis adaptadores de servidor Intel Pro/100 S y el segundo (de servicios de fondo) tenía dos adaptadores Intel Pro/100 S. NSTL configuró 25 máquinas cliente con Windows 2000 Server. Cada máquina cliente tenía un procesador Intel Pentium III a 450 MHz y 128 MB de memoria RAM. Cada cliente tenía instalado un adaptador Ethernet 10/100 3C905-TX de 3Com. Se separaron los clientes en cuatro grupos y cada grupo se colocó en su propio concentrador de 100 Mbits.

Cada concentrador se conectó a una NIC del servidor de aplicaciones para el usuario. Los dos adaptadores restantes del servidor de aplicaciones para el usuario se emplearon para la conexión al servidor de servicios de fondo. Se configuraron los clientes para crear 200 túneles cada uno, hasta un total de 5.000 túneles. Una vez creados los 5.000 túneles, NSTL utilizó una

prueba personalizada suministrada por Microsoft para generar y medir el tráfico UDP en la red.

La tercera prueba, la prueba de tráfico sostenido de túnel, evaluó el número de túneles que podían mantenerse con el tráfico UDP existente, con una tasa fija de datos de 33,6 Kbits/segundo. 33,6 Kbits/segundo era una tasa de conexión totalmente saturada para un usuario VPN con acceso telefónico a 56 KB. El banco de pruebas fue el mismo que en la prueba anterior. NSTL utilizó la herramienta de prueba personalizada suministrada por Microsoft para generar y medir el tráfico UDP en la red.

Resultados de las Pruebas de NSTL.

Reenvío de Paquetes.

En la figura 1 se compara VPN de Windows 2000 con PPTP y L2TP/IPSec con respecto a los otros dispositivos VPN. Empezando por el mayor tamaño de trama de 1406 bytes, el proveedor 1 presentaba el rendimiento máximo de 95 Mbits/segundo o un 95% de utilización de la red. El proveedor 2 conseguía rendimientos de 80 Mbits/segundo o el 80% de utilización de la red. El proveedor 3 obtenía un rendimiento de 40 Mbits/segundo o el 40% de utilización de la red. El proveedor 8 obtenía un rendimiento de 10 Mbits/segundo o el 10% de utilización de la red. No se probó Windows 2000 en el tamaño de trama de 1406 bytes. En el tamaño de trama de 1280 bytes, Windows 2000 consiguió unos rendimientos de 70 Mbits/segundo o el 70% de utilización de la red con L2TP/IPSec. Para PPTP, Windows 2000 obtenía un rendimiento de 53 Mbits/segundo o el 53% de utilización de la red. Los proveedores de la prueba anterior no se evaluaron para el tamaño de trama de 1280 bytes. En el tamaño de trama de 256 bytes, el proveedor 1 presentaba el rendimiento máximo de 75 Mbits/segundo o un 75% de utilización de la red. Windows 2000 era el siguiente, con 54 Mbits/segundo o el 54% de utilización de la red con L2TP/IPSec. El proveedor 2 obtenía un rendimiento de 25 Mbits/segundo o el 25% de utilización de la red. El proveedor 3 era el siguiente, con 15 Mbits/segundo o el 15% de utilización de la red. Después estaba Windows 2000 con PPTP, con 14 Mbits/segundo o el 14% de utilización de la red. El proveedor 8 era el último, con un rendimiento de 2 Mbits/segundo o el 2% de utilización de la red. En el tamaño de trama de 64 bytes, el proveedor 1 consiguió un rendimiento de 25 Mbits/segundo o el 25% de utilización de la red. El proveedor 2 era el siguiente, con 10 Mbits/segundo o el 10% de utilización de la red. Tanto Windows 2000 (con L2TP/IPSec) como el proveedor 3 presentaban unos rendimientos de 5 Mbits/segundo o el 5% de utilización de la red. Después estaba Windows 2000 con PPTP, con 4 Mbits/segundo o el 4% de utilización de la red. El proveedor 8 obtenía un rendimiento de 1 Mbits/segundo o el 1% de utilización de la red.

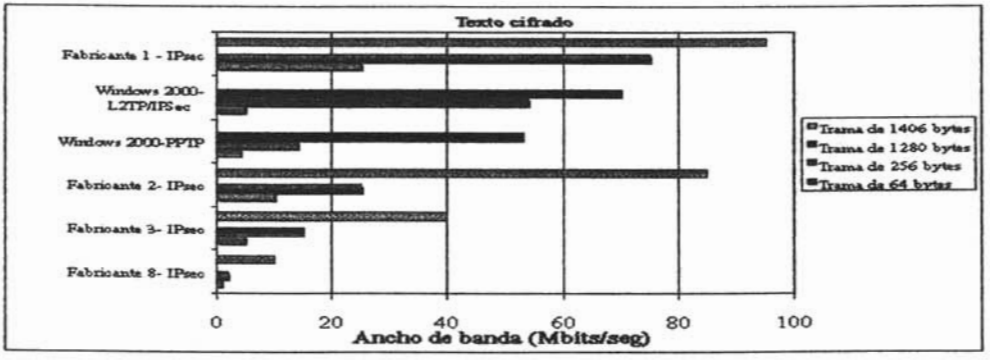


Figura 1 Reenvío de Paquetes.

Prueba de Túneles Máximos.

La figura 2 muestra un gráfico que representa la prueba de túneles máximos. VPN de Windows 2000 fue capaz de mantener 5.000 túneles con velocidades de 13,8 Kbits/segundo para L2TP/IPSec y 16,3 Kbits/segundo para PPTP. Para un usuario típico conectado a través de un enlace VPN a 56 KB, el rendimiento promedio estaba realmente entre 10 y 15 Kbps. Esto se debe al uso de la red por ráfagas propio de los usuarios remotos. Los rendimientos agregados de cada uno fueron de 79,7 Mbits/segundo en el caso de PPTP y 67,2 Mbits/segundo para L2TP/IPSec. NSTL no probó los otros dispositivos VPN de la prueba anterior.

Figura 2 Prueba de Túneles Máximos.

Prueba de Tráfico Sostenido de Túnel.

En la figura 3 se muestran los resultados obtenidos en la prueba de tráfico sostenido de túnel. NSTL fue capaz de crear 2.600 túneles cuando utilizaba PPTP. Cada túnel mostraba rendimientos de 33,6 Kbits/segundo. Para el usuario de VPN de acceso telefónico a 56 Kb, 33,6 Kbits/segundo representa una conexión de red totalmente saturada. En el caso de L2TP/IPSec se crearon 2000 túneles con un rendimiento de 33 Kbits/segundo. El agregado de L2TP/IPSec es 64,2 Mbits/segundo.

Figura 3 Tráfico Sostenido de Túnel.

Nota Este gráfico representa los resultados de la prueba de tráfico sostenido de túnel. Con un rendimiento fijo de 33,6 Kbits/segundo con PPTP se establecieron 2.600 túneles. Con un rendimiento de 32,9 Kbits/segundo con L2TP/IPSec se establecieron 2.000 túneles.

Conclusiones.

Los resultados de este informe ilustran que, en cuanto al reenvío de paquetes, la característica VPN de Windows 2000 es comparable a los dispositivos VPN basados en hardware líderes de la industria. Las otras pruebas realizadas por NSTL confirman que Windows 2000 puede ofrecer un rendimiento más que adecuado como dispositivo VPN general.

La característica VPN incluida en el sistema operativo Windows 2000 ofrece flexibilidad del servidor sin poner en peligro el rendimiento y la escalabilidad propios de los dispositivos hardware.

Acerca de NSTL

NSTL Inc es la organización de pruebas de hardware y software independiente líder del mundo, y se dedica a ofrecer servicios y herramientas de prueba de alta calidad a la comunidad informática. NSTL tiene amplia experiencia en el desarrollo y la realización de pruebas objetivas con el fin de evaluar productos nuevos y ya existentes para medir su compatibilidad, rendimiento, funcionalidad y facilidad de uso. Los servicios de pruebas de NSTL también se utilizan para el diseño de capacidades, análisis de impacto y ayuda a las adquisiciones. La experiencia y minuciosidad de NSTL ofrecen a los proveedores, agencias gubernamentales y corporaciones un medio rentable y de alta calidad para evaluar, diferenciar y evaluar productos informáticos.

Este informe se ha preparado bajo contrato para Motorola Internet and Networking Group y contiene los aspectos más importantes de las pruebas realizadas por NSTL a petición de Motorola Internet and Networking Group, de acuerdo con los parámetros proporcionados en el informe completo.

Comparativa entre windows 2000 y 2003 Server.

Windows 2000 es un sistema operativo con varios propósitos, con un soporte integrado para cliente/servidor y redes parejas. Se ha diseñado la familia de productos Windows 2000 para aumentar la fiabilidad, proporcionar mayores niveles de disponibilidad del sistema y conseguir dimensionabilidad de una pequeña red a una gran red entre empresas. Windows 2000 incorpora tecnologías que reducen el costo total de licencia permitiendo a las organizaciones aumentar el valor de sus inversiones existentes mientras disminuyen los costes totales de informática. Además, Windows 2000 incorpora un amplio soporte de Internet y aplicaciones, y ha sido construido a partir del éxito conseguido con Windows NT como un sistema operativo servidor para aplicaciones a Internet.

Windows Server 2003 es un sistema operativo de propósitos múltiples capaz de manejar una gran gama de funciones de servidor, en base a sus necesidades, tanto de manera centralizada como distribuida. Algunas de estas funciones del servidor son:

- Servidor de archivos e impresión.
- Servidor Web y aplicaciones Web.
- Servidor de correo.
- Terminal Server.
- Servidor de acceso remoto/red privada virtual (VPN).
- Servicio de directorio, Sistema de dominio (DNS), y servidor DHCP.
- Servidor de transmisión de multimedia en tiempo real (Streaming).
- Servidor de infraestructura para aplicaciones de negocios en línea (tales como

Planificación de recursos de una empresa y software de administración de relaciones con el cliente.

Windows Server 2003 cuenta con cuatro beneficios principales:

Beneficio	Descripción
Seguro	Windows Server 2003 es el sistema operativo de servidor más rápido y más seguro que ha existido. Windows Server 2003 ofrece fiabilidad al: Proporcionar una infraestructura integrada que ayuda a asegurar que su información de negocios estará segura. Proporcionar fiabilidad, disponibilidad, y escalabilidad para que usted pueda ofrecer la infraestructura de red que los usuarios solicitan.
Productivo	Windows Server 2003 ofrece herramientas que le permiten implementar, administrar y usar su infraestructura de red para obtener una productividad máxima. Windows Server 2003 realiza esto al: Proporcionar herramientas flexibles que ayuden a ajustar su diseño e implementación a sus necesidades organizativas y de red. Ayudarle a administrar su red proactivamente al reforzar las políticas, tareas automatizadas y simplificación de actualizaciones. Ayudar a mantener bajos los gastos generales al permitirles a los usuarios trabajar más por su cuenta.
Conectado	Windows Server 2003 puede ayudarle a crear una infraestructura de soluciones de negocio para mejorar la conectividad con empleados, socios, sistemas y clientes. Windows Server 2003 realiza esto al: Proporcionar un servidor Web integrado y un servidor de transmisión de multimedia en tiempo real para ayudarle a crear más rápido, fácil y seguro una Intranet dinámica y sitios de Internet. Proporcionar un servidor de aplicaciones integrado que le ayude a desarrollar, implementar y administrar servicios Web en XML más fácilmente. Brindar las herramientas que le permitan conectar servicios Web a aplicaciones internas, proveedores y socios.
Mejor economía	Windows Server 2003, cuando está combinado con productos Microsoft como hardware, software y servicios de los socios de negocios del canal brindan la posibilidad de ayudarle a obtener el rendimiento más alto de sus inversiones de infraestructura. Windows Server 2003 lleva a cabo esto al: Proporcionar una guía preceptiva y de fácil uso para soluciones que permitan poner rápidamente la tecnología a trabajar. Ayudarle a consolidar servidores aprovechando lo último en metodologías, software y hardware para optimizar la implementación de su servidor. Bajar el coste total de propiedad (TCO) para recuperar rápido la inversión.

Anexo II.- Pruebas de Rendimiento para Windows 2000 Server Realizado por NSTL

Microsoft Windows Server 2003: El doble de rendimiento

	Windows Server 2003 Web Edition	Windows Server 2003 Standard Edition	Windows Server 2003 Enterprise Edition	Windows Server 2003 Datacenter Edition
Servicios de Directorio Activo	Sí	Sí	Sí, incluido metadirectorio	Sí, incluido metadirectorio
Servicios de Ficheros	Limitado **	Sí	Sí	Sí
Servicio de Impresión	No	Sí	Sí	Sí
Clustering	No	No	8 Nodos	8 Nodos
Servicios de Balanceo de Carga	Sí	Sí	Sí	Sí
Servicios IIS	Sí - Servidor web dedicado a este propósito	Sí	Sí	Sí
Servicios de Fax	No	Sí	Sí	Sí
Cortafuegos básico	No	Sí	Sí	No
Servicios de Terminal	Administración Remota	Servidor, Administración Remota	Servidor, Administración Remota Session Directory	Servidor, Administración Remota Session Directory
Límite VPN	1	1000 conexiones concurrentes	Ilimitada	Ilimitada
Windows System Resource Manager	No disponible	No disponible	Si	Si

** Limitado a 10 conexiones SMB para publicación web exclusivamente.

Comparativa Con Versiones Anteriores

	Windows NT Server 4.0	Windows 2000 Server	Windows Server 2003
Directorio Activo	No disponible	Incluido	Mejorado con renombrado de directorios, modo de aplicación de Directorio Activo y replicación más eficiente
Políticas de grupo	No disponible	Incluido	Mejorada con decenas de nuevas características
Consola de gestión de Políticas de grupo	No disponible	No disponible	Proporciona gestión de estaciones de trabajo basada en directorios, permitiendo cambios sobre múltiples usuarios / máquinas mediante una sola orden administrativa
Internet information Services 6.0	No disponible	No disponible	Mejoras significativas en la arquitectura realizadas para superar los requisitos de fiabilidad de los clientes
Recuperación Automática del Sistema (ASR)	No disponible	No disponible	ASR permite la restauración en un solo paso del sistema operativo, el estado del sistema y la configuración del hardware
Servicio Volume Shadow Copy	No disponible	No disponible	Permite a los usuarios recuperar versiones previas de archivos almacenados en unidades de red sin intervención administrativa
.NET Framework integrada	No disponible	Está disponible la descarga de algunos componentes *	Plataforma de aplicaciones completamente integrada
Servicios UDDI Empresariales	No disponible	No disponible	Ayuda a las empresas a organizar y catalogar los servicios Web
Re-autentificación wireless más rápida	No disponible	No disponible	Asegura una experiencia de usuario sin interrupciones
Gestor de Recursos del Sistema de Windows	No disponible	No disponible	Empleado para establecer las limitaciones de recursos asignadas a aplicaciones servidor
Gestiona tu servidor/ configura tu servidor	No disponible	Limitado a la configuración del servidor	Muestra tareas administrativas comunes, listas de comprobación y ayuda relevante para realizar estas tareas

Glosario.

ASCII: (código estándar estadounidense para el intercambio de información) Alfabeto de datos utilizado en los PC de IBM para determinar la posición de la cadena de 7 bits de ceros y unos que representa cada carácter (alfabético, numérico o especial).

AppleTalk: Sistema de red Apple que transfiere datos a velocidades de 230 kilobytes por segundo sobre cable de par trenzado apantallado. Sustituido por el termino LocalTalk.

ADSL: Línea de suscripción asimétrica digital. Tecnología de compresión que permite a los hilos telefónicos convencionales transportar hasta 6 Mbps.

Asíncrono: Transmisión de información por unidades separadas que no llevan una cadencia fija en el tiempo y se separan por tanto mediante códigos separadores de control.

ATM (Asynchronous Transfer Mode) Nuevo protocolo de comunicación de alta velocidad (según la versión de decenas a más de 100 Mbps) basado en paquetes de tamaño fijo (5 bytes de cabecera y 48 bytes de datos).

Arquitectura: La topología y el diseño de una red.

Autenticación: Proceso de identificar positivamente a la entidad que solicita el acceso. La autenticación por lo general se realiza por medio de una función criptográfica.

Algoritmo: Conjunto de pasos matemáticos o sistemáticos usados como formula para realizar funciones repetitivas o problemáticas, como un algoritmo de encriptación que se utiliza para convertir texto simple en texto cifrado.

Banda base: Red que trasmite las señales como una pulsación de corriente directa en vez de variaciones en una señal radiofrecuencia.

Banda ancha: Canal o medio de transmisión capaz de trasmitir mas frecuencias que un canal de voz estándar de 3 Khz.

Bus: Consiste de una ruta común de transmisión y cuenta con una serie de nodos incorporados. A veces se le denomina topología de red lineal.

Byte: Grupo de 8 bits

Bit: Unidad mas pequeña de información. En trasmisiones digitales , se refiere al cero y al uno.

Bugs: error

Crackers: (intruso) Un "cracker" es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los "intrusos", y suelen disponer de muchos medios para introducirse en un sistema. Ver también: "hacker", "Computer Emergency Response Team", "Trojan Horse", "virus", "worm".

CERT (Computer Emergency Response Team) Organismo creado por el gobierno federal estadounidense para la seguridad de sistemas y redes informáticos.

CPU (Central Process Unit) El cerebro de un ordenador. Estrictamente, la unidad central de proceso de un computador.

Cortafuegos: Una maquina que conecta el perímetro de la red confiable de una compañía a una red no confiable. Proporciona proteccion contra ataques al proporcionar filtración en puertos, traducción de direcciones y tecnologías para inspección, y puede fungir como Proxy frente a las solicitudes internas.

Criptografía: ciencia de cifrado y descifrado.

Cifrado: Proceso de tomar un texto legible y convertirlo en un formato ilegible por medio de una función criptográfica.

CHAP/PAP: (Protocolo de autentificación y acuerdo mutuo / protocolo de autentificación de contraseña) Protocolo estándar de autentificación para conexiones PPP.

Datagrama: La unidad básica de comunicación del protocolo IP y por tanto de Internet.

DCE :(Data Communications Equipment) Nombre genérico para aparatos como el módem o la interfaz entre una máquina y un medio de transmisión.

DES : (Data Encryption Standard) Algoritmo de encriptación estandarizado por la administración estadounidense.

DOS : (Disk Operating System) Sistema Operativo hegemónico en los ordenadores personales en la década de los ochenta y primera mitad de los noventa, inicialmente realizado por Microsoft y que hoy tiene distintas versiones según fabricantes.

DCE: (equipos de comunicaciones de datos) Se refiere a cualquier componente de red X.25 que implementa el estándar CCITT X.25.

DTE: (Equipo terminal de datos) Designa aquellos dispositivos de usuario final que tienen acceso a una red X.25 utilizando el estándar CCITT X.25, LAP/LAB y X.25 PAP.

DNS: Servidor del servicio de nombres de dominio que asocia un nombre humano amigable (aunque con una estructura definida) a una dirección IP. Por todo internet y dentro de las intranets corporativas, las jerarquías de los servidores DNS consultan bases de datos internas y aportan referencias en respuesta a peticiones de ordenadores cliente.

DMZ: Área LAN/WAN de una empresa que opera fuera de sus defensas o perímetro de seguridad.

Datagrama: Paquete de información generado por la ordenador que contiene lo esencial de las direcciones fuente y destino de las ordenadores en comunicación. Protocolos como TCP/IP integran a menudo datagramas con protocolos de niveles más altos que garantizan su trasmisión integral.

Dominio: Secuencia de nombres separados por puntos que sirven como mnemotécnico a las direcciones IP. En las direcciones de correo se refiere sólo a la parte que está a la derecha de la arroba (@).

Ethernet: Cable de red y esquema de protocolo de acceso desarrollado en su origen por Xerox . Es la topología LAN preponderante en estos momentos.

Encapsulacion: Proceso de colocar un datagrama dentro de un paquete de datos de otro paquete de la red; se puede utilizar con los mismos protocolos o con protocolos distintos.

Extranet: Servidor de internet empleado por los clientes externos, los proveedores, etc.

Estación de Trabajo: Término que engloba a cualquier computador de gama media, es decir, más potente que un computador personal pero sin llegar a ser un gran computador (*mainframe*). Generalmente suelen correr un Sistema Operativo multiproceso y multitarea como UNIX®.

Encaminador: Mecanismo Hardware o Software para direccionar mensajes entre nodos y subredes que, atendiendo a su estado, pretende hacerlo de la forma más eficiente posible. En inglés, router.

FTAM: (Acceso y gestión de transferencia de archivos) Protocolo OSI que da acceso a archivos de otros sistemas.
Frame Relay:

FTP :(Protocolo de transferencia de archivos) Protocolo que describe como una ordenador puede servir de anfitrión para otras ordenadores permitiendo así las transacciones de archivos.

FEAL: Criptosistema desarrollado en Japón, con una cifra de bloque de 64 bits y una clave de 64 bits.

Frame Relay : Servicio de transmisión sobre líneas de alta velocidad. En España se asocia a la red Ibernet..

Gateway: Hoy se utiliza el término "router" (direccionador) en lugar de la definición original de "gateway". Actualmente una pasarela es un programa o dispositivo de comunicaciones que transfiere datos entre redes que tienen funciones similares pero operativas diferentes. Ver también: "mail gateway", "router."

Gopher: (Gopher) Un servicio de distribución de información que ofrece colecciones jerarquizadas de información en Internet. Gopher utiliza un protocolo simple que permite a un cliente Gopher acceder a información desde cualquier servidor Gopher que esté accesible, proporcionándole un único "espacio Gopher" (Gopher space) de información. Están disponibles también versiones de dominio público para cliente y servidor. Ver también: "archie", "archive site", "Wide Area Information Servers

Hacker: (pirata) Una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores. Este término se suele utilizar indebidamente como peyorativo, cuando en este último sentido sería más correcto utilizar el término "cracker". Ver también: "cracker".

H.320 : Estándar del CCITT para la videoconferencia, que es el más utilizado en los equipos comerciales basados en PC y RDSI.

Handshake :Parte inicial del protocolo en el que dos máquinas se ponen de acuerdo sobre el formato, velocidad y secuencia que seguirán en el resto de la comunicación.

Hardware: Referente a la parte física material (fija e invariable) de un dispositivo electrónico.

Hipertexto: Es un texto que contiene referencias al mismo u otros textos, liberando de la restricción de una lectura lineal.

Host : (anfitrión) Máquina en Internet o en una red en general, usualmente accesible desde las demás. El número de hosts servía para medir el crecimiento de Internet, pero hoy la mayoría de usuarios lo hacen por conexiones eventuales (ad hoc) por teléfono por lo que no se contabilizan como hosts.

HTML : (HyperText Markup Language) Implementación concreta del SGML, que define un formato hipermedia utilizado en el WWW que permite incluir hiperenlaces a otros documentos en la Red. Es un tipo de SGML. Existen las versiones HTML 1.0, HTML 2.0, HTML+ y HTML 3.0, aparte de las extensiones propias de algunos navegadores.

HTTP : (HyperText Tranfer Protocol) Protocolo utilizado para conectar los recursos WWW entre los servidores y los clientes. Es el característico http:// que aparece en los URL del WWW.

IP:(Protocolo Internet) estándar que describe el software que sigue la pista de la dirección internet por varios nodos, encamina los mensajes de salida y reconoce los mensajes de entrada.

Intranet: Red IP que da servicio a las organizaciones y a sus socios comerciales. Incluye a menudo servidores Web, servidores de correo, y otros servicios que están en internet pero los canales de comunicaciones tienen acceso restringido.

ISO: (Organización internacional para la normalización) Organización internacional de estándares técnicos que desarrollo el modelo OSI de interconexión de sistemas abiertos.

ISP: Los proveedores de servicio internet establecen conexiones de gran ancho de banda a internet, las subdividen y venden conexiones mas lentas a individuos y organizaciones. Un ISP también ofrece habitualmente servicios de anfitrión de páginas web.

ISDN: (Red Digital de Servicios Integrados) Tecnología en plena evolución que está empezando a ser ofrecida por las compañías telefónicas más Importantes. **ISDN**: combina servicios de voz y digitales a través de la red en un solo medio, haciendo posible ofrecer a los clientes servicios digitales de datos así como conexiones de voz a través de un solo "cable". Los estándares de la ISDN los especifica la CCITT. Ver también: "CCITT". [Fuente: RFC1208]

IETF: El grupo para tareas de ingeniería internet es uno de los dos órganos de trabajo del consejo de actividades de internet. Trabaja para el fomento y desarrollo de estándares para internet.

Kbps : (kilobits por segundo) Unidad de medida de ancho de banda.

Kilobyte: (kb) Unidad de información equivalente a 1.024 bytes.

MIME : (Multipurpose Internet Mail Extensions) Extensiones al formato texto permitido en los documentos de correo que permite añadir ficheros de todo tipo, reconociendo el formato para poder lanzar las aplicaciones ligadas

NIC: (Network Information Center) Centro de una subred en Internet, donde se puede encontrar información sobre la misma o sobre toda Internet.

Netbeui: (interfaz extendida de usuario de netbios) Versión aumentada del protocolo netbios utilizados por sistemas operativos de red como LAN Manager, LAN Server y Windows para trabajo en grupo y windows NT. Formaliza la interfaz para programadores e integra mas funciones.

Netbios: (Sistema básico de entrada/salida en red) Nivel de software desarrollado en su origen por IBM y Sytec para enlazar un sistema operativo de red con hardware especifico. Puede también establecer las comunicaciones entre estaciones de trabajo en red en el nivel de transporte.

NAT: descubre

OS/2: Sistema Operativo de IBM para PC.

Proxy: Máquina o sistema intermedio que almacena los URI de las últimas peticiones de recursos y las proporciona de su memoria en sucesivas peticiones, minimizando el acceso a los recursos remotos y, por tanto, optimizando el rendimiento del conjunto.

Protocolo: Compendio de normas que permiten la comunicación. En el caso concreto de la informática, se aplica a una serie de especificaciones o estándares del formato de los mensajes que describe para todos los niveles cómo se debe realizar la comunicación de dos dispositivos físicos (computadores) o lógicos.

PC: (Personal Computer) Se refiere en general a cualquier ordenador personal, aunque desde el mundo Macintosh se suele aplicar sólo a aquellos basados en procesadores Intel

PPP: (Point-to-Point Protocol) Protocolo para acceso por módem a Internet. Muy similar al SLIP pero sólo uno de los dos se puede utilizar al mismo tiempo.
descubre

Puertos:
1. Uno de los canales físicos de E/S de un computador, que pueden ser serie (COMs) o paralelos.
2. Punto de entrada de una aplicación o llamada cuando se hacen telnets.

Ruteador: Véase Encaminador.

RDSI: (Red Digital de Servicios Integrados) Más que una red es un tipo de líneas que permite la transmisión de voz y datos de forma digital y con un ancho de banda mayor que las líneas telefónicas convencionales .

Socks: Librería de programación que permite interactuar a las aplicaciones con el protocolo TCP/IP. brom

SLIP : (Serial Line IP) Protocolo para acceso por módem a Internet. Muy similar al PPP pero sólo uno de los dos se puede utilizar al mismo tiempo. El SLIP, a diferencia del PPP, sólo puede funcionar sobre TCP/IP, no tiene compresión ni detección de errores. Además es más lento.

SSL : (Secure Source Layer) Protocolo de seguridad para el WWW propuesto por Netscape.

Teletrabajo : Trabajo que se realiza sin lugar fijo o desde casa utilizando las nuevas posibilidades telemáticas.

Token Ring : Tecnología de conexión de redes en anillo por pase de testigo.

Tunneling :
1. IP Tunneling o Tunnel IP es una técnica todavía por estandarizar por la IETF que permite realizar redes virtuales privadas dentro de Internet. 2. En el HTTP es una técnica para obligar a que los mensajes pasen por un nodo intermediario.

TCP : Véase TCP/IP.

TCP/IP : (Transmission Control Protocol / Internetworking Protocol) Conjunto de protocolos utilizado en Internet. Incluye los protocolos IP, TCP, UDP, ICP.

Telnet: Protocolo (o el programa que lo implementa) de emulación de terminal y que permite la sesión remota entre computadores.

UNIX® : Sistema Operativo muy popular y potente proveniente del ámbito académico y hoy usado por la mayoría de estaciones de trabajo y *mainframes*.

UDP : (User Datagram Protocol) Otro de los protocolos de la familia TCP/IP para la transmisión de información. En este se envían paquetes sueltos sin mantener una conexión continua.

URL : (Uniform Resource Locator) Un puntero a una dirección de cualquier recurso Internet, ya sea correo electrónico, FTP, Telnet, o, más comúnmente, una página Web.

Web: Nombre coloquial del WWW.

Win16: Referente al modo de memoria de 16 bits de Windows 3.0, 3.1 y 3.11 trabajo en grupo.

Win32: Referente al modo de memoria de 32 bits de Windows NT y 95.

Windows: Entorno gráfico sobre DOS (en sus versiones 3.x) y Sistema Operativo completo (en sus versiones 95 y NT) orientado a ventanas de Microsoft.

Winsock: (Windows Socket) Es una DLL para utilizar el protocolo TCP/IP bajo Windows.

Workstation: Véase Estación de Trabajo.

World-Wide Web: Véase WWW.

WWW : (World-Wide Web) Servicio que combina el multimedia y el hipertexto para "navegar" por Internet, obteniendo información dispersa por toda Internet. Utiliza el formato HTML y el protocolo HTTP. Se refiere usualmente como Web o también como W3.

X.25 :Norma de conexión de computadores, estándar internacional adoptado por la UIT que aunque se llegó a utilizar mucho, cada día está en más desuso.

X.400: Estándar adoptado por la UIT para el correo electrónico y también en desuso.

X.500: Base de datos distribuida que permite la consulta de datos (dirección postal o electrónica, teléfono o fax) sobre personas, y organizaciones en todo el mundo.

Bibliografía:

Mark N. (2000), **Designing the total area network**, España: Pearson Educación.

Pepelnjak, I.(2001), **Arquitectura MPLS y VPN**, España: Pearson Educación.

Fowler, D.(1999), **Virtual private networks**, EU: M. Kaufmann.

Mairs J. (2002), **VPNs : a beginner's guide**, EU: : McGraw-Hill/Osborne.

Briere, D. (1990), **Virtual networks : A buyer's guide**, EU: Artech house.

Robledo Sosa. C.(1999), **Redes de computadoras**, Mexico, D.F. : Instituto Politecnico Nacional.

Black, U. D. (1987), **Redes de computadoras : Protocolos, normas e interfaces**, España: Macrobit : Serie Ra-Ma.

Huidobro Moya, J. M. (1992), **Redes de comunicaciones**, España: Paraninfo.

Raya J. L , Raya C. (2000), **Redes Locales**, México:,Alfaomega, Serie RA-MA

Tenenbaum A. S. (1997), **Redes de Computadoras**, México: Pearson, 3° edición

Gs comunicaciones (1998), ***Telecomunicaciones:* Redes de Datos**, México: Mc. Graw Hill

Clark D. L. (2001), **Guía para el Administrador de Redes Privadas Virtuales**, México: Mc Graw Hill Interamericana editores S.A. de C.V.

Scambray J., McClure S., Kurtz G. (2001), **Hackers 2**, España: Osborne Mc Graw Hill

Mason A. G. (2002), **Redes Privadas Virtuales de cisco**, España: Cisco press

Scott C., Wolfe P. & Erwin M. (1999). **Virtual Private Networks**, Estados Unidos: O'Reilly

Brown S. (2001), **Implementación de Redes Privadas Virtuales RPV**, México: Mc Graw Hill interamericana editores S.A. de C.V.

Smith R. (1997) , **Internet Cryptography**, Estados Unidos: Addison-Wesley

Goralski W., Waciowski D. (1999), **Virtual Private Network** , Estados Unidos: Computer technology Research corp.

Raya J.L., Raya E. (2001), **Windows® 2000 Server**, España: Alfaomega serie Ra-Ma

Sosinnski B., Moskowits J. (2000), **Aprendiendo Windows® 2000 Server en 24 horas**, México: PrenticeHall

Virtual Private Network Consortium (2005) "VPN Comsortium" en linea: http://www.vpnc.org/

VPN: Virtual Private Networking (2005) "Articles&Resourses" en linea: http://compnetworking.about.com/cs/vpn/

Universidad de Valencia (2005) "configuración de acceso vpn con Windows® 98" en línea: http://www.uv.es/ciuv/cas/vpn/vpnw98.html

Universidad de Valencia (2005) "configuración de acceso vpn con Windows® 2000" en línea: http://www.uv.es/ciuv/cas/vpn/vpnw2000.html

Universidad de Valencia (2005) "configuración de acceso vpn con Windows® XP" en línea: http://www.uv.es/ciuv/cas/vpn/vpnwxp.html

Universidad de Valencia (2005) "configuración de encriptación"en línea: http://www.uv.es/ciuv/cas/vpn/vpnencr.html

Software Engineering Institute (2005) "CERT Cordination Center" en linea: http://www.cert.org

SecurityFocus (2005) "Security" en línea: http://www.securityfocus.com

Jabber (1999) "Redes Privadas Virtuales" en linea: http://www.argo.es/~jcea/artic/vpn1.htm

Microsoft (2005) en línea : http://support.microsoft.com/default.aspx?Scid=%2Fisapi%2Fgomscom%2Easp%3Ftarget%3D%2Fintlkb%2Fspain%2Fe10%2F7%2F19%2Easp&LN=ES-ES

Collado Rguez, Mª Montserrat, Conde Rey, Silvia; Dafonte Pérez, Eva, (2005) "Redes Privadas Virtuales" en línea:
www.latinet.net/live/spanish/products_pn_vpn.phtml

Wikipedia (2005) "Windows® NT" en linea: http://es.wikipedia.org/w/index.php?title=Microsoft_Windows®_NT&action=edit

Wikipedia (2005) "Windows® 2000 Server" en linea: http://es.wikipedia.org/w/index.php?title=Windows®_2000_server&action=edit

Wikipedia (2005) "Windows® ME" en linea: http://es.wikipedia.org/w/index.php?title=Windows®_ME&action=edit

Wikipedia (2005) "Windows® 98" en linea: http://es.wikipedia.org/wiki/Windows®_98

Wikipedia (2005) "Windows® 98SE" en linea: http://es.wikipedia.org/wiki/Windows®_98_SE

Wikipedia (2005) "Windows® XP" en linea: http://es.wikipedia.org/wiki/Windows®_XP

Lycos (2005) "Windows®" en línea: http://usuarios. lycos.es/ betzweb/ hobbies.html

Microsoft Tech Net (2005) " Seguridad en redes privadas virtuales" en línea: http://www.microsoft.com/latam/technet/articulos/Windows®2k/msppna/default.asp

Microsoft Windows® 2000 (2001) "Protocolo de túnel Punto a Punto (PPTP)" en línea: http://www. microsoft.com/ Windows®2000/ es/professional/help/default.asp?url=/Windows®2000/es/professional/help/access_pptp.htm

Microsoft Windows® 2000 (2001) "Cifrado de datos" en línea: http://www.microsoft.com/Windows®2000/es/advanced/help/default.asp?url=/Windows®2000/es/advanced/help/data_encryption.htm

Microsoft Windows® 2000 (2000) "MS-CHAP Versión 2" en línea: http://www.microsoft.com/Windows®2000/es/server/help/sag_RASS_MSCHAPv2.htm

Mª Nieves Gutiérrez González, Ana Rosa Sancho Buzón, Amadeo Casas Cuadrado (2005) "Estudio_VPN" en línea:
http://redes-linux.aii-inone.net/manuales/vpn/Estudio_VPN.pdf

Rubén González Antolín, Borja Ruiz Arroyo (2005) "VPN Redes Privadas Virtuales" en línea:
http://www.infor.uva.es/~jvegas/docencia/ar/seminarios/VPN.pdf

Windows® 2000(2005) "Seguridad de red privada virtual de Microsoft" en línea: http://rapanui.upa.cl/manuales/m_w2k.htm

Asignaturas (2005) "Redes Privadas Virtuales" en línea: http://asignaturas.diatel.upm.es/seguridad/VPN.htm

Netsystem (2005) "Instalación y configuración PPTP Windows® 98" en línea: http://support.netsystem.com:8080/vpn_ppp98_esp.asp

Netsystem (2005) "Instalación y configuración PPTP Windows® ME" en línea: http://support.netsystem.com:8080/vpn_pppME_esp.asp

Netsystem (2005) "Instalación y configuración PPTP Windows® 2000" en línea: http://support.netsystem.com:8080/vpn_ppp2K_esp.asp

Netsystem (2005) "Instalación y configuración PPTP Windows® XP" en línea: http://support.netsystem.com:8080/vpn_pppXP_esp.asp

Microsoft TechNet (2005) "Authentication Protocols" en línea:
http://www.microsoft.com/resources/documentation/Windows®/XP/all/reskit/en-s/ Default.asp?ur i=/resources/ documentation/Windows®/XP /all/reskit/en-us/prcg_cnd_pysl.asp

Microsoft Windows® 2000 (2005)"Autenticación" en línea: http://www.microsoft.com/Windows®2000/es/server/help/default.asp?url=/Windows®2000/es/server/help/sag_SEconceptsAuth.htm

Guenul (1997) "Redes" en línea: http://www. monografias.com /trabajos5/redman/redman.shtm

Geocities (2005)"Glosario de términos" en línea: http:// www. geocities. com /Athens/2693/glosario.html

Glosario de términos (2005) en línea: http://www.ivia.es/~sto/alice/glos/

Consejo Superior de Informática (2005) "Redes de área metropolitana" en línea: http://www.csi.map.es/csi/silice/gesred.html

Seguridad (2005) en línea: (http://asignaturas.diatel.upm.es/seguridad/VPN.htm.2005).

Microsoft (2005) en línea: (http ://www. microsoft. com/ windows2000/ es/ advanced/ help/ default.asp?url=/windows2000/es/advanced/help/data_encryption.htm.2005)