Universidad Autónoma
del Estado de Hidalgo

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA

IMPLANTACIÓN DE UNA RED PRIVADA VIRTUAL

TESIS PARA OBTENER EL TITULO
DE INGENIERÍA EN ELECTRÓNICA Y
TELECOMUNICACIONES

PRESENTA:

ESAÚ ARIAS LOA

ASESOR:

ING. ALEJANDRO AYALA ESPINOSA DE LOS MONTEROS

Pachuca de Soto Hidalgo, México. Enero del 2007

Agradecimientos

Agradezco a DIOS, por ser mi principal guía, por darme la fuerza necesaria para salir adelante y lograr alcanzar esta meta.

A mi Universidad Autónoma del Estado de Hidalgo, por darme la oportunidad de aprender y forjarme como profesional.

Agradecimiento especial para mi Asesor Guía Ing. Alejandro Ayala Espinosa de los Monteros, por su amistad, paciencia y su constante apoyo durante el desarrollo de esta tesis y para la culminación de la misma.

Al Ing. Miguel A. Rosas Yacotú, M. en C. Elías Varela Paz, Ing. Sandra Luz Hernández Mendoza, L. en C. Clara Mercado Jaramillo, Ing. José Salvador Ávila Flores, y al Ing. Mariano Arumir Rivas por el tiempo dedicado a revisar y corregir este trabajo.

A todos los catedráticos de la Ingeniería en Electrónica y Telecomunicaciones por su apoyo en mi formación profesional.

Gracias.

Dedicatorias

A mis padres: Javier Arias Carrasco y María de los Ángeles Loa Flores, por enseñarme a luchar hacia delante, por su gran corazón y capacidad de entrega, pero sobre todo por enseñarme a ser responsable, gracias a ustedes he llegado a esta meta. Los Amo.

A mis hermanos: Guadalupe, Javier y Yaressi, por mostrarme que ocupo un lugar especial en sus vidas y que siempre han sido mis amigos con quien he compartido maravillosos momentos.

A mis sobrinos Ángela y Eloy, dios los bendiga mis niños adorados.

A mi novia: Daniela por la ayuda y comprensión que me ha ofrecido.

A mis amigos y enemigos que me han enseñado a ser mejor cada día.

Resumen

En esta tesis se propone un esquema en la que los escenarios de una red privada virtual se configuran mediante el sistema operativo Microsoft Windows NT 4.0 para una organización. Aunque la configuración de su red puede ser diferente a la descrita en este documento, los conceptos básicos de redes privadas virtuales son útiles para cualquier entorno de red.

El uso tanto de redes públicas como privadas para crear una conexión de red se denomina red privada virtual (VPN).

El propósito de la presente investigación es comprender el uso y funcionamiento de las redes virtuales aprovechando la seguridad y costos mínimos que esta ofrece para realizar la conexión de un cliente remoto (móvil) a la red local de la empresa Logistic Meginter S.A. de C. V.

En los siguientes capítulos veremos el uso de las redes privadas virtuales en dicha organización y las tecnologías subyacentes que las hacen funcionar: El Protocolo de Túnel Punto a Punto (Point to Point Tunneling Protocol), PPTP, las redes privadas virtuales, la seguridad y el enrutamiento.

Índice general

Índice de figuras

Índice de Tablas

Introducción

Las siglas VPN (Virtual Private Network) significan Red Virtual Privada y no es mías que una conexión con la apariencia de un enlace dedicado (Punto a punto o Frame Relay) pero que se desarrolla a través de una red compartida,"internet". Utilizando una técnica llamada "Tunneling", los paquetes de información viajan a través de una red pública en una especie de "Túnel privado" que simula una conexión punto a punto y que aísla dicho trafico del resto de la red. Es como si, una vez conectados a Internet, tendiéramos un cable o circuito virtual y privado entre los usuarios de una misma organización que se encuentren en ese momento conectado.

Es llamada virtual porque depende de conexiones virtuales, esto es, conexiones temporales que no tienen una presencia física real, pero consiste en el ruteo de paquetes sobre varias máquinas dentro de Internet sobre una base de ruteo adicional.

La novedad en estas conexiones, o intercambio de paquetes PPP (Protocolo Punto a Punto) es que se realiza a través de una red pública de datos, como internet y no a través de enlaces directos o líneas dedicadas. Lo que se trata es de encapsular protocolos de red ya existentes (IPX, IP y Netbeui) en paquetes PPP y estos a su ves son encapsulados en protocolos de Tunneling, PPTP, proporcionado por Microsoft en Windows 98 y Windows NT 4.0, resultado: de una manera sencilla, podremos compartir redes locales remotas a través de VPN a costo de llamada local (ISP) y sin necesidad de contratar costosas líneas dedicadas.

Las VPN traen consigo disminución de costos de comunicaciones que suponen los enlaces directos entre las redes de la empresa, así como también permite a los usuarios remotos (móviles) acceder a los recursos de la empresa a través de una simple conexión a Internet y reduce los considerables costos de mantenimiento y soporte de los usuarios.

Microsoft Windows NT 4.0 incluye soporte para la tecnología de redes privadas virtuales, que aprovecha la conectividad IP de Internet para conectar clientes y oficinas remotas.

Logistic Meginter S.A. de C. V. es una organización dedicada al diseño y fabricación de productos electrónicos que posee su sede corporativa principal en México D.F. y tiene sucursales y socios comerciales de distribución repartidos por todo el país. Logistic Meginter S.A. de C. V. ha desarrollado una solución de red privada virtual mediante el sistema operativo Microsoft Windows NT 4.0 con el fin de conectar a los usuarios con acceso remoto, sucursales y socios comerciales.

Antecedentes.

El concepto de VPN ha estado presente desde hace algunos años en el mundo de la redes. A mediados de los 80's, grandes portadoras fueron ofrecidas como VPN para servicios de voz, de manera que las compañías podían tener la apariencia de una red privada de voz, mientras compartían recursos de una red mucho mayor. Este concepto se está aplicando ahora tanto para voz como para datos de la misma manera. Una VPN es una red de datos aparentemente privada, pero la cual utiliza los recursos de un red de información mucho mayor. La Internet es la plataforma ideal para crear una VPN.

Inicialmente los viajantes, empleados de Logistic Meginter S.A. de C.V. accedían a los datos que necesitaban de la central mediante llamadas telefónicas, en ella se encontraban varias operadoras encargadas de acceder a los datos y comunicárselos a los empleados.

Ante al gran desarrollo de las tecnologías de telecomunicaciones se pensó en una reestructuración total en el modo de acceder a los datos por parte de los viajantes, creando una red que interconectara a éstos con la central y posibilitando que tuvieran acceso total a todos los equipos conectados a la red con independencia del tiempo o del lugar donde se encontraran.

La empresa deseaba también una garantía de seguridad en las transferencias de información que evitara que sus datos fuesen interceptados por personas ajenas a la empresa.

Justificación

Todo tipo de personas y organizaciones requieren de metodologías para transmitir o recibir información de forma rápida y eficiente. Además que esta información sea segura y esto ha llevado a idear tecnologías y actualización de las ya existentes con el propósito de satisfacer las necesidades de cada organización por tal motivo esta tesis opta por captar información que sea útil para cualquier profesionista y así llevar a cabo una comunicación con otros equipos aprovechando al máximo su capacidad como lo son las Redes Privadas Virtuales.

Las Redes Privadas Virtuales (VPN) constituyen una tecnología a la cual se le está dando cada vez mayor importancia puesto que permiten la transmisión de información a grandes distancias sin necesidad de implantar una compleja y costosa infraestructura de red. Es por eso que es importante que cualquier Ingeniero que desee desarrollarse en el área de las redes de telecomunicaciones conozca esta tecnología.

Objetivos de la Tesis

Objetivo general:

Implementar una red virtual para el acceso remoto de los usuarios móviles a la red local de la empresa Logistic Meginter S.A. de C. V. Así como su funcionamiento y sus elementos que la componen.

Objetivos específicos:

Los objetivos específicos son los siguientes:

- Proporcionar movilidad a los empleados.
- Acceso a la base de datos central sin utilización de operadores telefónicos.
- Interconexión total a la red de todos los comerciales (empleados), de forma segura a través de una infraestructura pública.
- Intercambio de información en tiempo real.
- Correo electrónico corporativo.
- Acceso remoto a la información corporativa.
- Teletrabajo.

Estructura de la tesis

Esta tesis se encuentra dividida en seis capítulos y las referencias bibliográficas, el capitulo 1 descripción general de redes privadas virtuales; contiene una introducción a las VPN y proporciona las herramientas fundamentales de las VPN para su análisis de conexión.

En el capítulo 2 Descripción del Proyecto; el cual es el punto de parida se menciona la parte fundamental por la cual se implementa la VPN a la empresa Logistic Meginter S.A. de C.V.

El capítulo 3 Protocolo de Túnel Punto a Punto; se hace referencia al protocolo en especial como es PPTP; también se describen todas las características del mismo y su forma de Encapsulación.

Capítulo 4 Seguridad y Direccionamiento para la VPN de Logistic Meginter; En esta sección se describen las funciones de seguridad de las conexiones VPN con PPTP ya que la seguridad es una parte importante para la VPN que se introducirá a Logistic Meginter, de igual forma se estudiara el funcionamiento de las VPNs, para así entender como se afecta el direccionamiento (addressing) y el enrutamiento (routing) para la creación de la VPN.

En el Capitulo 5; Resolución de problemas de las VPNs; se enfoca a resolver los problemas comunes de las VPNs, como la conectividad IP, del establecimiento de la conexión de acceso remoto y del enrutamiento. Y se enlistan consejos para la resolución de estos para aislar el problema de configuración o de infraestructura que esta causando el problema en la VPN.

Finalmente las conclusiones y trabajo futuro se presentan en el capítulo 6.

Capítulo1

Descripción general de Redes Privadas Virtuales

Una red privada virtual, es una extensión de una red privada que utiliza enlaces a través de redes públicas o compartidas como Internet. Con una VPN se pueden enviar datos entre dos computadoras a través de redes públicas o compartidas en una manera que emula las propiedades de un enlace punto a punto privado.

Para emular un enlace punto a punto, los datos son encapsulados o envueltos, con una cabecera que proporciona la información de enrutamiento (routing) que le permite atravesar la red pública o compartida para llegar a su destino. Para emular un enlace privado, los datos enviados son encriptados para tener confidenciabilidad. Los paquetes (packets) que son interceptados en la red pública o compartida son indescifrables sin las claves de encriptación. El enlace en el cual los datos son encapsulados y encriptados se conoce como una conexión de red privada virtual (VPN).

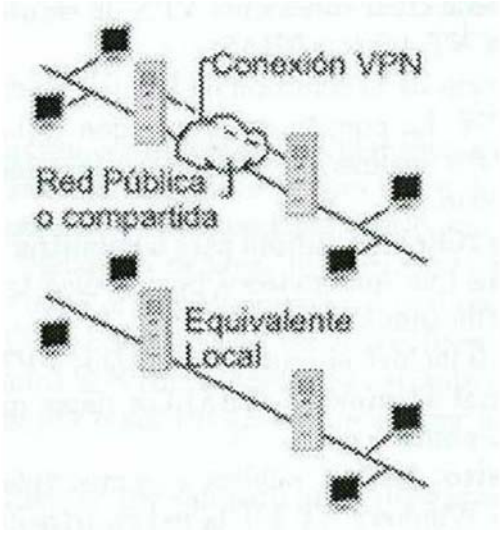

Figura 1.1: Red Privada Virtual (Virtual Private Network VPN)

Con las conexiones VPN los usuarios que trabajan en casa o de manera móvil pueden tener una conexión de acceso remoto a un servidor de la organización utilizando la infraestructura proporcionada por una red pública como Internet. Desde el punto de vista del usuario, la VPN es una conexión punto a punto entre la computadora, el cliente VPN, y el servidor de la organización, el servidor VPN. La infraestructura exacta de la red pública o compartida es irrelevante porque desde el punto de vista lógico parece como si los datos fueran enviados por un enlace privado dedicado.

Con las conexiones VPN, tanto las conexiones de acceso remoto como las conexiones enrutadas, una organización puede cambiar de líneas rentadas (loased lines) o accesos telefónicos (dial-up) de larga distancia a accesos telefónicos locales o líneas rentadas con un proveedor de servicio de Internet (Internet Service Provider, ISP).[1] [14]

1.1. Elementos de una conexión VPN.

Una conexión VPN de Windows NT 4.0 incluye los siguientes componentes, tal como se ilustra en la figura 1.2.

Servidor VPN. Una computadora que acepta conexiones VPN de clientes VPN. Un servidor VPN puede proporcionar una conexión de acceso remoto VPN o una conexión de enrutador a enrutador.

Cliente VPN. Una computadora que inicia una conexión VPN con un servidor VPN. Un cliente VPN o un enrutador tiene una conexión de enrutador a enrutador. Las computadoras con Microsoft® Windows NT® versión 4.0, Microsoft® Windows® 95 y Microsoft® Windows® 98 pueden crear conexiones de acceso remoto VPN a un servidor VPN con Windows NT 4.0. Las computadoras con Windows NT Server 4.0 que ejecutan el Servicio de Enrutamiento y Acceso Remoto (Routing and Remote Access Service, RRAS) puede crear conexiones VPN de enrutador a enrutador con un servidor VPN con Windows NT 4.0 con RRAS.

Túnel. La porción de la conexión en la cual sus datos son encapsulados.

Conexión VPN. La porción de la conexión en la cual sus datos son encriptados. Para conexiones VPN seguras, los datos son encriptados y encapsulados en la misma porción de la conexión.

Protocolos de túnel. Se utilizan para administrar los túneles y encapsular los datos privados. (Los datos que son enviados por el túnel también deben de ser encriptados para que sea una conexión VPN).

Windows NT 4.0 incluye el protocolo de túnel PPTP.

Datos del túnel (tunneled data). Los datos que son generalmente enviados a través de un enlace punto a punto.

Red de transito. La red pública o compartida que es cruzada por los datos encapsulados. Para Windows NT 4.0, la red de tránsito es siempre una red IP.[2] [11]

---

[1] www.es.wikipedia.org/wiki/Red privada virtual

[2] www.ugr.es/informatica/redes/vpn/vpn.htm

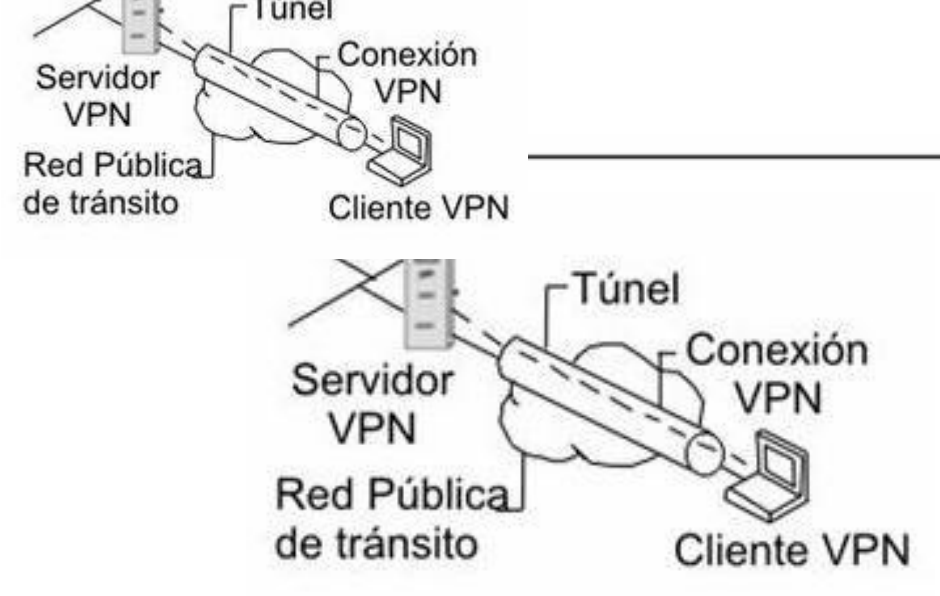

Figura 1.2: Componentes de una conexión VPN

1.2. Tipos de VPN.

Existen diferentes formas de que una organización pueda implementar una VPN. Cada fabricante o proveedor ofrece diferentes tipos de soluciones VPN. Cada corporación tendrá que decidir la que mías le convenga. Los tipos diferentes de VPN son:

- VPN de firewall
- VPN de router y de concentrador
- VPN de sistema operativo
- VPN de aplicación
- VPN de proveedor de servicios

1.2.1.VPN de firewall.

Un firewall (llamado también cortafuegos o servidor de seguridad) es un sistema de seguridad que implanta normas de control de acceso entre dos o más redes. Se trata de un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el Web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no. Un firewall puede ser un dispositivo software o hardware.

Es muy común que se utilice un firewall para proporcionar servicios VPN. Empresas como Cisco Systems, Nortel Networks y 3Com ofrecen en muchos de sus dispositivos firewall soporte para VPN. Una VPN basada en firewall tiene la ventaja de que simplifica la arquitectura de la red al establecer un único punto de control de seguridad. Además,

los ingenieros de redes solo tienen que hacerse expertos en una tecnología, en lugar de tener que aprender a administrar un firewall y la VPN de forma separada.

Entre los inconvenientes se puede mencionar que tener la VPN en un firewall convierte al dispositivo en algo más complejo, por lo que se debe ser más cuidadoso en su configuración o de lo contrario cualquier intruso podría tener acceso no autorizado a la red. Otra desventaja ocurre debido a que tener firewall y VPN juntos, se ejerce presión al rendimiento del firewall. Esto ocurre principalmente si se tienen conectados cientos o incluso miles de usuarios.

1.2.2. VPN de router y de concentrador

Empresas como Cisco, Nortel y 3Com entre otros también ofrecen servicios VPN integrados dentro de un router o un dispositivo llamado concentrador VPN. Tanto el router como el concentrador VPN están especialmente diseñados para las conexiones VPN sitio a sitio y acceso remoto. Cuenta con las tecnologías VPN más importantes y los métodos de autenticación y cifrado para proteger los datos transmitidos.

Este dispositivo esta especialmente diseñado para las VPN, por lo que se trata de la solución VPN más rápida. Resulta ser mías fácil agregarles tarjetas con el fin de incrementar el rendimiento. Dependiendo de la implementación, estas VPN pueden configurarse para utilizar certificados, servicios de autenticación externos o claves de seguridad.

1.2.3. VPN de sistema operativo

Los sistemas operativos como Windows de Microsoft, Netware de Novell o Linux en sus diferentes distribuciones (Red Hat, Debian) ofrecen servicios de VPN ya integrados. La principal ventaja de esta solución es que resulta ser económica ya que en un mismo sistema operativo se pueden contar con una gran variedad de servicios (servidor Web, de nombres de dominio, acceso remoto, VPN) y mejora los métodos de autenticación y la seguridad del sistema operativo. Tiene la desventaja de que es vulnerable a los problemas de seguridad del propio sistema operativo. Estas VPN se utilizan mías para el acceso remoto.

1.2.4. VPN de aplicación

Este tipo de VPN es poco común. Una VPN de aplicación es un programa que añade posibilidades VPN a un sistema operativo. Sin embargo, este programa no queda integrado con el sistema operativo. La ventaja de este tipo de VPN es que la aplicación añade seguridad extra a la que podría ofrecer una VPN integrada al sistema operativo. Un ejemplo de esta VPN es el programa ViPNet de lnfotecs.

La desventaja es que estas VPN no soportan una gran cantidad de usuarios y son mucho mías lentas que una VPN basada en hardware. Si se utilizan en Internet, son vulnerables a las fallas de seguridad del sistema operativo que contiene a la aplicación.

1.2.5. VPN de proveedor de servicios

Este tipo de VPN es proporcionada por un proveedor de servicios. Al principio las VPN de proveedor de servicios se basaban en tecnologías tales como X.25 y Frame Relay, posteriormente ATM y SMDS y finalmente se ofrecen redes basadas en IP. El proveedor de servicios es la empresa propietaria de la infraestructura tales como equipos y líneas de transmisión que ofrece líneas dedicadas virtuales a sus clientes.

El cliente se conecta a la red del proveedor de servicios a través de un dispositivo de equipo terminal del cliente (CPE) como puede ser un router. El CPE se conecta a través de medios de transmisión al equipo del proveedor de servicios, que puede ser X.25, Frame Relay, un conmutador ATM o un router IP. La línea virtual que se le proporciona al cliente mediante el proveedor de servicios se le llama circuito virtual (VC).

El proveedor de servicios puede cargar o una tarifa plana para el servicio VPN, que habitualmente depende del ancho de banda disponible para el cliente, o una tarifa basada en el uso, que puede depender del volumen de datos intercambiados o de la duración del intercambio de datos.

Acuerdos a nivel del servicio (SLA, Service Level Agreements). Los SLA son contratos negociados entre proveedores VPN y sus abonados en los que se plantean los criterios de servicio que el abonado espera tengan los servicios específicos que reciba. La SLA es el único documento que está a disposición del abonado para asegurar que el proveedor VPN entrega el servicio o servicios con el nivel y calidad acordados. Si se ha de implementar una VPN basada en proveedor de servicios, este documento es de vital importancia para asegurar un buen servicio.[3] [7]

1.3. Topologías de VPN.

La topología VPN que necesita una organización debe decidirse en función de los problemas que va a resolver. Una misma topología puede ofrecer distintas soluciones en diferentes compañías u organizaciones. En una VPN podemos encontrar las siguientes topologías:

Para las VPN de sitio a sitio:

- Topología radial
- Topología de malla completa o parcial
- Topología hibrida

Para las VPN de acceso remoto:

[3] Redes Privadas Virtuales de Cisco Secure

- Topología de acceso remoto

En las VPN basadas en ATM y Frame Relay, los enlaces que conectan las oficinas centrales con sus sucursales son circuitos virtuales (VC), mientras que en las VPN basadas en IP como Internet, estos enlaces son los túneles que se establecen a través de Internet.

1.3.1. Topología radial.

En una VPN de sitio a sitio, ésta es la topología más común. Aquí, las sucursales remotas se conectan a un sitio central, como se puede ver en la figura 1.3. Las sucursales podrían intercambiar datos entre ellas, sin embargo, este tipo de datos resulta ser muy insignificante. La mayor parte del intercambio de datos se da con las oficinas centrales de la compañía. Los datos intercambiados entre las sucursales siempre viajan a través del sitio central.

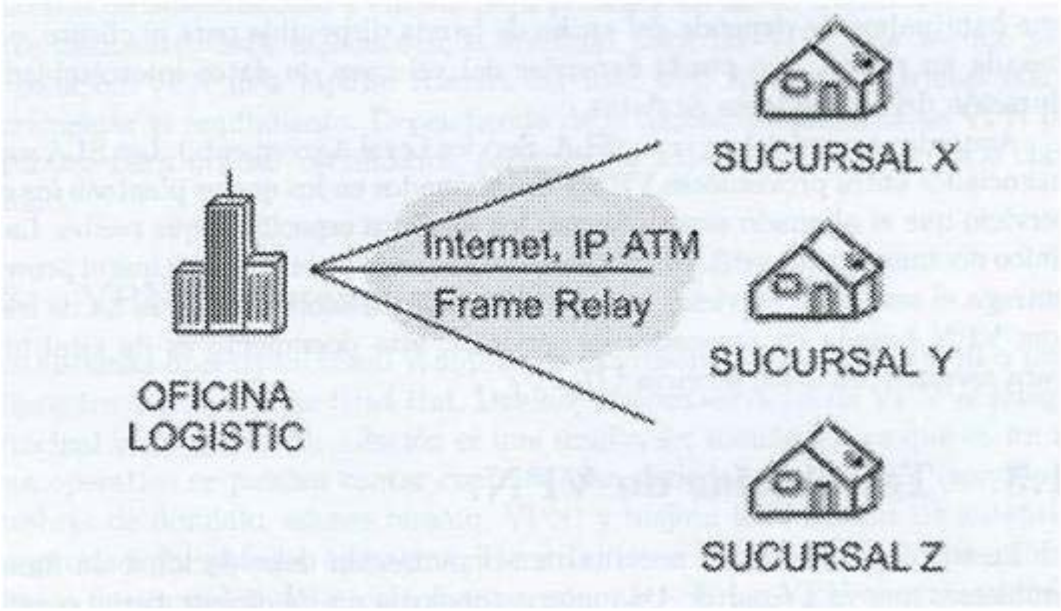

Figura 1.3: Topología radial

1.3.2. Topología de malla completa o parcial.

Es implementada en corporaciones que no tienen una estructura demasiado jerárquica. Aquí, las diversas LAN de la compañía pueden realizar un intercambio constante de datos entre ellas. Una empresa puede utilizar una topología de malla completa si todas las LAN se comunican entre si o una topología de malla parcial, si sólo algunas LAN mantienen intercambio de datos. En la gran mayoría de los casos se utiliza sólo malla parcial. La figura 1.4 muestra una topología de malla:

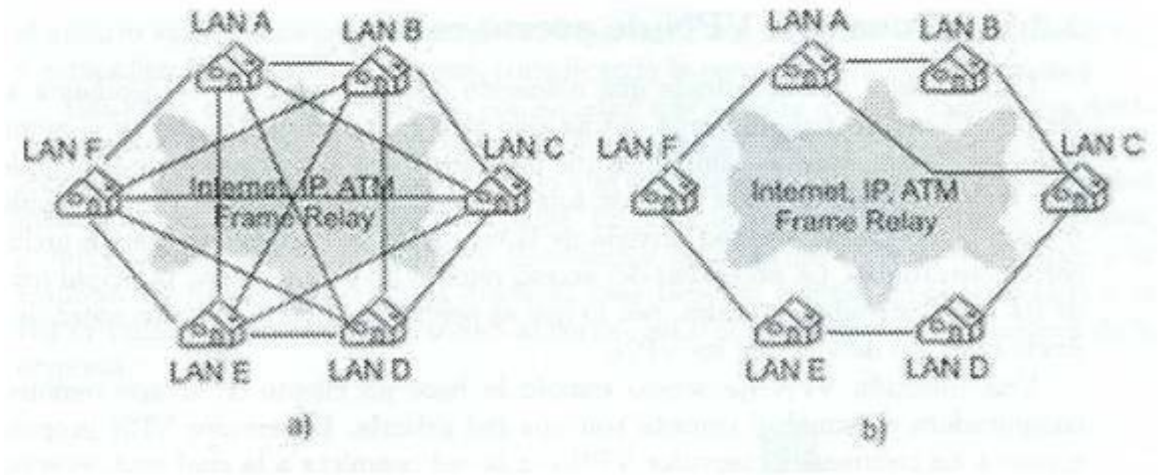

Figura 1.4: Topología de malla: a) Completa b) Parcial

1.3.3. Topología hibrida.

Las redes VPN grandes combinan la topología radial y la topología de malla parcial. Como ejemplo, una empresa multinacional podría tener acceso a redes implementadas en cada país con una topología radial, mientras que la red principal internacional estaría implementada con una tecnología de malla parcial.

1.3.4. Topología de acceso remoto.

Esta topología consiste en un enlace punto a punto entre el usuario remoto y la oficina central utilizando tramas tunneling PPP intercambiadas entre el usuario remoto y el servidor VPN. El usuario y el servidor establecen conectividad usando un protocolo de capa 3, siendo el mías común IP, sobre el enlace PPP entonelado e intercambian paquetes de datos sobre el.[4] [11]

1.4. Conexiones VPN.

Crear la VPN es muy similar a establecer una conexión punto a punto utilizando el acceso telefónico a redes (dial-up networking) y los procedimientos de enrutamiento de marcado por demanda (demand-dial routing procedures). Hay dos tipos de conexiones VPN: la conexión VPN de acceso remoto y la conexión VPN de enrutador a enrutador.

[4] www.ugr.es/informatica/redes/vpn/vpn.htm

1.4.1. Conexión VPN de acceso remoto.

Conectarse a una red desde una ubicación distante es lo que se denomina acceso remoto. El acceso remoto a una red ha sido algo de gran importancia en el mundo de las redes, ya que muchas compañías que promueven viajes de trabajo de sus empleados o el trabajo desde el hogar o desde una pequeña oficina remota. Y estos empleados necesitan conectarse a la red privada de la compañía para consultar ciertos archivos o correo electrónico. La necesidad del acceso remoto ha sido la causa principal del auge de las redes privadas virtuales, por lo que es preciso analizarlo un poco antes de verlo desde el punto de vista de las VPN.

Una conexión VPN de acceso remoto la hace un cliente de acceso remoto, una computadora personal, y conecta con una red privada. El servidor VPN proporciona acceso a los recursos del servidor VPN o a la red completa a la cual está conectado el servidor VPN. Los paquetes (packets) enviados desde el cliente remoto a través de la conexión VPN se originan en la computadora cliente de acceso remoto.

El cliente de acceso remoto (cliente VPN) se autentifica a si mismo ante el servidor de acceso remoto (el servidor VPN) y, para autentificación mutua, el servidor se autentifica a si mismo ante el cliente.

Necesidades de acceso remoto.

Con el incremento de las relaciones comerciales a nivel internacional, la movilidad geográfica de puestos de trabajo está llevando a las redes privadas a una situación bastante complicada. Los usuarios precisan conexiones que les permitan el acceso a las corporaciones desde cualquier lugar del mundo. Estas necesidades, unidas a las surgidas como consecuencia de la demanda de telecomunicaciones a tiempo completo, están aumentando drásticamente el número de oficinas remotas que una compañía debe interconectar. Como resultado, muchas redes privadas están convirtiéndose en redes muy complicadas de administrar.

El establecimiento de un sistema de acceso remoto en una red debe ser planeado cuidadosamente por lo que se debe definir claramente quienes van a necesitar del acceso remoto y que tecnología se utilizara para satisfacer las necesidades de esos usuarios.

De acuerdo a la figura 1.5, existen diferentes tipos de usuarios dependiendo las necesidades de una organización y esto hará que las soluciones de acceso remoto también varíen de acuerdo a dichas necesidades. Los usuarios pueden ser de la siguiente forma:

- Usuarios móviles
- Usuarios de oficina remota

Usuarios móviles. Son aquellos que necesitan realizar viajes de trabajo a otro estado o país. Estos usuarios requieren de acceder a los recursos de la red de la oficina principal tales como su correo electrónico o sus archivos desde esa ubicación distante. Si

el usuario viaja a otro país, entonces tiene que lidiar con diferentes sistemas telefónicos y compañías de telecomunicaciones, complicando la conexión a la red corporativa.

Usuarios de oficina remota. Son aquellos que acceden a la red corporativa desde una ubicación fija distante como es una pequeña oficina o el hogar. El tele trabajo es una forma flexible de organización del trabajo que consiste en el desempeño de la actividad profesional en el domicilio del trabajador. Engloba una amplia gama de actividades, e implica el uso de computadoras y la conexión permanente entre el trabajador y la empresa. El usuario que trabaja desde su casa tiene su computadora conectada a la red privada y desde ahí tienen acceso al correo electrónico o algunas aplicaciones de la empresa.

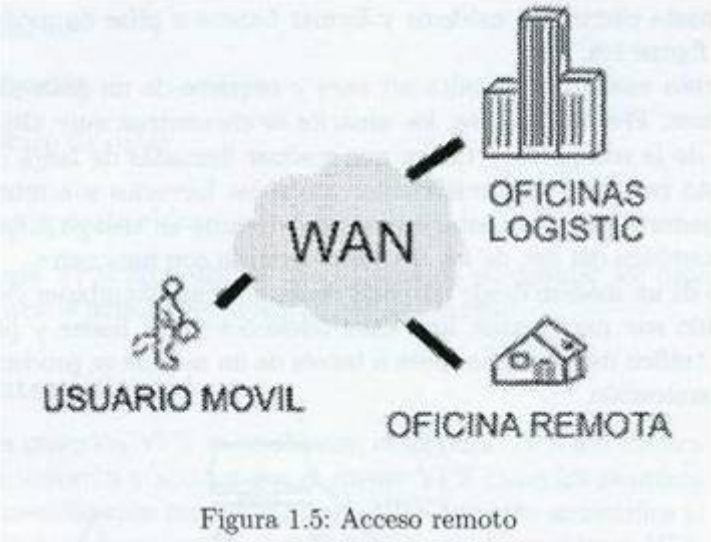

Figura 1.5: Acceso remoto

Si una compañía requiere de un sistema de acceso remoto lo primero que se tiene que evaluar es que tipo de usuarios tiene, ya sea móviles, de oficina remota o ambos. Una vez hecho esto, lo que debe hacerse es definir las necesidades de estos usuarios que se deben satisfacer. Estas necesidades pueden ser:

- Acceso remoto al correo electrónico.
- Acceso remoto a los archivos del usuario.
- Acceso remoto a una aplicación centralizada.
- Acceso remoto a aplicaciones personalizadas o programas groupware.
- Acceso remoto a la intranet o extranet.

Después de examinar estas necesidades, lo siguiente es estimar los requerimientos del ancho de banda para los diferentes usuarios. Esto es necesario para determinar qué tipo de conexión es necesaria para establecer el acceso remoto. También es importante determinar si dicha conexión es económicamente rentable para la empresa.

Acceso remoto antes de las VPN.

Antes de que las VPN fueran tomadas como opción para el acceso remoto, era común que una corporación instalara módems desde los cuales el usuario remoto hacia una llamada para estar en conexión con la red corporativa. En redes donde no hay muchos usuarios remotos se pueden agregar solo uno o dos módems a una computadora configurada como Servidor de Acceso Remoto (RAS, Remote Access Server). En el caso de organizaciones que mantienen muchos usuarios remotos, es preciso instalar desde decenas hasta cientos de módems y formar bancos o pilas de módems como se puede ver en la figura 1.6.

El acceso remoto así resulta ser caro y requiere de un gran soporte por parte de las empresas. Frecuentemente, los usuarios se encuentran muy alejados de las oficinas centrales de la compañía y tienen que realizar llamadas de larga distancia o llamada 0-800. Esto resulta ser especialmente caro si las llamadas son internacionales y si los teletrabajadores requieren estar conectados durante un tiempo largo. El acceso remoto requiere también del uso de los RAS que también son muy caros.

El uso de un módem desde otro país causa muchas dificultades ya que las velocidades de conexión son muy lentas, una línea telefónica no es buena y puesto que la mayor parte del tráfico internacional pasa a través de un satélite se producen muchos retrasos en la comunicación.

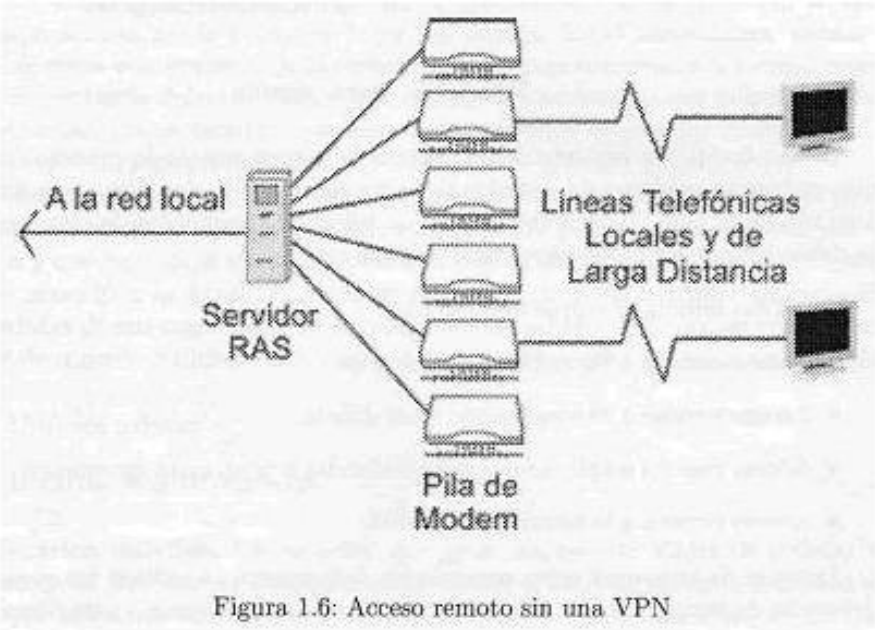

Figura 1.6: Acceso remoto sin una VPN

1.4.2. Conexión VPN de enrutador a enrutador.

Una conexión VPN de enrutador a enrutador es hecha por un enrutador y conecta dos porciones de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la cual el servidor VPN esta conectado. El enrutador que llama (el cliente VPN) se autentifica así mismo ante el enrutador que responde (el servidor VPN), y para autentificación mutua, el enrutador que responde se autentifica a si mismo ante el enrutador que llama.[5] [7]

1.5. Propiedades de la conexión VPN utilizando PPT.

- Encapsulación.
- Autentificación.
- Encriptación de datos.

1.5.1. Encapsulación.

La tecnología VPN proporciona una manera de encapsular los datos privados con una cabecera que le permite atravesar la red de transito.

1.5.2. Autentificación.

Para que la conexión VPN se establezca, el servidor VPN autentifica al cliente VPN que intenta la conexión y verifica que el cliente VPN tiene los permisos apropiados. Si se utiliza la autentificación mutua, el cliente VPN también autentifica al servidor VPN, proporcionando protección contra el suplantamiento de servidores VPN.

1.5.3. Encriptación de datos.

Para asegurar la confidenciabilidad de los datos que atraviesan la red de transito pública o compartida, estos son encriptados por el emisor y desencriptados por el receptor. El proceso de encriptación y des encriptación depende de que tanto el emisor como el receptor conozcan una misma clave de encriptación.

Los paquetes enviados que sean interceptados a lo largo de la conexión VPN en la red de tránsito son ininteligibles para cualquiera que no tenga la clave de encriptación común. La longitud de la clave de encriptación es un parámetro de seguridad importante. Pueden utilizarse técnicas computacionales para determinar la clave de encriptación. Tales técnicas requieren mías poder y tiempo de calculo entre mías grande sea la clave de encriptación. Por lo tanto, es importante utilizar un tamaño de clave lo mías grande posible.

[5] Redes Privadas Virtuales de Cisco Secure

Además, entre mías información esté encriptada con la misma clave, mías fácil es descifrar los datos encriptados.[6] [14]

1.6. Conexiones VPN sobre Internet.

Al utilizar una conexión VPN sobre Internet, se evitan gastos de larga distancia a la vez que toma ventaja de la disponibilidad global de Internet.

1.6.1. Acceso remoto sobre Internet.

En lugar de que el cliente de acceso remoto tenga que hacer una llamada de larga distancia a un servidor de acceso de redes (Network Access Server, NAS) corporativo o contratado, el cliente puede llamar a un ISP local. Al utilizar la conexión física establecida con el ISP local, el cliente de acceso remoto inicia una conexión a través de Internet hacia la del servidor VPN de la organización. Una vez que la conexión VPN es creada, el cliente de acceso remoto tiene acceso a los recursos de la red local (correo, impresoras en red, archivos, etc.).

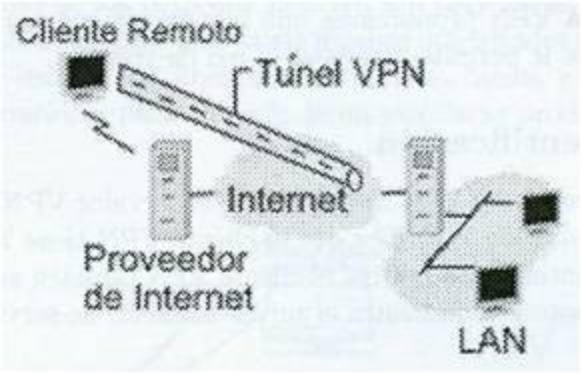

Figura 1.7: Acceso remoto sobre Internet

1.7. Administrando las redes privadas virtuales.

Las redes privadas virtuales deben ser administradas como cualquier otro recurso de red. Respecto a la seguridad de la VPN, particularmente con las conexiones VPN sobre Internet, debe tratarse cuidadosamente. Hay que considerar las siguientes preguntas:

- ¿Dónde se almacenarán los datos de la cuenta del usuario?
- ¿Quien puede crear conexiones VPN?
- ¿Cómo verificará el servidor VPN la identidad del usuario que esté tratando de hacer la conexión VPN?

[6] www.es.wikipedia.org/wiki/Red privada virtual

- ¿Cómo registrará el servidor VPN la actividad de la VPN?

- ¿Cómo puede el servidor VPN ser administrado utilizando los protocolos de administración de redes e infraestructura estándar?

1.7.1. Administrando a los usuarios.

Debido a que es administrativamente infactible tener cuentas de usuario separadas en servidores separados para el mismo usuario y tratar de mantenerlas actualizadas simultáneamente, la mayoría de los administradores establece una base de datos maestra para las cuentas en el controlador de dominio primario (Primary Domain Controller, PDC).

1.7.2. Administrando los accesos.

La administración de accesos para conexiones VPN de acceso remoto para Windows NT 4.0 se hace a través de la configuración de las propiedades del acceso telefónico en las cuentas de los usuarios.

Para administrar el acceso remoto de un modo individual, se activaría la opción Grant dialin permission to user en las propiedades de aquellas cuentas de usuarios que podrán crear conexiones de acceso remoto y modificar las propiedades del Servicio de Acceso Remoto o del Servicio de Acceso Remoto y Enrutamiento de acuerdo a los parámetros necesarios para la conexión.

1.7.3. Administrando la autentificación.

El Servicio de Acceso Remoto de Windows NT 4.0 utiliza la autentificación de Windows NT, El Servicio de Acceso Remoto y Enrutamiento de Windows NT 4.0 (Routing and Remote Access Service, RRAS) puede ser configurado para utilizar ya sea Windows NT o RADIUS como un agente de autentificación.

1.7.4. Autentificación de Windows NT 4.0

Si seleccionamos a Windows NT 4.0 como el agente de autentificación, entonces las credenciales de los usuarios enviadas por los usuarios que intentan establecer las conexiones remotas son autentificadas utilizando los mecanismos de autentificación de Windows NT 4.0.

1.7.5. Administración de red.

La computadora que actúa como servidor VPN puede participar en un ambiente con el Protocolo Simple de Administración de Redes (Simple Network Management Protocol, SNMP) como un agente SNMP si el Servicio SNMP de Windows NT 4.0 está instalado. El servidor VPN registra la información de administración en varios identificadores de objetos de la Base de Información de Administración de Internet (Internet Management Information Base, MIB) II, el cual se instala con el servicio SNMP de Windows NT 4.0.[7] [9]

[7] Check Point NG VPN-1/Firewall-1.

Capítulo 2

Descripción del Proyecto.

2.1. Descripción del área de estudio.

A continuación se describe la manera en que el escenario de red privada virtual se configuraría mediante el sistema operativo Windows NT server a la empresa Logistic Meginter S.A. de C.V.

El servidor VPN, que se encuentra en la oficina central, proporciona acceso remoto y conexiones VPN PPTP. Además, el servidor VPN proporciona el enrutamiento de paquetes hacia ubicaciones en Internet.

Esta empresa será provista de una dirección IP fija con un dominio en Internet proporcionado por un proveedor que además proveerá una página Web, cuentas de correo electrónico y servidor FTP.

Todo esto será creado, mantenido y administrado por dicha empresa la que pagara una cuota mensual.

Desde 1990 Logistic Meginter posee Redes de Área Local instaladas en cada uno de las sedes que tiene distribuidas. Estas redes satisfacen actualmente los requerimientos de los usuarios, no obstante limitan las posibilidades de crecimiento para futuros desarrollos y cambios tecnológicos.

Se propone la siguiente solución: Creación de una Red Privada Virtual (VPN) para interconectar todas las sedes de una forma segura.

2.1.1. Localización.

La presente investigación tuvo lugar en la empresa Logistic Meginter S.A. de C.V., en el Distrito Federal, uno de los 32 Estados en que se divide el territorio mexicano. Cuyas coordenadas geográficas son: Al norte 19º 36´, al sur 19º 03´ de latitud norte; al este 98º 57´, al oeste 99º 22´ de longitud oeste. El Distrito Federal colinda al norte, este y oeste con el Estado de México y al sur con el estado de Morelos. El Distrito Federal representa el 0.1 % de la superficie del país, con una superficie de 1,489.86 Km2.

2.1.2. La Empresa (Logistic Meginter S.A. de C.V.)

Logistic Meginter S.A. de C.V. fue constituida en 1980. Se dedica a la fabricación y distribución de productos electrónicos, siendo una de las empresas mías importantes en México D.F. Logistic Meginter S.A. de C.V. es miembro de la prestigiosa asociación nacional de fabricantes de productos electrónicos (ANFPE), y colabora en diferentes proyectos con distintas Universidades de todo el país.

Logistic Meginter es una potencia industrial global. Es el tercer fabricante de productos electrónicos del país y sus productos son los que mías se venden actualmente en América Latina.

2.1.3. La Problemática de la Empresa.

Logistic, cuya sede está en México D.F., tiene un personal con un alto índice de desplazamientos, sobre todo en los departamentos de ventas y de soporte técnico. Antes de implementar su solución VPN, Logistic tenía facturas telefónicas mensuales muy elevadas, ya que los usuarios llamaban directamente a su sede central desde cualquier lugar del mundo.

Mientras que los productos de Logistic son los preferidos de millones de personas en todo el mundo, lo que hace funcionar a esta empresa es la información. Para estar a la vanguardia del mercado, llevar los productos adecuados al mercado y para mantener una organización global de gran éxito.

La base de usuarios remotos de la empresa, que tradicionalmente soportaba un caro sistema de acceso remoto (RAS) de números 800, esta creciendo geométricamente. Cualquiera del personal de la empresa que tuviera una computadora portátil podía llamar (los directivos, ejecutivos de cuentas y directores regionales remotos), con lo que se formaba una comunidad de usuarios remotos que crecía muy rápidamente.

2.2. Necesidades de la Empresa.

Para satisfacer las necesidades de la comunidad remota, se tiene que aumentar su capacidad, pero todo aumento en la capacidad de RAS, incluyendo módems y servicios de red, exige una inversión adicional de capital. El creciente número de bancos de módems también provoca que sea necesaria mas gestión y personal para dar soporte a los frecuentes cambios en el software y a la corrección de configuraciones.

Pero toda esta inversión y este esfuerzo no pueden satisfacer las demandas de la comunidad remota. Los usuarios siguen teniendo problemas con la velocidad de los módems y con las desconexiones. La gestión del entorno del acceso telefónico se ha convertido en una presión importante para los recursos de Logistic Meginter. Todo lo que esta fuera del edificio esta también fuera del control de la empresa y se necesita recuperar el control.

Lo que obliga a estudiar el acceso telefónico es lo siguiente: sencillamente no se puede seguir luchando contra la capacidad y el coste de los módems. Se Ofrece servicios 800 a los usuarios de acceso telefónico y es terriblemente caro. Y como la cantidad de usuarios sigue creciendo y los tiempos de conexión son mayores, no se puede soportar el coste de que tres personas se conecten y desconecten a otros hasta ocho horas después.
Por consiguiente uno de los retos mas importantes es el alto coste de RAS:

- El escalado de los usuarios remotos.
- Los plazos de entrega para aumentar la capacidad.
- El hardware añadido.
- La configuración de las líneas RDSI.

La empresa presenta problemas en la comunicación en cuanto a la movilidad de sus viajantes, la velocidad de acceso a los datos de la central y la seguridad contra elementos externos. Se requiere la interconexión de los 25 viajantes empleados de la empresa con la intranet de la empresa y entre ellos mismos, posibilitando la capacidad a todos ellos de conectarse en cualquier momento, en cualquier lugar, poder acceder a los datos del servidor central y a cualquier elemento conectado a ella, tales como ordenadores de la red Lan, otros viajantes conectados a la red, impresoras remotas, faxes, etc.

2.2.1. La necesidad de conexión con los distribuidores de forma flexible.

Uno de los recursos empresariales más importantes de la empresa Logistic Meginter es la extranet que comunica con su creciente número de distribuidores y proveedores. Pero Logistic se da cuenta de que la creación de las conexiones de la extranet requiere una infraestructura de firewalls independiente y además de otros inconvenientes de añadir más recursos a la red de una empresa.

Logistic, como cualquier otra empresa, se topa con muchos problemas por resolver al conectarse con empresas externas e independientes. Junto con los largos plazos de espera para configurar cada empresa asociada, al final de la relación con el distribuidor hay que desconectar su conexión. Se perdería la inversión en infraestructura.

2.2.2. Retos a los que se enfrenta la Empresa.

- Una creciente base de usuarios remotos.
- El alto coste de ampliar la infraestructura remota.
- La dificultad de incorporar y separar a los distribuidores externos de su infraestructura privada.

- Los requisitos de las comunicaciones cifradas.

Es por eso que se propone una red virtual privada (VPN) para resolver todos los problemas a la vez.

2.3. Solución VPN.

2.3.1. Elección de la mejor solución.

Tras analizar la situación, se identifican las aplicaciones, grupos, servicios y tecnologías a las que la VPN tiene que dar soporte: usuarios remotos, empresas asociadas distribuidoras, cifrado de enlaces y sesiones remotas y ciertos grupos internos (aquellos grupos internos que necesiten comunicaciones en red cerradas, por ejemplo consultores o departamentos).

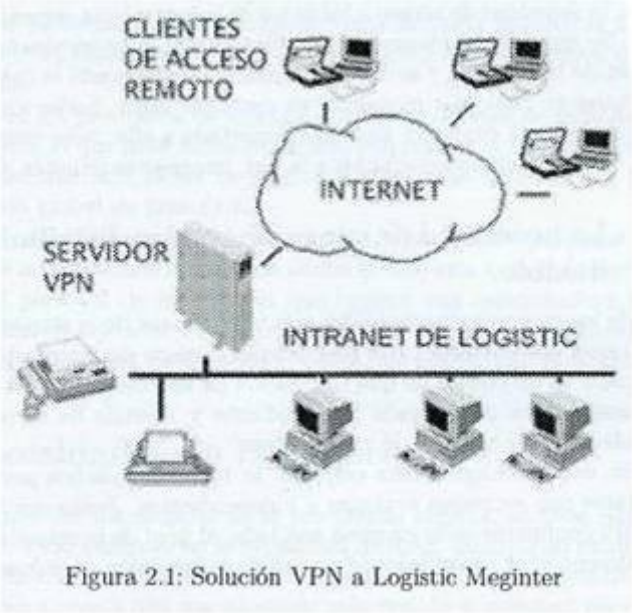

Figura 2.1: Solución VPN a Logistic Meginter

2.3.2. Ventajas que promete la Solución VPN.

- La eliminación de los módems y la conexión a través de ISP locales reducirá considerablemente la complejidad del acceso remoto.

- La migración a una solución basada en Internet reducirá los costes tanto del acceso a los números 800 como de la creación de una infraestructura privada adicional.

- Se pueden aprovisionar las conexiones de los distribuidores en cualquier momento y en cualquier lugar (la conexión y desconexión de distribuidores externos pasa a ser rápida y fácil. El ancho de banda puede controlar las aplicaciones que funcionan a través de la conexión VPN) y las VPN pueden funcionar a través de varios medios de transporte: analógico, RDSI, TI, línea digital de abonado (DSL) y módem cable.

2.3.3. Beneficios que obtiene Logistic Meginter de la VPN.

La estrategia de VPN de Logistic proporciona tremendos beneficios. La migración de una solución RAS a través de números 800 a una solución económica basada en ISP con túneles cifrados reducirá en un gran porcentaje el precio de la conectividad remota. La ampliación de la solución es infinitamente más sencilla, ya que utiliza un cliente por software y su conexión es neutral al medio, aceptando DSL, cable y acceso telefónico. El envío del software de cliente de VPN a través de la red significa que el acceso de los proveedores se realiza en un instante. Lo único que necesitan es una conexión a Internet.

Al finalizar su relación con el proveedor, Logistic puede desconectarle quitándole sus privilegios. Se acabaron las lentas conexiones con infraestructuras pesadas. La solución VPN proporciona a Logistic mayor agilidad que nunca. Desde el punto de vista de las auditorias, la solución VPN satisface sus necesidades de seguridad. Todas las sesiones tienen triple cifrado DES, con lo que la infraestructura de Logistic con total seguridad se puede llevar a los lugares más idóneos para satisfacer las necesidades de la empresa.

2.3.4. VPN es la mejor solución para las empresas encrecimiento.

Logistic Meginter es una empresa global en crecimiento y requiere mantener su ventaja sobre sus competidores, necesita soluciones flexibles y avanzadas para sus comunicaciones, y la solución VPN segura es una de ellas. Pero cualquier empresa, sin importar su tamaño, puede beneficiarse con una VPN.

Las razones que empujaron para adoptar dicha solución en ese sentido son, fundamentalmente de costes: resulta mucho más barato interconectar a los empleados utilizando una infraestructura pública que desplegar una red físicamente privada, también abaratará los costes en facturas telefónicas

debido a que las tarifas de conexión a Internet son sensiblemente más baratas que las de las llamadas directas sobre todo con las relacionadas con la telefonía móvil.

En los enlaces Cliente-Red que se crearán se encapsula PPP (Point To Point Protocol), Las tramas del cliente se encapsulan en PPP, y el PPP resultante se encapsula para crear el VPN. Este tipo de enlace nos proporciona un acceso seguro de un cliente a la red, con total movilidad y con independencia del Proveedor de Servicios de Internet (ISP) por el que se entre.

2.4. Pliego de Condiciones Técnicas.

Los equipos necesarios para la realización del proyecto tienen que cumplir como mínimo las especificaciones y características técnicas mencionadas. *Servidor.*

Tabla 2.1; Especificaciones y Características Técnicas del Servidor

Tipo de Procesador	Pentium IV
Número de procesadores	2
Caché L2	1 MB
Memoria	4096MB
Subsistema de disco	Integrated Dual Channel Ultra2 SCSI LVD, ServeRAID-4L Ultral60 SCSI Adapter, 54,6GB instalado
Tipo de disco duro	Ultral60 SCSI
Máximum storage capacity	218,4GB
Ranuras y bahías (totales/disponibles)	PCI 5(4) x 10(5)
CD-ROM	40X
Interfaz de red	Ethernet integrada
Monitor	19"

Ordenador Portátil

Tabla 2.2: Especificaciones y Características Técnicas del Cliente

Tipo de Procesador	Intel® Core(TM)2 Dúo Mobile
Memoria	1 GB
Capacidad del disco	80 GB
Monitor	13,3"
Soporte para PCMCIA	2 Tipo I/II ó 1 Tipo III
CD-ROM	U24X
Audio	Crystal Semiconductor CS4624/CS4297a
Velocidad del fax/módem	56K V.90 Integrado con Ethernet 10/100 (Intel)
Interfaz de red	Ethernet integrada
Sistema operativo instalado	Microsoft Windows 98 Second Edition

Capítulo 3

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 la red IP como Internet.

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 paquetes encapsulados pueden estar encriptadas o comprimidas o ambas cosas.

El PPTP supone la disponibilidad de la red IP entre los clientes PPTP y un servidor PPTP. Los cliente PPTP podrían estar ya conectados a una red IP por la que pueden tener acceso al servidor PPTP, o los clientes PPTP podrían 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 para la empresa 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).

La MPPE proporciona solamente la encriptación del enlace, pero no proporciona encriptación punto a punto. La encriptación punto a punto es la encriptación de datos entre la aplicación cliente y el servidor que contiene los recursos o servicios que son accesados por la aplicación cliente.

Para servidores PPTP sobre Internet, el servidor PPTP es un servidor VPN con PPTP con una interface con Internet y una segunda interface con la Red Local.

3.1. Mantenimiento del túnel con el control de conexión del PPTP.

El control de conexión del PPTP está entre las direcciones IP del cliente PPTP que utiliza un puerto TCP asignado dinámicamente y la dirección IP del servidor PPTP que utiliza el puerto TCP reservado 1723. El control de conexión PPTP lleva a cabo el control de la llamada del PPTP y la administración de mensajes que son utilizados para mantener el túnel PPTP.

Esto incluye la transmisión periódica de mensajes PPTP Echo-Request y PPTP Echo-Reply para detectar fallas en la conexión entre el cliente y el servidor PPTP. Los paquetes de control de conexión PPTP consisten de una cabecera IP, una cabecera TCP y un mensaje de control PPTP como se ilustra en la tabla 3.1. El paquete de control de conexión PPTP en la tabla 3.1 también incluye una cabecera de la capa de enlace de datos y una cola. [11]

Tabla 3.1: Paquete de control de conexión PPTP

Cabecera de enlace de datos	IP	TCP	Mensaje de control PPTP	Cola del enlace de datos

La tabla 3.2 lista los principales mensajes de control PPTP que son enviados sobre la conexión de control PPTP. Para todos los mensajes de control, el túnel PPTP específico es identificado por la conexión TCP.

Tabla 3.2: Mensajes de administración y control de llamada del PPTP

Tipo de mensaje	Propósito
Start-Control-Connection-Request	Enviado por el cliente PPTP para establecer la conexión de control. Cada túnel PPTP requiere que se establezca una conexión de control antes que pueda ser enviado cualquier otro mensaje PPTP.
Start-Control-Connection-Reply	Enviado por el servidor PPTP para responder al mensaje Start-Control-Connection-Request.
Outgoing-Call-Request	Enviado por el cliente para crear un túnel PPTP. Incluido en el mensaje Outgoing-Call-Request hay un identificador de llamada (Call-ID) que es utilizado en la cabecera GRE para identificar el tráfico de un túnel específico.
Outgoing-Call-Reply	Enviado por el servidor PPTP en respuesta al mensaje Outgoing-Call-Request.
Echo-Request	Enviado por el cliente PPTP o el servidor PPTP como un mecanismo para mantener la conexión. Si el Echo-Request no es respondido, el túnel PPTP eventualmente será terminado.
Echo-Reply	La respuesta a un Echo-Request.
WAN-Error-Notify	Enviado por el servidor PPTP por el servidor PPTP a todos los clientes VPN para indicar condiciones de error sobre la interface PPP del servidor PPTP.
Set-Link-Info	Enviado por el cliente PPTP o el servidor PPTP para establecer las opciones PPP negociadas.
CalI-Clear-equest	Enviado por el cliente PPTP indicando que el túnel será terminado.
Call- Disconnect-Notify	Enviado por el servidor PPTP en respuesta a un Call-Clear Request o por otras razones para indicar que un túnel será terminado. Si el servidor PPTP termina el túnel, se envía un CalI-Disconnect-Notify.
Stop-Control-Connection-Request	Enviado por el cliente PPTP o el servidor PPTP para informar al otro que la conexión de control será terminada.
Stop-Control-Connection-Reply	Utilizado para responder al mensaje Stop-Control-Connection-Request.

Códigos de error. Los códigos de error determinan si ocurrió un error en la conexión PPTP. En la tabla se muestran cuales pueden ser estos errores.

Tabla 3.3: Códigos de error en PPTP

Código	Nombre	Descripción
0	None	No hay error
1	Not-connected	Todavía no existe una conexión de control para este par PAC-PNS
2	Bad-Format	La longitud es errónea o el valor de la Magic Cookie es incorrecto
3	Bad-Value	Uno de los valor de algún campo esta fuera de rango o un campo reservado no esta en ceros
4	Not-Resource	Recursos insuficientes para manejar este comando
5	Bad-Call-ID	El identificador de llamada es incorrecto
6	PAC-Error	Un error especifico ocurrió en el PAC

3.1.1. Túneles en PPTP.

PPTP requiere del establecimiento de un túnel para la comunicación entre una pareja PAC-PNS. Los datos de usuario que transporta PPTP son tramas PPP, las cuales son encapsuladas utilizando GRE. El túnel es utilizado para transportar todas las tramas PPP que pertenecen a una sesión entre una pareja PAC-PNS. Una clave presente en la cabecera GRE indica a cual sesión pertenece una determinada trama PPP. De esta manera, las tramas PPP son transportadas por rutas distintas pero dentro de un único túnel. El proceso de ensamblado de un paquete PPTP al momento de ser transmitido se muestra en la figura 3.1

Como se puede observar en la figura 3.1, el cliente crea los datos a enviar a los cuales se les asigna una dirección IP privada. Posteriormente, el software PPTP utiliza la cabecera GRE mejorada para permitir el transporte de la cabecera PPP privada y además encapsular el paquete dentro de otra cabecera IP la cual es Pública. Finalmente, el controlador PPP añade la cabecera PPP pública la cual permitirá al paquete viajar al otro extremo del túnel. Tratándose de una VPN, la información debe ser cifrada para evitar que sea utilizada por usuarios no autorizados.

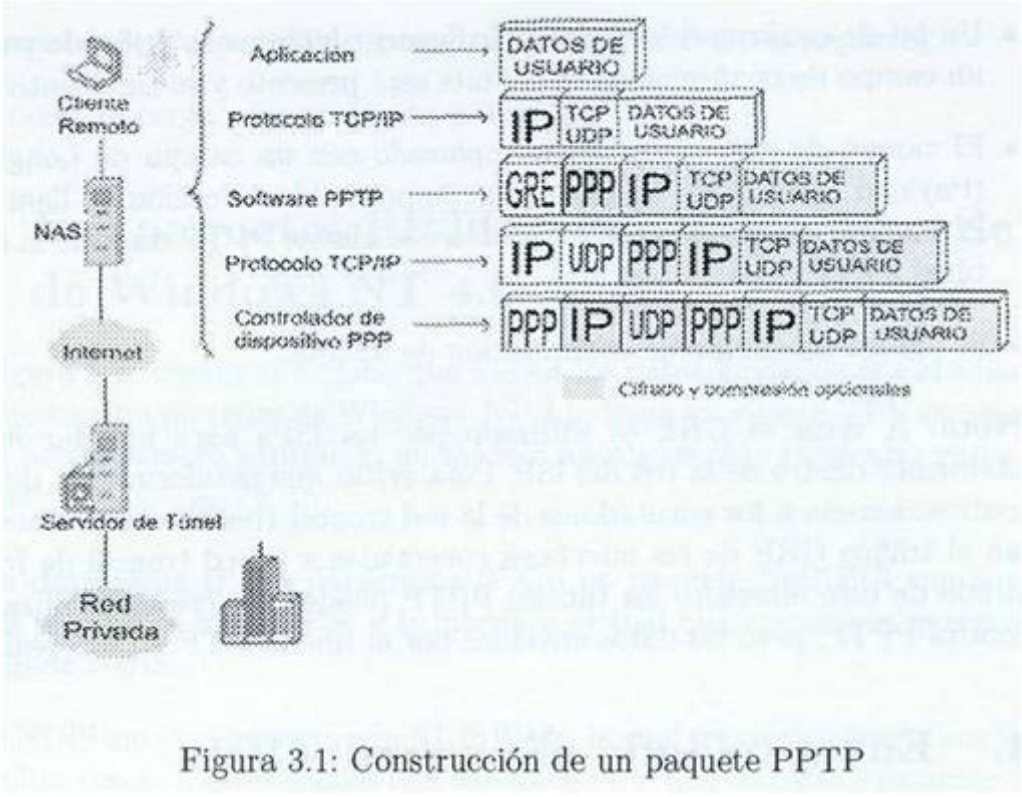

Figura 3.1: Construcción de un paquete PPTP

3.2. Envío de datos con PPTP.

El envío de datos con PPTP se logra con múltiples niveles de Encapsulación. La tabla 3.4. Muestra la estructura resultante de los datos enviados por el túnel de PPTP.

Tabla 3.4: Datos del túnel PPTP

Cabecera de enlace de datos	Cabecera IP	Cabecera GRE	Cabecera PPP	Cola del enlace de datos

3.3. Encapsulación del paquete PPP.

La carga inicial PPP es encriptada y comprimida con una cabecera PPP para crear un paquete (frame) PPP. El paquete PPP es luego encapsulado con una cabecera GRE modificada. 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.

Para PPTP, la cabecera GRE es modificada de la siguiente manera:

- Un bit de confirmación (acknow ledgement bit) que es utilizado para indicar que un campo de confirmación de 32 bits está presente y es significativo.

- El campo de clave (key) es reemplazado con un campo de Longitud de Carga (Payload Length) de 16 bits y un campo de identificación de llamada (Call ID). El campo de identificación lo establece el cliente PPTP durante la creación de un túnel PPTP.

- Se agrega un campo de confirmación de 32 bits.

Nota: A veces el GRE es utilizado por los ISPs para mandar información de enrutamiento dentro de la red del ISP. Para evitar que la información de enrutamiento sea re direccionada a los enrutadores de la red troncal (backbone) de Internet, los ISPs filtran el trafico GRE de las interfaces conectadas a la red troncal de Internet. Como resultado de este filtrado, los túneles PPTP pueden ser creados utilizando mensajes de control PPTP, pero los datos enviados por el túnel PPTP no son re direccionados.

3.4. Encapsulando el paquete GRE.

La carga resultante encapsulada por PPP y GRE es luego encapsulada con una cabecera IP conteniendo las direcciones IP destino y origen apropiados para el cliente y el servidor PPTP.

3.4.1. Encapsulación en la capa del enlace de datos.

Para ser enviado por un enlace LAN o WAN, el datagrama IP es encapsulado con una cabecera y una cola de acuerdo a la tecnología de la capa del enlace de datos (data-link layer) de la interface física del emisor. Por ejemplo, cuando los datagramas IP son enviados en una interface Ethernet, el datagrama IP es encapsulado con una cabecera y una cola Ethernet. Cuando los datagramas IP son enviados sobre un enlace WAN punto a punto, tal como una línea telefónica analógica o ISDN, el datagrama IP es encapsulado con una cabecera y una cola PPP.

3.5. Procesamiento de los datos enviados con PPTP.

Al recibir los datos enviados por el túnel PPTP, el cliente o el servidor PPTP:

1. Procesa y elimina la cabecera y la cola del enlace de datos.

2. Procesa y elimina la cabecera IP.

3. Procesa y elimina las cabeceras GRE y PPP.

4. Desencripta, descomprime, o ambas la carga PPP (si se requiere).

5. Procesa la carga para recepción o reenvío.

3.6. Los paquetes PPTP y la arquitectura de redes de Windows NT 4.0

La figura 3.2. ilustra el camino que toman los datos enviados por el túnel a través de la arquitectura de redes de Windows NT 4.0 desde un cliente VPN en una conexión VPN de acceso remoto utilizando un módem analógico. Los siguientes pasos describen el proceso:

1. Un datagrama IP, un datagrama IPX o un paquete NetBEUI son enviados por sus protocolos apropiados a la interface virtual que representa la conexión VPN usando NDIS.
2. El NDIS envía el paquete a la NDISWAN, la cual en cripta o comprime los datos, o ambas cosas, y proporciona una cabecera PPP que consiste solamente del campo de Identificación de Protocolo PPP (PPP Protocol ID). No se agregan los campos de banderas (Flags) o de Verificación de Secuencia de Paquetes (Frame Check Sequence, FCS). Esto supone que la dirección y la compresión de los campos de control fueron negociadas durante la fase del Protocolo de Control de Enlace (Link Control Protocol, LCP) del proceso de conexión PPP.
3. El NDISWAN envía los datos al controlador del protocolo PPTP, el cual encapsula el paquete PPP con una cabecera GRE. En la cabecera GRE, el identificador de llamada (Call-ID) se establece al valor apropiado para identificar el túnel.
4. El controlador del protocolo PPTP envía el paquete resultante al controlador del protocolo TCP/IP.
5. El controlador del protocolo TCP/IP encapsula los datos enviados por el túnel PPTP con una cabecera IP y envía el paquete resultante a la interface que representa la conexión de acceso telefónico al ISP local usando NDIS.
6. El NDIS envía el paquete resultante al NDISWAN, que proporciona las cabeceras y las colas PPP.
7. El NDISWAN envía el paquete PPP resultante al controlador WAN apropiado que representa el hardware del acceso telefónico (por ejemplo, el puerto asíncrono de una conexión por módem).[8] [12]

[8] www.microsoft.com/

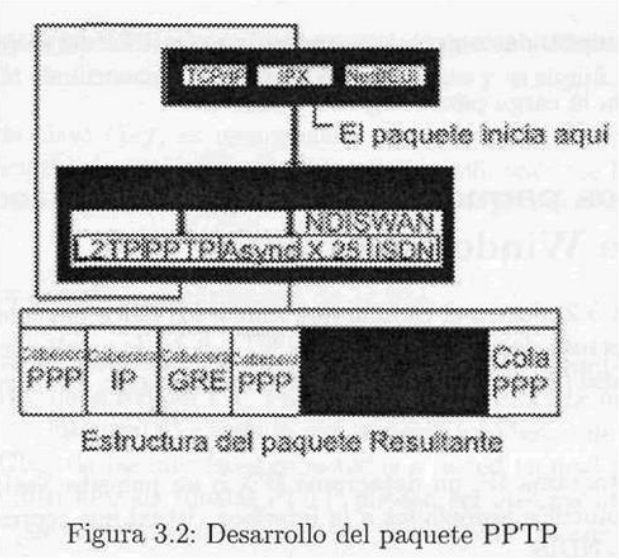

Figura 3.2: Desarrollo del paquete PPTP

Capítulo 4

Seguridad y Direccionamiento para la VPN de Logistic Meginter.

Seguridad para la VPN.

4.1. Necesidad de seguridad en una VPN

Cuando se diseñaron los primeros protocolos para redes, la seguridad no era un punto importante puesto que las redes sólo eran utilizadas por universidades e investigadores. Nadie pensaba en que alguien pudiera interceptar mensajes. Sin embargo, conforme las redes pasaron a tener un propósito comercial cuando las empresas las adoptaron y con la llegada de Internet, la seguridad pasó a ser una cuestión de vital importancia al momento de implementar redes.

Con la llegada de Internet, cualquier computadora conectada es susceptible de ser atacada por personas que no deben ingresar a ellas. Los ataques a redes provocan muchas pérdidas económicas a las empresas. Según una encuesta del Computer Security Institute (CSI), el 70 % de las organizaciones encuestadas declararon que sus redes habían sido atacadas y el 60 % afirmaba que los incidentes procedían de las propias empresas. Por lo tanto, es necesario tomar las medidas necesarias para proteger la VPN de Logistic Meginter.

La seguridad cobra especial importancia al momento de la implementación de la VPN a la empresa puesto que la información privada de la organización atraviesa una red pública, es necesario proveer a la VPN de mecanismos que aseguren la confidencialidad y la integridad de los datos transmitidos y también para evitar el acceso a la red privada.

La seguridad de la VPN debe ir más allá que simplemente controlar el acceso seguro a los recursos de la red. también debe proveer mecanismos para administrar la implementación de pólizas de seguridad que garanticen el desarrollo exitoso de la VPN. La mejor opción es establecer también, antes de que se establezca la conexión cifrada con una oficina o LAN remota, unos niveles de seguridad que deben cumplirse. La comprobación de los niveles de seguridad que deben cumplir los equipo remotos que se deseen conectar a Logistic debe ser lo mas amplia posible.

Sin duda, es necesario establecer un sistema de chequeo del status de seguridad de los equipos remotos conectados mediante VPN a la red corporativa. Y el chequeo debe ser percibido por el usuario remoto como una ayuda a la seguridad general, no como una imposición corporativa y además, debe hacerse con suficiente amplitud como para abarcar productos y sistemas de seguridad no corporativos, sino elegidos por el tele trabajador en su ámbito doméstico.

La autenticación de usuarios y encriptación de datos son características de seguridad muy fuertes. Y en la VPN que se implantara en Logistic la tecnología que es elegida es IPSec.[9] [13]

4.2. IPSec

IPSec, garantiza la privacidad e integridad de los datos que viajan por la red pública. también permite la autenticación de los extremos de la comunicación. El uso de VPN trae consigo innumerables ventajas, pero también trae innumerables riesgos. Hay que tener en cuenta que el empleo de la VPN a Logistic implica abrir las puertas de nuestra red a un amplio rango de usuarios, usuarios que ni siquiera podemos ver, e incluso ni conocemos. Además, estos usuarios están accediendo a datos sensibles de la empresa que deben estar protegidos. Un uso erróneo de la VPN puede ser catastrófico para el la empresa.

Sin embargo, asegurando quien está accediendo a nuestra red y controlando desde dónde está accediendo, la VPN se convierte en una potente herramienta para la empresa. Planteando un escenario básico de la VPN basada en IPSec, podemos añadir mejoras para conseguir una VPN segura.

4.3. Escenario de partida.

La forma más sencilla e inmediata de abordar la implantación de la VPN con IPSec es utilizar un equipo en la sede central que concentre los túneles que provengan de usuarios y oficinas remotos y terceras empresas. Los túneles en los extremos remotos pueden ser generados por diversos dispositivos: clientes VPN, cortafuegos (firewalls), routers, etc.

IPSec permite utilizar, como método de autenticación de los extremos del túnel, las claves pre compartidas. En un escenario a gran escala o en el que no se tenga un canal seguro, la distribución y renovación de estas claves se convierte en un enorme problema. Este método no es recomendable, y por tanto, es necesario adoptar otra solución para realizar la autenticación de los extremos del túnel.

Certificados digitales e Infraestructura de Clave pública (PKI). La primera mejora es aprovechar la capacidad que tiene IPSec de autenticar los extremos de la comunicación mediante certificados digitales. El uso de certificados digitales elimina el problema de la distribución de claves, ya que un certificado digital, al ser publico, puede ser distribuido por un canal inseguro.

[9] www.cisco.com/

Implantar un sistema PKI para emitir los certificados digitales nos permite tener el control absoluto de la emisión, renovación y revocación de los certificados digitales usados en la VPN. Las siglas PKI infunden una idea de extrema complejidad que tiempo atrás era justificable, pero actualmente existen en el mercado productos sencillos y seguros que facilitan enormemente su uso. A demás, su utilización no se limita sólo a las VPNs sino que la misma infraestructura puede utilizarse para aplicaciones como cifrado de correo electrónico, firma digital, etc.

Autenticación fuerte. Con el uso de certificados digitales, se garantiza la autenticación de los elementos remotos que generan el túnel, pero ¿qué ocurre en el caso de los usuarios remotos? ¿Realmente se esta autenticando a los usuarios?

Esta pregunta tiene dos respuestas, dependiendo de dónde se almacene el certificado digital y la clave privada:

1. Si el certificado digital y la clave privada se almacenan, protegidos por un PIN, en una tarjeta inteligente que el usuario lleva consigo, la respuesta es que sí estamos autenticando al usuario.

   Actualmente existen en el mercado Clientes IPSec compatibles con el estándar PKCS#11 que permiten la lectura de tarjeta inteligente para obtener el certificado digital y la clave privada. Desafortunadamente, aún no existe un estándar definido que permita la implantación a gran escala de lectores de tarjetas en los PCs. Por lo tanto, esta opción en algunos casos no es abordable.

2. Si, por el contrario, el certificado digital y la clave privada se almacenan en el propio PC, la respuesta es que no estamos autenticando al usuario, sino al PC. Para autenticar al usuario, algunos fabricantes de sistemas VPN han añadido un segundo nivel de autenticación.

   El uso de passwords es un nivel adicional de seguridad, pero no es el mas adecuado, ya que carecen de los niveles de seguridad necesarios en este tipo de entorno: son fácilmente reproducibles, pueden ser capturadas y realmente no autentican a la persona, ya que la autenticación se basa en un solo factor (lo que uno sabe).

   La forma mas adecuada de autenticar a los usuarios remotos, a falta de tarjetas inteligentes, es el uso de sistemas de autenticación fuerte. Estos sistemas se basan en la combinación de dos factores, lo que uno tiene (una token) y lo que uno sabe (un PIN). De esta forma nos aseguramos completamente de que sólo las personas autorizadas acceden a nuestra VPN.

Autorización y control de acceso. Una vez que se sabe a ciencia cierta quien está al otro lado del túnel, mediante el uso de certificados digitales y de sistemas de autenticación fuerte, se debe abordar el siguiente aspecto para securizar la VPN: controlar dónde están accediendo las oficinas y usuarios remotos; y lo que es aún más crítico: controlar dónde están accediendo las empresas con las que se forma una extranet mediante nuestra VPN.

Este control de acceso se podrá realizar utilizando sistemas de control de acceso o firewalls, y sistemas de autorización. De esta manera se aplicarán políticas de acceso a determinados sistemas en función de usuarios o grupos de usuarios, asegurando así, por ejemplo, que terceras empresas sólo acceden a aquellos sistemas o aplicaciones estrictamente necesarios.

Direccionamiento par la VPN en Logistic Meginter.

Para comprender como funcionan la VPN, se debe entender como es afectado el direccionamiento (addressing) y el enrutamiento (routing) para la creación de VPNs de acceso remoto y de VPNs de enrutador a enrutador. La VPN crea una interface virtual que debe de ser asignada a una dirección IP apropiada y se deben de cambiar o agregar rutas para asegurar que el trafico apropiado sea enviado a través de la conexión VPN segura, en lugar de ser enviado por la red de transito pública o compartida.

4.4. Conexión VPN de acceso remoto.

Para la conexión VPN de acceso remoto, una computadora crea una conexión de acceso remoto a un servidor VPN. Durante el proceso de conexión se asigna una dirección IP al cliente y modifica la ruta por defecto para que el tráfico de la ruta por defecto sea enviado sobre la interface virtual.

4.5. Direcciones IP y el cliente VPN de acceso telefónico.

Para los 25 clientes VPN de Logistic de acceso telefónico que se conectan a Internet antes de crear la conexión VPN con un servidor VPN en Internet, dos direcciones IP son asignadas:

- Cuando se crea la conexión PPP, la negociación con el IPCP y el NAS del ISP asigna una dirección IP pública.
- Cuando se crea la conexión VPN, la negociación con el servidor VPN se asigna una dirección IP de la intranet.

En cualquier caso, la dirección IP asignada al cliente debe estar accesible por los servidores de la red de la empresa.

Los datos enviados por el túnel y a través de la VPN son direccionados desde la dirección del cliente asignada por el servidor hasta la dirección de la intranet. La cabecera IP mas externa es direccionada entre la dirección IP del cliente asignada por el ISP y la dirección pública del servidor. Debido a que los enrutadores en Internet solamente procesan la cabecera IP más externa, los enrutadores de Internet dirigirán los datos del túnel a la dirección IP pública del servidor.

Un ejemplo del direccionamiento de un cliente de acceso telefónico se muestra en la figura 4.1, donde la organización utiliza direcciones privadas en la red local y los datos enviados por el túnel están dentro de un datagrama IP.[10] [7]

[10] Redes Privadas Virtuales de Cisco Secure

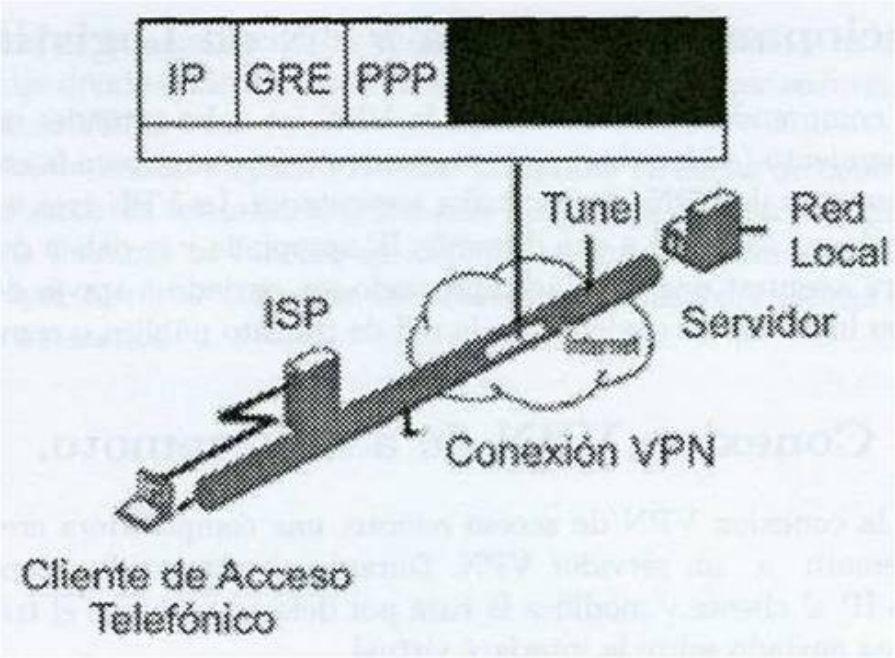

Figura 4.1:

Direccionamiento publico y privado en los datos del túnel PPTP.

4.6. Rutas por defecto y los clientes de acceso telefónico.

Cuando un cliente llama al ISP, recibe una dirección IP pública del NAS del ISP. No se asigna la dirección de un gateway por defecto como parte del proceso de negociación IPCP. Por lo tanto, para accesar todas las direcciones de Internet, el cliente agrega una ruta por defecto a su tabla de enrutamiento utilizando la interface conectada al ISP. Como resultado de esto, el cliente puede redirigir los datagramas IP al NAS del ISP desde donde son enrutados a su localización en Internet.

4.7. Rutas por defecto y las VPN sobre Internet.

Cuando el cliente de acceso telefónico llama al ISP, agrega una ruta por defecto utilizando la conexión al ISP como se muestra en la figura 4.2. En este punto, puede accesar todas las direcciones de Internet a través del enrutador en el NAS del ISP.

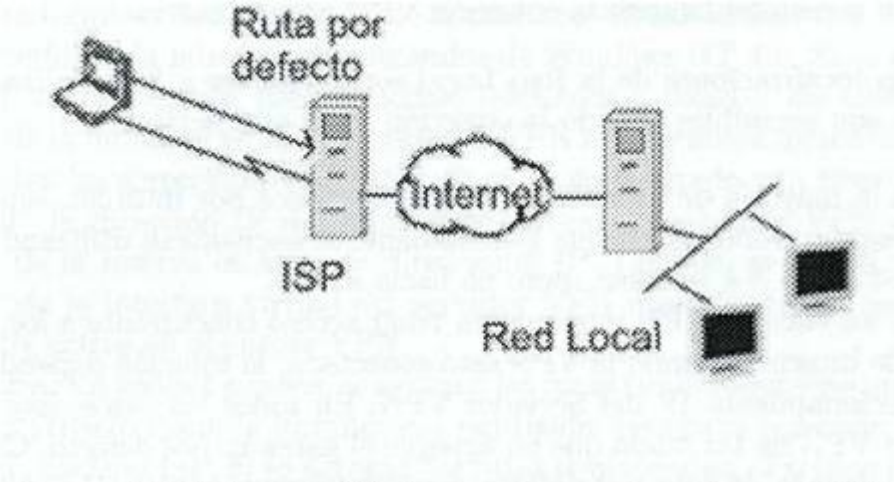

Figura 4.2: Ruta por defecto creada cuando se llama al ISP.

Una vez que el cliente VPN crea la conexión VPN, se agrega otra ruta por defecto y una ruta al servidor hacia la dirección IP del servidor del túnel, como se ilustra en la figura 4.3. La ruta por defecto previa es grabada pero ahora tiene una métrica superior. EI agregar la nueva ruta por defecto significa que todas las direcciones de las localizaciones de Internet, excepto la dirección IP del servidor del túnel, no estarán accesibles mientras dure la conexión VPN.

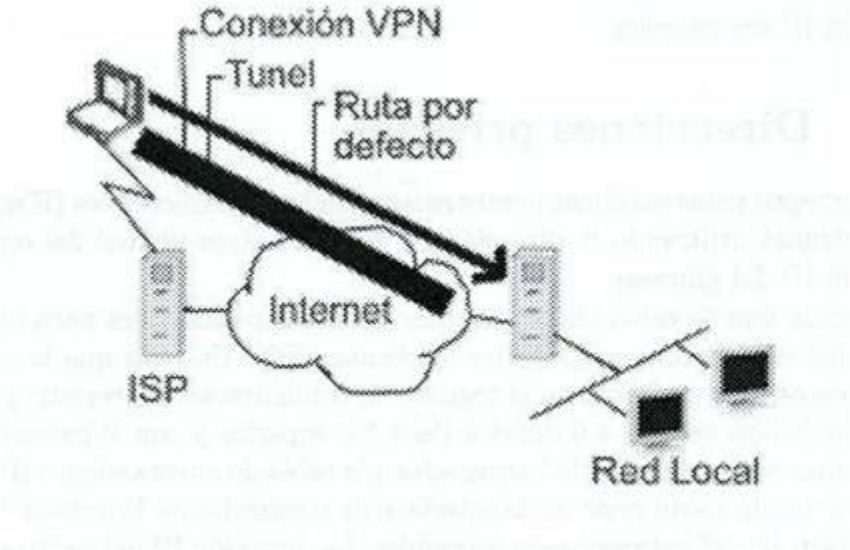

Figura 4.3: Ruta por defecto creada cuando se inicia la VPN.

Tal como en el caso de un cliente de acceso telefónico a Internet, cuando un cliente VPN de acceso telefónico que usa creación voluntaria de túneles crea una conexión VPN a un servidor VPN de la Red Local a través de Internet, una de las siguientes cosas ocurre:

- Las localizaciones de Internet son accesibles y las localizaciones de la red local no son accesibles cuando la conexión VPN no está activa.
- Las localizaciones de la Red Local son accesibles y las localizaciones de Internet no son accesibles cuando la conexión VPN está activa.

Para la mayoría de los clientes VPN conectados por Internet, este comportamiento no representa problema porque generalmente se encuentran utilizando la comunicación de la Red Local o a Internet, pero no hacia ambas.

Para los clientes VPN que quieren tener acceso concurrente a los recursos de la red local y de Internet cuando la VPN está conectada, la solución depende de la naturaleza del direccionamiento IP del Servidor VPN. En todos los casos, hay que configurar la conexión VPN de tal modo que no agregue el gateway por defecto. Cuando la conexión VPN sea creada, la ruta por defecto persistirá apuntando al NAS del ISP, permitiendo el acceso a todas las direcciones de Internet.

Dependiendo del tipo de direccionamiento que se use en la intranet, se habilita el acceso concurrente a los recursos de la intranet y de Internet de la manera siguiente:

4.8. Direcciones públicas.

Se agregan rutas estáticas persistentes para los identificadores (IDe) de la red pública de la intranet utilizando la dirección IP de la interface virtual del servidor VPN como dirección IP del gateway.

4.9. Direcciones privadas.

Se agregan rutas estáticas persistentes para los identificadores (IDs) de la red privada de la intranet utilizando la dirección IP de la interface virtual del servidor VPN como dirección IP del gateway.

En cada uno de estos casos, las rutas estáticas persistentes para los IDs de la red de la intranet necesitan ser agregadas al cliente VPN. Una vez que las rutas persistentes sean agregadas se grabaran en el registro de configuraciones (registry). Con Microsoft Windows NT; versión 4.0 Service Pack 3 o superior y con Windows NT 4.0 las rutas persistentes no son en realidad agregadas a la tabla de enrutamiento IP (y no son visibles con el comando route print en la interface de comandos de Windows NT 4.0) hasta que la dirección IP del gateway sean accesibles. La dirección IP del gateway estará accesible cuando se haga la conexión VPN.

Para cada ruta, invoque a la utilidad route con la siguiente sintaxis en la interface de comandos de Windows NT 4.0: ROUTE ADD <ID de Red de la Intranet>MASK <Mascara de Red><dirección IP de la interface virtual del servidor VPN>-p.

La dirección IP del gateway en el comando route de cada ruta a la intranet es la dirección IP asignada a la interface virtual del servidor, no la dirección IP de la interface del servidor VPN a Internet.

Se puede determinar la dirección IP de la interface virtual del servidor VPN usando el comando ipconfig en la interface de comandos de Windows NT 4.0. Si se utiliza DHCP para obtener las direcciones para el acceso telefónico a redes y los clientes VPN, la dirección IP de la interface virtual del servidor VPN es la primera dirección IP obtenida cuando se piden las direcciones de DHCP. Si se ha configurado una reserva estática de direcciones IP, la dirección IP de la interface virtual del servidor VPN es la primera dirección IP de la reserva estática de direcciones IP. También se puede determinar la dirección IP de la interface virtual del servidor VPN observando los detalles de una conexión VPN activa en el cliente VPN.

Advertencia: En todos los casos, se agregan las rutas cuidadosamente para asegurarse que el tráfico privado hacia la intranet sea redirigido usando la conexión VPN y no la conexión PPP hacia el ISP. Si se agregan las rutas equivocadas, el trafico que se intenta redirigir a través de la VPN en forma encriptada será enviada en forma no encriptada a través de Internet, Por ejemplo, si en la red local se está utilizando el ID de red pública 207.46.1 30.0 (mascara de subred 255.255.255.0) y por error se agrega una ruta estática persistente para 207.46.131.0, todo el trafico a la red local en 207.46.130.0 será redirigido a través de Internet en forma no encriptada, en lugar de ser encriptada y enviada a través de la conexión VPN. [13]

Capítulo 5

Resolución de problemas de las VPNs.

Para resolver los problemas de las VPNs, se debe resolver problemas de conectividad IP, del establecimiento de la conexión de acceso remoto y del enrutamiento.

5.1. Problemas comunes de las VPNs.

Los problemas con las VPN generalmente caben dentro de las siguientes categorías:

- El intento de conexión es rechazado cuando debería de ser aceptado.
- No se pueden accesar localizaciones más allá del servidor VPN.
- No se puede establecer un túnel.

Utilizar los siguientes consejos de resolución de problemas para aislar el problema de configuración o de infraestructura que está causando el problema en la VPN.[11] [10]

5.2. El intento de conexión es rechazado cuando debería ser aceptado.

Usando el comando ping, verificar que el nombre del servidor o la dirección IP del servidor VPN es accesible. Si se está usando el nombre del servidor, verifique que el nombre del servidor es convertido a su dirección IP correcta. Si el comando ping no tiene éxito, el filtreado de paquetes del Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol, ICMP) podría estar evitando el paso de los mensaje ICMP hacia y desde el servidor VPN.

[11] www.cisco.com/global/ES/solutions

- Verificar que el Servicio de Acceso Remoto o el Servicio de Acceso Remoto y Enrutamiento estén siendo ejecutados en el servidor VPN.
- Verificar que todos los puertos PPTP en el servidor VPN no estén ya siendo utilizados. Si es necesario, configurar las propiedades del Protocolo de túnel Punto a Punto en Control Panel-Network y cambie el número de Puertos PPTP para permitir más conexiones concurrentes.
- Verificar que el cliente VPN y el servidor VPN estén configurados para usar parámetros de autentificación comunes.
- Verificar que el cliente VPN y el servidor VPN estén configurados con parámetros de encriptación comunes.
- Verificar que los protocolos de la LAN que estén siendo usados por los clientes estén habilitados para acceso remoto.
- Verificar que las credenciales de los clientes que consisten de nombre de usuario, clave y nombre del dominio estén correctas y puedan ser validadas por el servidor VPN.
- Verificar que la cuenta de usuario correspondiente a las credenciales del usuario del cliente VPN tenga permiso de acceso telefónico.
- Verificar la configuración del agente de autentificación. Un servidor VPN con RRAS puede ser configurado para utilizar a Windows NT 4,0 o a RADIUS para autentificar las credenciales del cliente de acceso remoto.
- Para conexiones VPN de acceso remoto, verifique que los puertos PPTP estén configurados para recibir llamadas.

5.3. No se puede establecer un túnel.

- Verificar que el filtrado de paquetes en la interface de algún enrutador entre el cliente y el servidor VPN no esté evitando la redirección de tráfico del protocolo de túnel. En un servidor VPN con Windows NT 4.0, el filtrado de paquetes IP puede configurarse desde las propiedades avanzadas TCP/IP y desde la herramienta Administrador de RAS y Enrutamiento (Routing and RAS Admin). Revisar ambas cosas en busca de filtros que podrían estar excluyendo el tráfico de la VPN
- Verificar que el cliente Windows Proxy no esté ejecutándose actualmente en el cliente VPN. Cuando el cliente Windows Proxy está activo, las llamadas al API de WinSocks que son utilizadas para crear túneles y enviar datos por el túnel son interceptadas y redirigidas al servidor proxy configurado. Una computadora común servidor proxy permite a la organización accesar tipos

específicos de recursos de Internet (generalmente Web y FTP) sin conectar directamente a esa organización a Internet.

La organización puede utilizar identificadores de red IP privadas asignadas por InterNIC (tales como 10.0.0.0). Los servidores proxy son generalmente utilizados para que los usuarios privados puedan tener acceso a recursos públicos en Internet como si estuvieran directamente conectados a Internet. Las conexiones VPN son utilizadas generalmente para que usuarios autorizados en Internet tengan acceso a los recursos privados de la organización. Una sola computadora puede actuar como servidor proxy (para los usuarios privados) y servidor VPN (para los usuarios autorizados en Internet) para facilitar ambos intercambios de información.[12] [14]

5.4. Herramientas para resolución de problemas.

Las siguientes herramientas con las que puede recolectar información adicional acerca de la causa de su problema con la VPN, están incluidas con Windows NT 40.

5.4.1. Monitor de Red.

Use el Monitor de Red (Network Monitor) una herramienta de captura y análisis de paquetes, para ver el tráfico enviado entre un servidor y un cliente VNP durante el proceso de conexión VPN y durante la transferencia de datos. No es posible interpretar las porciones encriptadas del trafico VPN con el Monitor de Red.

La interpretación correcta del tráfico de acceso remoto y de la VPN con el Monitor de Red requiere una profunda comprensión de PPP, PPTP y otros protocolos.

5.4.2. Registro y rastreo PPP.

El registro PPP (PPP log) o el rastreo PPP (PPP tracing) registran la secuencia de las funciones de programación invocadas durante un proceso, ya sea a una ventana de consola o a un archivo. Habilite el registro PPP o el rastreo PPP para los componentes de acceso remoto e intente la conexión de nuevo. Después de ver la información rastreada, reinicie los parámetros de rastreo a sus valores por defecto. [12]

[12] www.es.wikipedia.org

Capítulo 6

Instalación, configuración y puesta a punto de una conexión VPN.

6.1. Conceptos Básicos

- PPTP usa una implementación de RAS de Microsoft y el PPP (Protocolo Punto a Punto) para establecer las conexiones con computadoras remotas usando líneas telefónicas automáticas (DIAL-UP), redes Ethernet o redes Token Ring. PPP proporciona autentificación a usuarios-remotos y encriptamiento de datos entre PPTP cliente y el PPTP servidor. así, para usar PPTP se deberá instalar y configurar un RAS con redes de trabajo con líneas automáticas y ambos PPTP clientes y PPTP servidores.
- Porque PPTP requiere un RAS y un protocolo PPP, se deberá establecer una cuenta PPP con el ISP (proveedor de servicios de Internet) para usar PPTP con cada una de las conexiones ISP para Internet.
- PPTP usa un dispositivo virtual llamado VPN. Cuando se configura un PPTP, instala y configura VPN en RAS tal como si estos fueran dispositivos físicos, tal como lo son los módems.
- PPTP se instala y se configura únicamente con PPTP clientes y PPTP servidores.
- Para mantener la seguridad de la red de la empresa, PPTP clientes deberá ser autentificado (tal como algún otro usuario remoto que este usando un RAS y una red de trabajo por línea automática) en orden para conectarse a la red privada de la empresa.
- Usar el Internet para establecer una conexión entre un PPTP cliente y un PPTP servidor, significa que el PPTP servidor deberá tener un valor, sancionando por medio de Internet las direcciones IP. Sin embargo, los paquetes de encapsulamiento IPX, NetBEUI, o TCP/IP, se envían entre el cliente PPTP y el servidor PPTP,

que pueden ser direccionados a computadoras sobre la red privada de la empresa usando direccionamientos de red o esquemas de nombramiento. El servidor PPTP desarma el paquete PPTP desde un cliente PPTP y traspasa el paquete a la computadora correcta sobre la red privada.

6.2. Instalación y configuración de PPTP sobre un servidor.

PPTP es instalado sobre una base de servidor Windows NT como un protocolo de red, usando el apartado de Protocolos en la opción de red del Panel de Control. Tú puedes adicionar, configurar y eliminar PPTP usando el apartado de Protocolos.

En esta sección se explica como instalar y configurar el protocolo PPTP sobre un servidor PPTP, de lo que asumimos lo siguiente:

- El servidor Windows NT, deberá tener instalada la versión 4,0.
- Uno o más adaptadores de red instalados. En muchos casos, dos o más adaptadores de red son requeridos: uno para conectarse a Internet y uno o más para conectarse a la red de la empresa.
- El TCP/IP deberá estar instalado y conectado dentro del adaptador de red hacia la red privada de la empresa, y el adaptador conectado a Internet.
- El protocolo de red usado en la red privada de la empresa, (TCP/IP, NetBEUI, o IPX) debe estar instalado y cargado al adaptador(es) conectados hacia la red privada de la empresa.
- El servidor PPTP estará configurado con una dirección IP estática.
- RAS, con llamada automática (dial-up) de red, estará instalada y configurada.
- El número de conexiones simultáneas con clientes PPTP remotos que prestara el servidor PPTP, por lo tanto se deberá configurar el número correcto de dispositivos VPN.

6.3. Configuración de una computadora con Windows NT versión 4.0 como un servidor PPTP.

Implica tres procedimientos principales:

1. Instalar el PPTP y posteriormente seleccionar el número de dispositivos VPN.
2. Adicionar los dispositivos VPN tal como puertos RAS y dispositivos.
3. Configurar las opciones de encriptamiento y autentificación.

6.3.1. Instalación de PPTP sobre un servidor PPTP.

Para instalar el protocolo PPTP en una computadora trabajando con Windows NT Server versión 4.0.

- Clic **Inicio**, en el punto de **configuración**, y clic en el **Panel de Control**.
- Doble clic en **Red** dentro de **Panel de Control**.
- Clic en la opción de **Protocolos**, y clic en **Adicionar** para desplegar el Protocolo de red seleccionado en la caja de dialogo. El cuadro de dialogo del **Protocolo de Red** Seleccionado se ilustra en la figura 6.1:

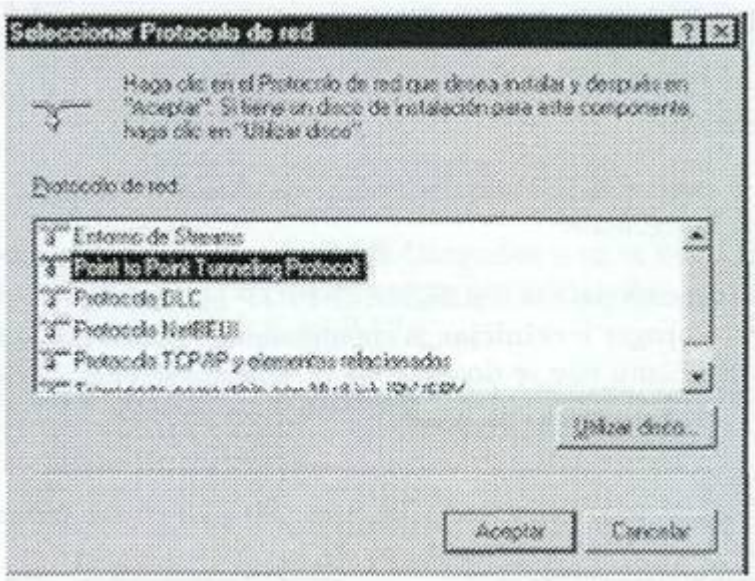

Figura 6.1: Seleccionar Protocolo de Red

- Seleccionar la opción de **Protocolo Punto por Punto** y hacer clic en **Aceptar.**

- Escribir el drive y la ubicación del directorio de los archivos de instalación de tu Servidor Windows NT versión 4.0 en el **Setup de Windows NT** en el cuadro de dialogo, y posteriormente hacer clic en **Continuar**. Los archivos del PPTP serian copiados desde el directorio de instalación, y aparecerla el cuadro de dialogo de configuración de PPTP, tal como se muestra en la figura 6.2:

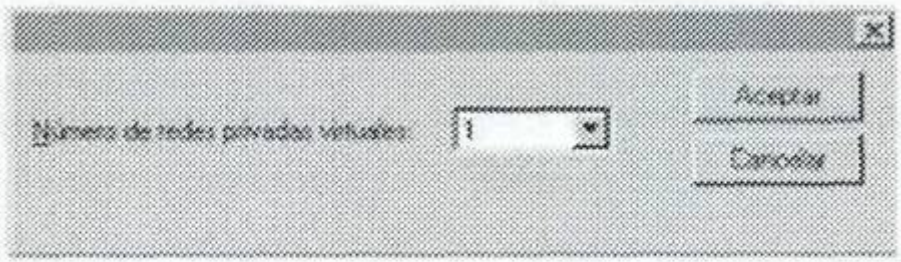

Figura 6.2: Selección de número de VPNs

- Hacer clic en la flecha del **número de Red Privada Virtual**, para seleccionar el número de VPNs simultáneas que se desee que soporte el servidor. Se puede seleccionar un número entre un rango de 1 y 256. Las VPNs múltiples son instaladas en un servidor PPTP para habilitar los clientes múltiples que se conectan simultáneamente al servidor PPTP. El servidor puede ser configurado para soportar como un número máximo de 256 simultaneas conexiones VPN.

- Hacer clic en **Aceptar**, y otra vez en **Aceptar** en el cuadro de dialogo de **Setup Message**.

- En el cuadro de dialogo del **Setup de Acceso Remoto**, se podría hacer más tarde lo siguiente:

a) Temporalmente para la instalación de PPTP haciendo clic en **Cancelar**, cerrando **Red**, y apagar o **reiniciar** la computadora. Nótese que se deberá ejecutar el procedimiento que se describe en la siguiente sección adicionar los Dispositivos VPN tal como los puertos RAS sobre un servidor PPTP, para completar la instalación de PPTP.

b) Continuar la instalación de PPTP haciendo clic en **Adicionar** para adicionar los dispositivos VPN instalados con PPTP para RAS. (Ver el paso 5 del siguiente procedimiento).

6.3.2 Adicionar un dispositivo VPN como puerto RAS sobre un servidor PPTP.

Antes de instalar PPTP, se deberá adicionar un dispositivo VPN al RAS. Siguiendo estos pasos para adicionar dispositivos VPN en una computadora corriendo con Windows NT Server versión 4.0.

Para configurar dispositivos VPN sobre un servidor PPTP.

1. Hacer clic en **Inicio**, en la opción **Configuración**, seleccionar **Panel de Control.**

2. Hacer doble clic en el icono de **Red** dentro del **Panel de Control.**

3. Hacer clic en la opción de **Servicios** y seleccionar **Servicio de Acceso Remoto.**

4. Hacer clic en Propiedades para desplegar el cuadro de dialogo de Instalación de Acceso Remoto.

5. Hacer clic en **Adicionar**. Aparecerla el cuadro de dialogo de adicionar dispositivo RAS, tal como se muestra en la figura 6.3:

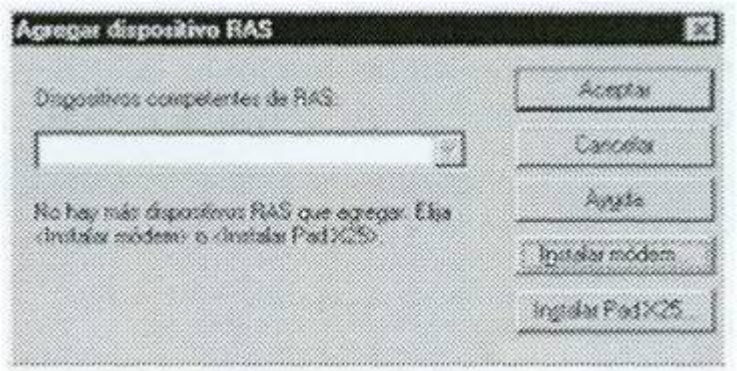

Figura 6.3: Agregar Dispositivo RAS

6. Hacer clic en **Dispositivos de RAS Cargados** y en la flecha que despliega la lista de dispositivos VPN, los cuales podrán ser adicionados y configurados como un puerto y dispositivo dentro del RAS.

7. Seleccionar un dispositivo VPN y hacer clic en **Aceptar**. Repetir los pasos 5, 6 y 7 hasta que todos las VPNs sean adicionadas al cuadro de dialogo de **Instalación de Acceso Remoto.**

8. Seleccionar un puerto VPN y hacer clic en **Configurar**. Verificar que la opción de **Llamadas solamente Recibidas** en el cuadro de dialogo de **Puerto Usado**, este seleccionada y hacer clic en **Aceptar** para regresar al cuadro de dialogo de **Instalación de Acceso Remoto**. (Si también se desea usar este servidor como un cliente PPTP y se quiera usar el dispositivo VPN para hacer llamadas al exterior como un dispositivo PPTP, selecciona Llamadas-Exterior -Dial-Out-).

9. Repetir el ultimo paso para cada dispositivo VPN que se vaya desplegando en el cuadro de dialogo de **Instalación de Acceso Remoto**. (De hecho, los dispositivo VPN en una computadora con Windows NT Server versión 4.0, son configurados automáticamente con la opción de **Llamadas Recibidas Únicamente**, pero se debería verificar esta configuración adicionalmente.)

10. Hacer clic en **Red** para que se despliegue el cuadro de dialogo de **configuración de Red**. Verificar que se reconozca el TCP/IP dentro del cuadro de **configuración de Servidor** en el cuadro de dialogo de **Configuración de Red**. Hacer clic en **Aceptar** para regresar al cuadro de dialogo de **Instalación de Acceso Remoto.**

11. Hacer clic en **Continuar**.

12. Cerrar **Red,** salir de esta opción y **reiniciar** la maquina.

6.3.3. Configuración de las opciones de encriptación y autentificación en un servidor PPTP.

Este apartado incluye procedimientos e información acerca de la configuración de un servidor PPTP. Estos son los 4 principales pasos:

- Encriptamiento de datos enviados sobre Internet.
- Aceptación de paquetes PPTP únicamente, desde Internet.
- Acceso a Redes Privadas.
- Habilitar el traspaso de IP.

Configuración de encriptamiento en el servidor para PPTP.

El encriptamiento de datos se instala por medio del protocolo de acceso remoto, PPP. Se puede habilitar el encriptamiento con la configuración de cada dispositivo VPN que anteriormente se haya adicionado y configurado en el RAS. Esta configuración es idéntica a la configuración de encriptamiento para otros dispositivos RAS, tales como el módem.

Para habilitar el Encriptamiento de un dispositivo VPN en un servidor PPTP.

1. Hacer clic en **Inicio**, en la opción **Configuración,** seleccionar **Panel de Control.**

2. Hacer doble clic en el icono de **Red** dentro del **Panel de Control.**

3. Hacer clic en la opción de **Servicios** y seleccionar **Servicio de Acceso Remoto.**

4. Hacer clic en **Propiedades** para desplegar el cuadro de dialogo de **instalación de Acceso Remoto** (mostrada a continuación).

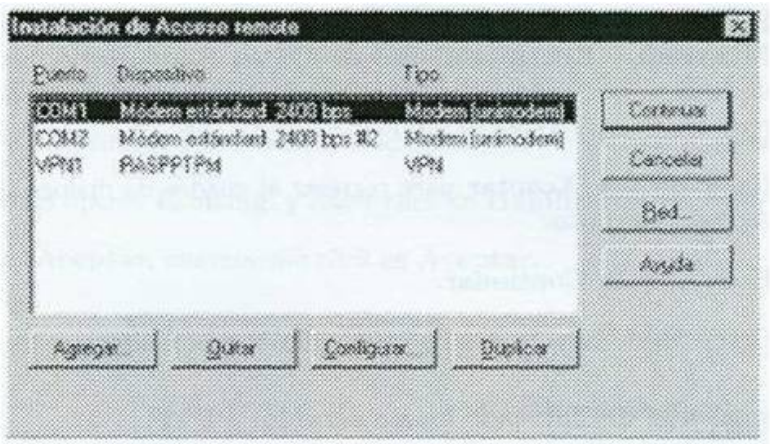

Figura 6.4: Instalación de Acceso Remoto

5 Seleccionar el dispositivo VPN para el cual se desee habilitar el encriptamiento, y hacer clic en **Red.** Aparecerá posteriormente el cuadro de dialogo **Configuración de Red.**

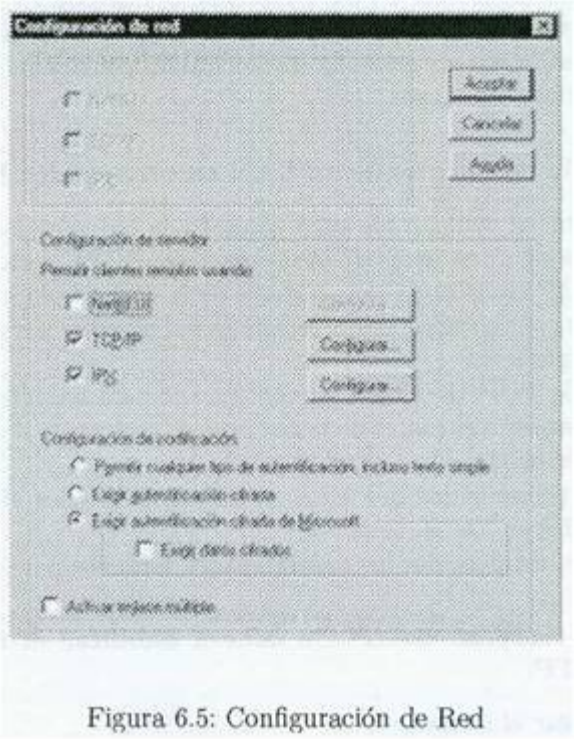

Figura 6.5: Configuración de Red

6. Seleccionar las opciones de **Autentificación - Encriptado requeridas por Microsoft** y **Encriptamiento de Datos Requeridos**. Estas configuraciones de RAS y PPP son basadas en Windows NT autentificación de todos los clientes remotos conectándolos al servidor PPP.

7. Hacer clic en **Aceptar** para regresar al cuadro de dialogo de **Instalación de Acceso Remoto.**

8. Hacer clic en **Continuar.**

9. Cerrar **Red,** salir de esta opción y **reiniciar** la maquina.

Configuración del filtrado en un servidor PPTP.

Habilitar el filtrado en un PPTP provee una forma de seguridad para la red privada por la configuración de un adaptador en la computadora que bloquee todos los paquetes, excepto los paquetes PPTP. En una computadora multiusuario, tal como un servidor PPTP con un adaptador conectado a la red de la empresa y otro adaptador conectador a internet, el filtrado de PPTP debería ser habilitado sobre un adaptador sobre del cual la conexión de PPTP haya sido hecha.

En otras palabras, si los usuarios remotos o móviles son conectados a la red de la empresa usando el servidor PPTP e Internet, el filtrado PPTP debería ser habilitado sobre un adaptador del servidor que esta conectado a Internet. En este caso, el filtrado de PPTP es habilitado por la configuración de las opciones del TCP/IP por el adaptador que fue conectado a Internet.

Configuración de enrutamiento LAN en un servidor PPTP.

RAS deberá ser configurado para accesar a la red privada usando los protocolos de red apropiados en orden para habilitar el servidor PPTP, para traspasar paquetes desde un cliente PPTP hacia el destino correcto de la computadora.

Un RAS es configurado para accesar a la red privada, un servidor PPTP requiere la siguiente configuración:

El protocolo TCP/IP deberá ser configurado para habilitar el traspaso de IP.

Automáticamente el router de la red privada (intranet) se suprimirá por el Registro de entrada adicionado.

Se deberá prevenir que desde los recursos modificados al RAS, las direcciones IP estarán incluidas en los paquetes.

Deberán ser establecidos los enrutamientos estáticos para la red privada.

Habilitar el traspaso de IP. Se deberá habilitar el traspaso de IP en un servidor PPTP.

Para habilitar el traspaso IP

1. Hacer clic en **Inicio,** en **configuración**, y clic en **Panel de Control.**
2. Doble clic en **Red** dentro del **Panel de Control.**
3. Clic en la opción de **Protocolos**, seleccionar TCP/IP y hacer clic en **Propiedades.**
4. Clic en la opción **Routing**, y hacer clic en **Habilitar IP Forwarding.**
5. Clic en **Aceptar**, nuevamente clic en **Aceptar.**

6.4. Instalación y configuración del cliente VPN basado en Windows 98.

6.4.1. Instalación de VPN sobre un cliente en Windows 98.

Para instalar el adaptador VPN en una computadora trabajando con Windows 98.

1. Clic **Inicio**, en el punto de **Configuración,** y clic en el **Panel de Control.**

2. Doble clic en **Red** dentro de **Panel de Control.**

3. Clic en la opción de **Agregar**, y clic en **Adaptador** para desplegar la caja de dialogo. El cuadro de dialogo del **Adaptador de Red** Seleccionado se ilustra en la figura 6.6:

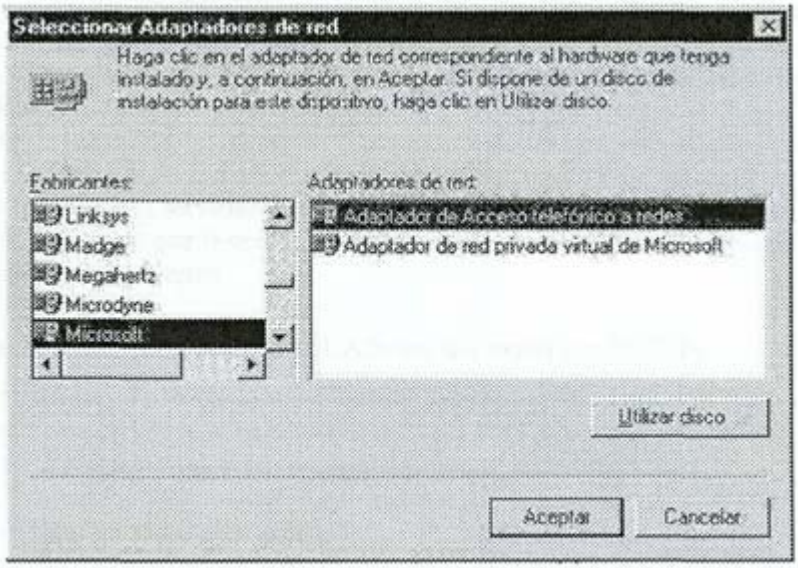

Figura 6.6: Selección de Adaptadores de Red

4. Seleccionar la opción de **Adaptador de Acceso telefónico a redes** y hacer clic en **Aceptar.**

5. Clic en la opción de **Agregar,** y clic en **Adaptador** para desplegar la caja de dialogo. El cuadro de dialogo del **Adaptador de Red Seleccionado** se ilustra en la figura 6.7:

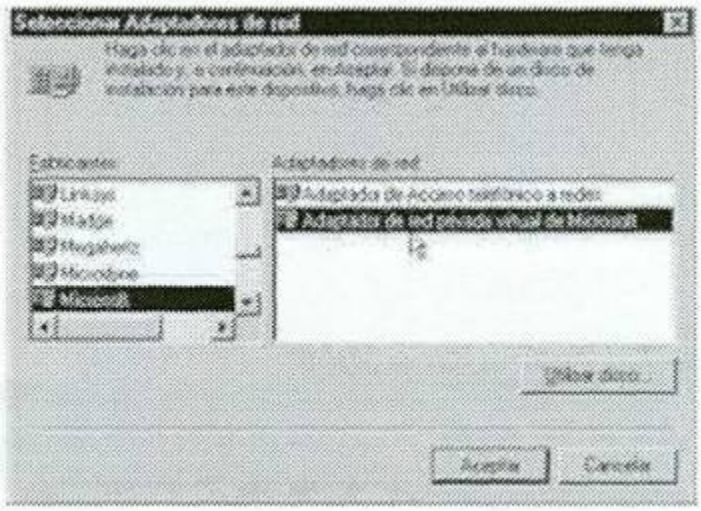

Figura 6.7: Selección de Adaptadores de Red II

6. Seleccionar la opción de **Adaptador de red privada virtual de Microsoft** y hacer clic en **Aceptar.**

7. Clic en **Aceptar** y **Reiniciamos** la maquina.

6.5. Configuración de acceso telefónico a redes con Windows 98

Para realizar la conexión VPN es necesario configurar el acceso al ISP y al PPTP Server.

Los siguientes procedimientos describen como usar una conexión telefónica a la red para configurar una conexión ISP y una PPTP

6.6. Creando la conexión para el ISP.

Si se esta usando un PPTP y una conexión telefónica a la red para conectarte al servidor PPTP con Internet, se necesita crear una conexión al ISP. Para crear una nueva entrada ISP con el uso del asistente para hacer una nueva conexión.

1. Hacer clic en **Inicio**, en **Programas**, en **Accesorios,** y hacer clic en **Acceso Telefónico a Redes.** Aparecerá la ventana de **Acceso telefónico a Redes.**

2. Hacer clic en **Realizar conexión**. Aparecerá el asistente para **Realizar una nueva conexión**.

3. Hacer clic en **Siguiente**. Aparecerá la siguiente pantalla.

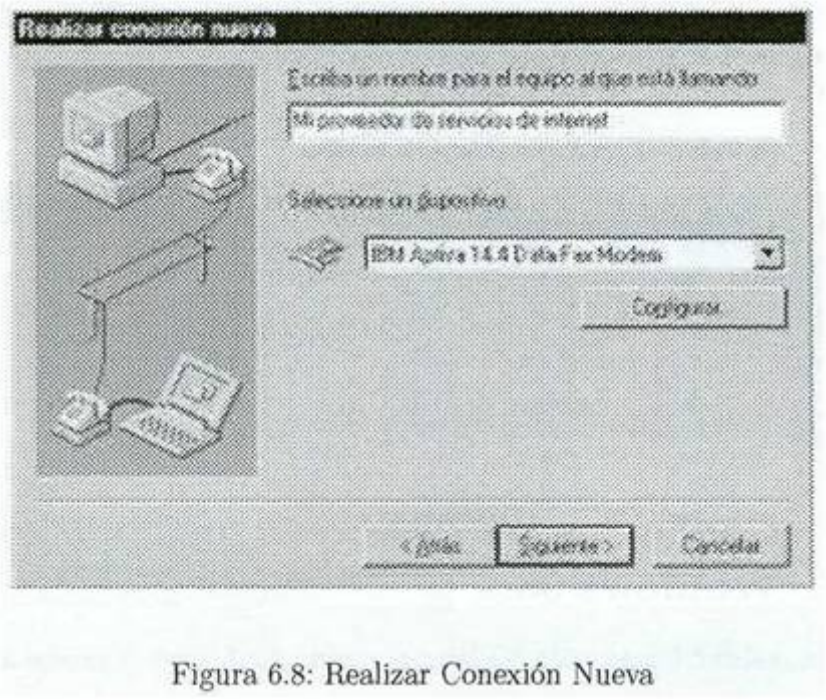

Figura 6.8: Realizar Conexión Nueva

4. Se escribe el nombre para la conexión, en **Escriba un nombre para el equipo al que esta llamando.**

5. Selecciona el tipo de módem en **Seleccione un dispositivo**, y hacer clic en **Siguiente**. Aparecerá la siguiente pantalla.

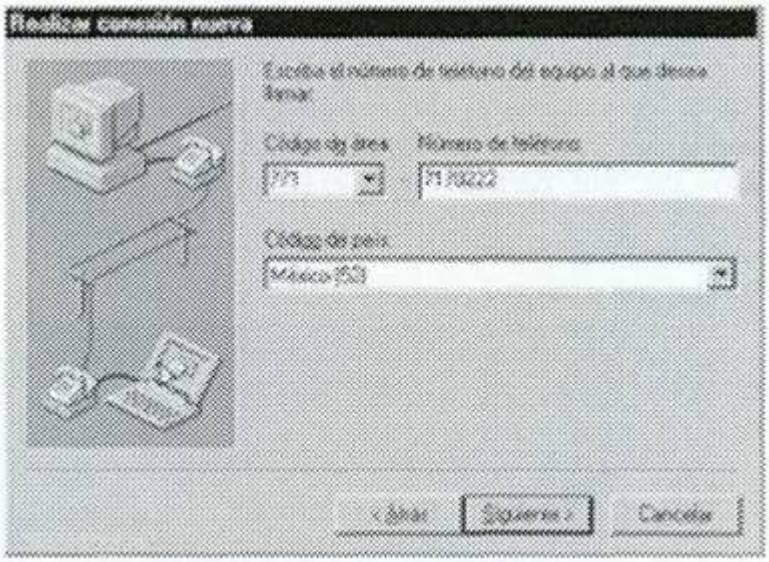

Figura 6.9: Realizar Conexión Nueva II

6. Escribe el número de teléfono del ISP en **Número de teléfono**.

7. Hacer click en **Siguiente**, y después en **Finalizar**. Un icono de conexión se ha creado en la carpeta de **Acceso telefónico a Redes**, tal como se muestra en la figura 6.10.

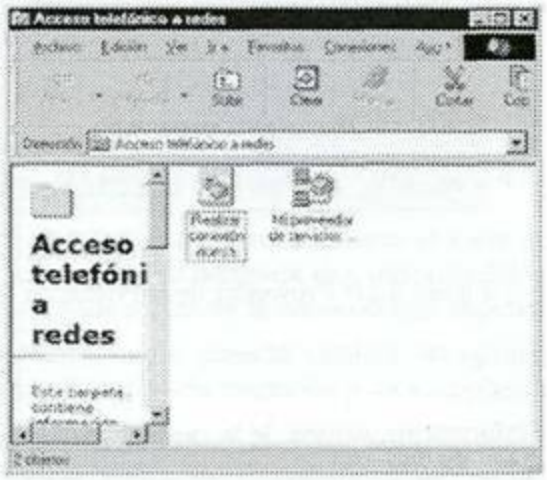

Figura 6.10: Acceso telefónico a Redes

8. Verificar la conexión, usando el siguiente procedimiento.

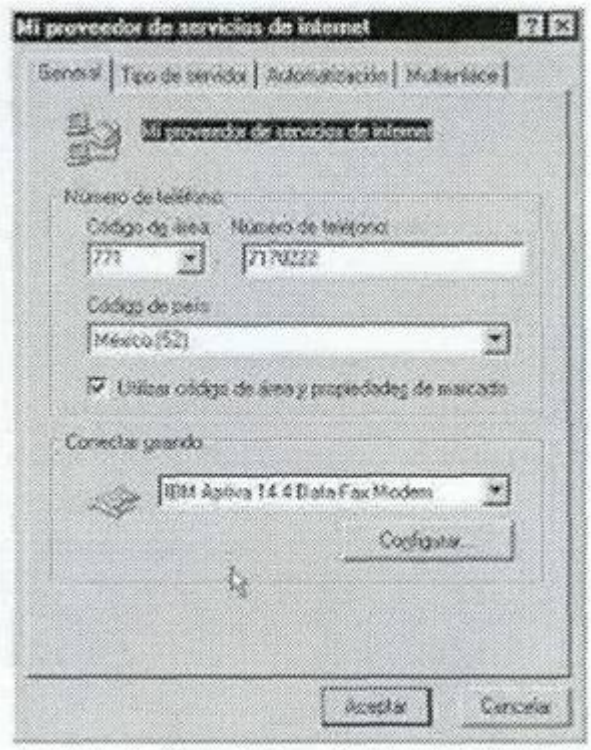

Figura 6.11: Proveedor de Servicios de Internet

6.6.1. Verificar o editar la conexión ISP.

1. Dentro de Mi PC, con el click derecho en el icono de conexión en la carpeta de **Acceso telefónico a Redes**, hacer click en **Propiedades** para verificar que tu conexión ISP este correctamente configurada. Aparecerá el siguiente cuadro de dialogo.

2. Revisar la información dentro de la pestaña de **General** para asegurar de que el número de teléfono sea el correcto y que el MODEM o dispositivo ISDN seleccionado también sea el correcto. De lo contrario hacer los cambios necesarios.

3. Hacer click en la pestaña de **Tipos de Servidor**. Esta pestaña se ilustra en la figura 6.12.

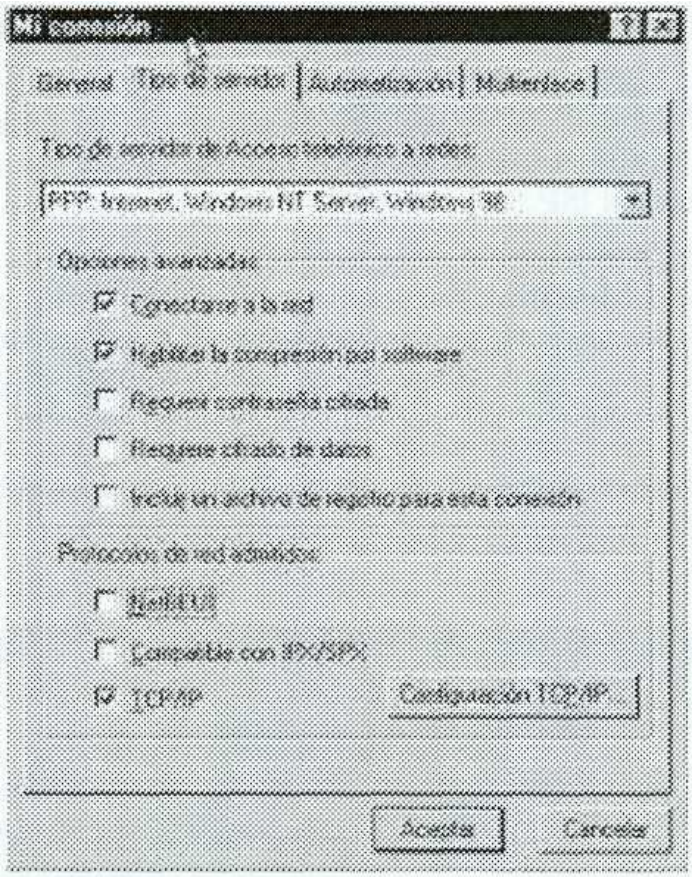

Figura 6.12: Mi Conexión

4. Revisa la información que contiene la pestaña de **Tipos de Servidor**.

5. Que el cuadro de Acceso telefónico por tipo de servidor, despliegue lo siguiente:"**PPP: Internet, Windows NT Server, Windows 98".**

6. En el cuadro de **Opciones Avanzadas**, borra el login de acceso a red que se encuentra en el cuadro. No es necesaria una conexión ISP para esta opción, aun borrando el login, puede realizarse la conexión más rápidamente.

   NOTA: Normalmente, no se necesita cambiar las opciones de Compresión de software habilitado y contraseña requerida para encriptamiento.

7. En el cuadro de **Protocolos de red Admitidos**, asegurarse de que el TCP/IP este seleccionado y que los otros protocolos de red no lo estén. Cancelando la selección de los otros protocolos de red, se habilita la conexión del ISP más rápidamente.

8. Hacer click en **Configuración de TCP/IP** se despliega el cuadro de dialogo de Configuración de PPP y TCP/IP. Asegurarse que la instalación del TCP/IP este

conformada por las configuraciones requeridas por el proveedor de ISP.

NOTA: Normalmente no se necesita cambiar los valores de la pestaña **Scripting**. Sin embargo, si el ISP requiere de entrar con un login manualmente, se puede usar un script para automatizar el proceso. Si se desea usar un script, consulta al proveedor del ISP para saber la configuración correcta.

También, normalmente no se cambian los valores de la pestaña **Multilink.** Para habilitar el **Multilink** usa dos dispositivos (tales como un módem o un dispositivo ISDN) del mismo tipo y velocidad para una liga simple de acceso telefónico externo. Si se tiene dos dispositivos y diversidad de multilink por parte del soporte del ISP, consulta al ISP para la configuración correcta.

9. Hacer click en Aceptar.

6.6.2. Creando la conexión al servidor PPTP.

Se deberá crear la conexión al servidor PPTP usando un dispositivo VPN.

Para crear una conexión de acceso telefónico externo al servidor PPTP usando un dispositivo VPN.

1. Hacer click en **Inicio**, en **Programas**, en **Accesorios**, y hacer click en **Acceso telefónico a Redes**. Aparecerá la ventana de **Acceso telefónico a Redes.**

2. Hacer click en la ventana de **Hacer una conexión nueva**. Aparecerá el asistente para Realizar una **conexión Nueva**, tal como se ilustra en la figura 6.13.

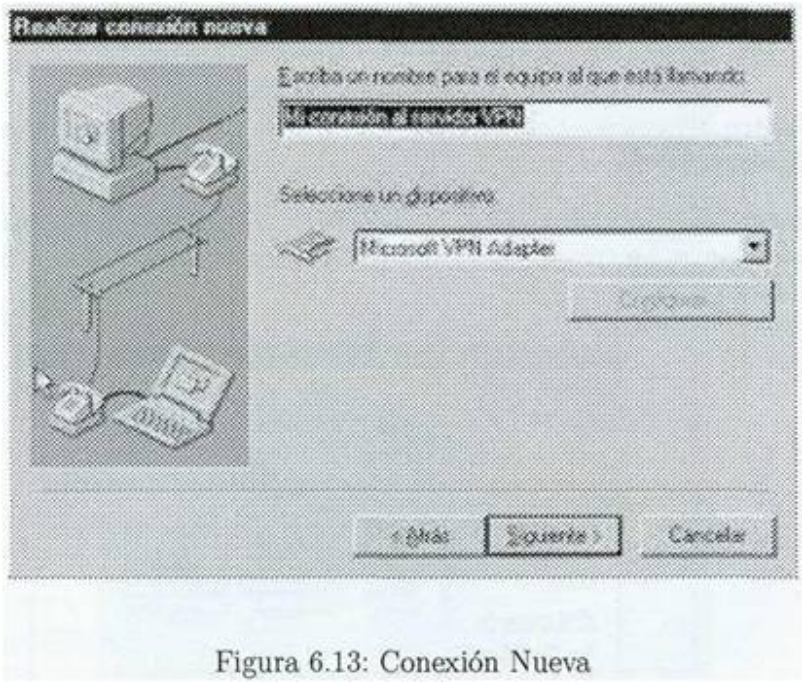

Figura 6.13: Conexión Nueva

3. Escribir el nombre de la conexión del servidor PPTP en el cuadro de escribe un nombre para la computadora a la que deseas enlazarte.

4. Selecciona el Adaptador de Microsoft VPN en la caja **Seleccionar un Dispositivo** y hacer click en **Siguiente**. Aparecerá el siguiente cuadro de dialogo.

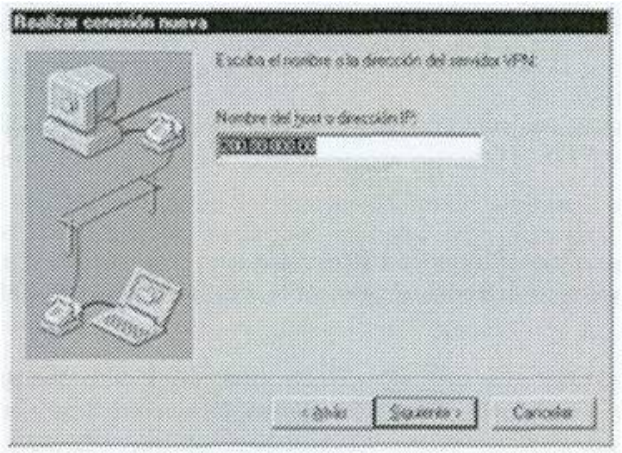

Figura 6.14: Conexión Nueva II

5. Dentro del cuadro del Nombre del Host y dirección IP, escribe el nombre o dirección IP del servidor PPTP que este conectado a Internet.

6. Hacer click en Siguiente, y después hacer click en Finalizar. Un icono de conexión se ha creado en a carpeta de Acceso telefónico a Redes, así como se ilustra en la figura 6.15:

Figura 6.15: Acceso Telefónico a Redes

7. Verificar que la conexión del servidor PPTP este usando el siguiente procedimiento.

Nota: Mantener en mente que después de que se conecto al servidor PPTP sobre una red remota, la estación de trabajo será conectada para la red remota tal como si se estuviera conectado físicamente a la misma. De todas formas, se deberá asegurar que la estación de trabajo y sus aplicaciones soporten los protocolos nativos de la red.

6.6.3. Para verificar o editar la conexión al servidor PPTP.

1. En **Mi PC**, con el click derecho en el icono de **conexión del servidor PPTP** dentro de la carpeta de **Acceso telefónico a Redes**, y hacer click en **Propiedades** para verificar que la conexión al servidor PPTP este configurada correctamente. El cuadro de dialogo del Servidor PPTP aparecerá, tal como se ilustra en la figura 6.16:

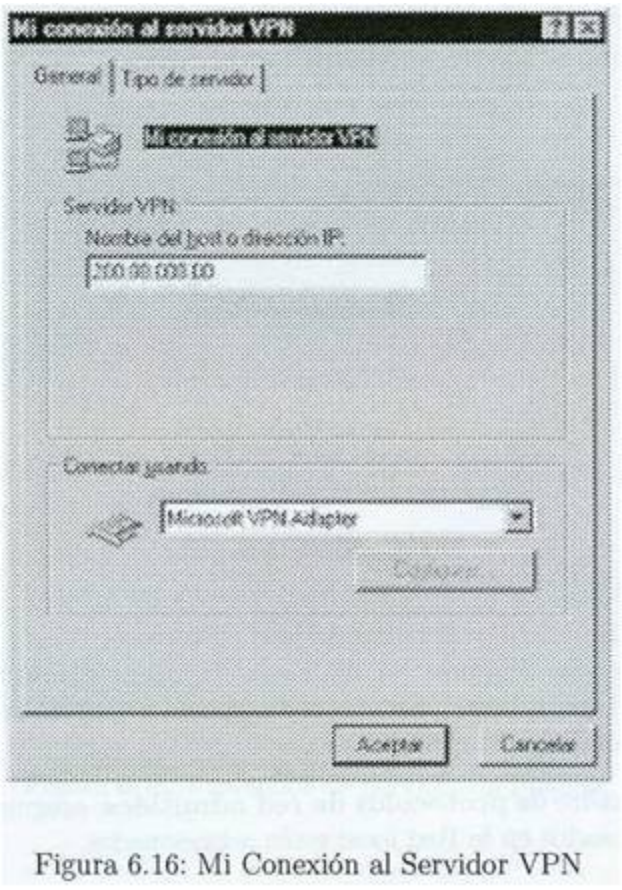

Figura 6.16: Mi Conexión al Servidor VPN

2. Revisar la información dentro de la pestaña de **General**, para asegurarse de que el nombre del Host o de la dirección IP este correcta y el adaptador VPN de Microsoft este seleccionado. Hacer los cambios necesarios.

3. Hacer click en la opción de **Tipos de Servidor**. Esta opción de Tipos de Servidor se ilustra en la siguiente figura:

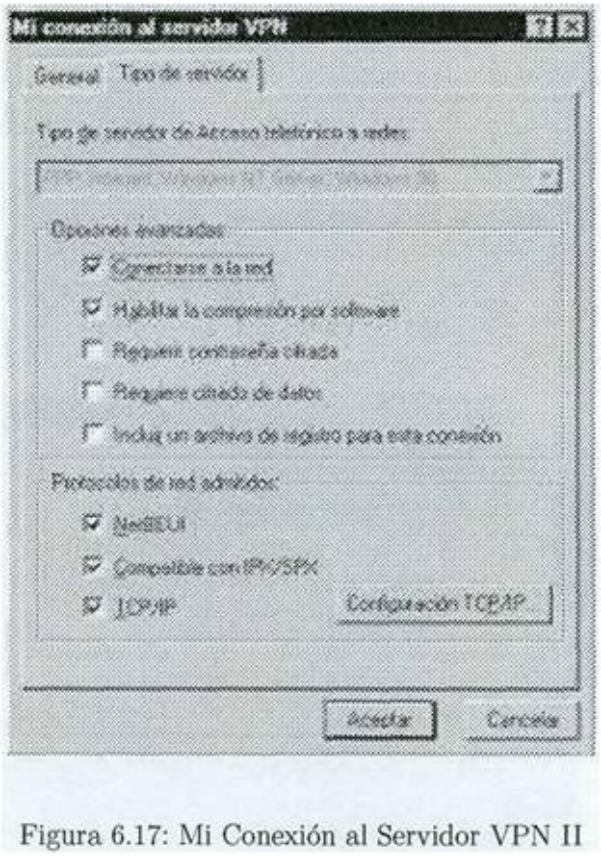

Figura 6.17: Mi Conexión al Servidor VPN II

4. Dentro del cuadro de **Opciones Avanzadas**, asegurarse de que en el cuadro de Login para entrar a red, este seleccionado, para entrar con un login a la red.

   Nota: El sistema operativo de red, así como el Windows para trabajo en grupo de Microsoft, Windows NT de Microsoft y Red de Novell requiere de que se accese con un login a la red. En contraste, generalmente las redes basadas en UNIX no requieren de hacer esto.

5. En el cuadro de **Protocolos de red admitidos**, asegurarse de que los protocolos de red usados en la Red local estén seleccionados.

6. Sí se usa el protocolo TCP/IP en la red privada, hacer click en **Configuración de TCP/IP** para que se despliegue el cuadro de Configuración de TCP/IP.

   Asegurarse de que la configuración TCP/IP este conformado por las configuraciones requeridas por un cliente.

7. Hacer click en **Aceptar.**

6.7. Conectando al Servidor VPN.

Primero, necesitamos conectarnos al ISP:

1. Hacer click a **"mi proveedor de servicio de Internet"** debemos contar con una cuenta de usuarios la cual la proporciona el Proveedor de Servicios de Internet.

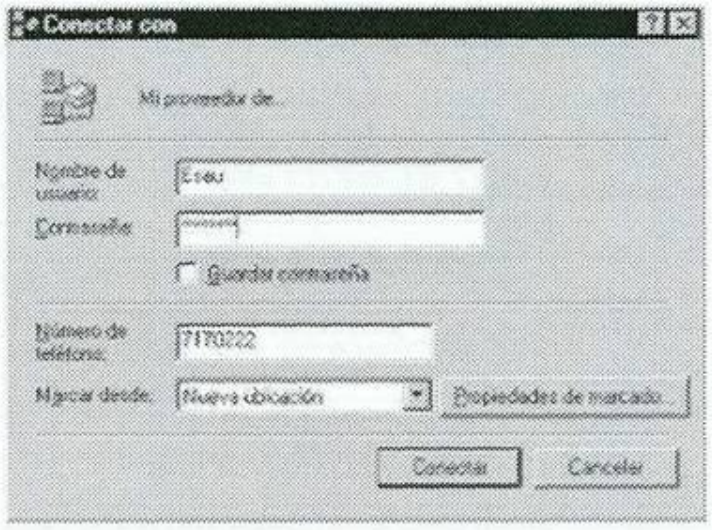

Figura 6.18: Proveedor de Servicio de Internet

2. Hacer click a **"mi conexión al servicio VPN",** debemos contar con una cuenta de usuario (NT) que tenga los derechos necesarios para acceder a la red local.

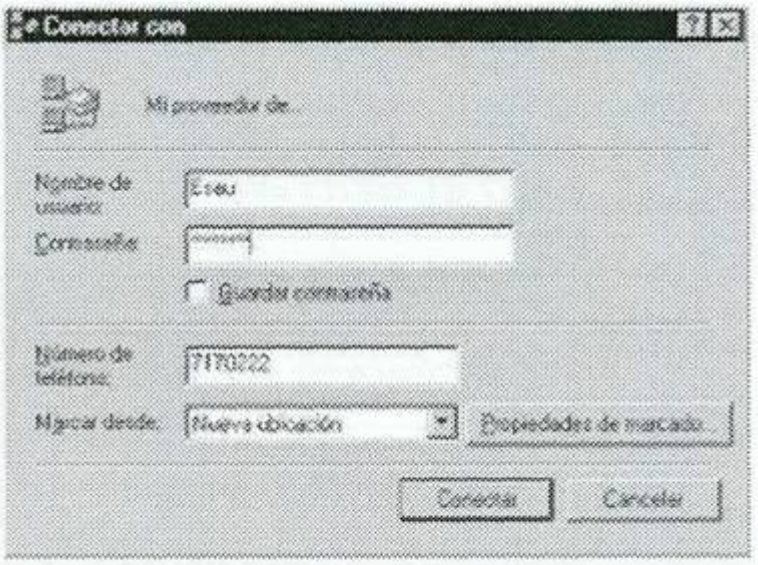

Figura 6.18: Proveedor de Servicio de Internet

3. Tendremos ahora 2 conexiones nuevas.
4. Para confirmar que estemos conectados a la red, únicamente daremos click a **Entorno de Red.**
5. **Listo estamos conectados.**

Comentarios y Referencias

Implementación de una solución VPN

Ejemplo de costos de la VPN

A continuación se muestra un ejemplo de como la solución VPN disminuye de manera significativa los costos económicos en comparación con una solución tradicional de acceso remoto. El calculo está basado en el numero de usuarios remotos simultáneos que se necesitan conectar y si se requieren clientes VPN basados en software, hardware o soluciones de router para los tele trabajadores.

Los datos se muestran en la siguiente tabla:

Tabla 6.1: Solución VPN

Variables	Datos
Número total de usuarios remotos que actualmente hacen llamadas usando un numero local	10
Número total de usuarios remotos que actualmente hacen llamadas de larga distancia o número 800	30
Horas promedio a la semana que cada usuario gasta en llamadas	10
Costo promedio por minuto de una llamada de larga distancia o número 800	$1
Número de usuarios de acceso remoto simultáneos que la solución VPN necesita soportar	25
Número de usuarios de acceso remoto con conexiones de banda ancha (cable o DSL) en sus hogares	5
Solución de cliente VPN basada en software, hardware o router	Cliente software

Los resultados son los siguientes:

Tabla 6.2: Resultados obtenidos de costos de la VPN

Costo mensual con solución tradicional dial-up de acceso remoto			Costo mensual de la VPN	
Usuarios remotos de larga distancia o numero 800		30	Total de usuarios dial-up	35
Horas promedio de llamadas por semana	X	10	Costo del ISP	X$200
Costo por minuto de una llamada de larga distancia o número 800	X	$1		7000
Minutos/Hora x Semana/Mes (constante)	X	240	Usuarios de banda ancha	5
			Costo del ISP	X500
				2500
Total con dial-up tradicional $72,000			Total con VPN: $9,500	
Ahorros mensuales: $62,500				
Costos de Hardware: 1 concentrador Cisco VPN 3005				
Total de costos de inversión mínimos; $40,000				
Periodo de reembolso: 1 mes				

Gastos de inversión. Con el fin de soportar a 25 usuarios simultáneos, por lo menos se implementa 1 concentrador Cisco VPN 3005 con un precio aproximado de $40,000.

Ahorros mensuales. Al implementar la VPN de acceso remoto a Logistic Meginter, los costos mensuales se reducen al utilizar un ISP que cobra $200 por usuario dial-up (módem 56 Kbps) o $500 para usuarios de banda ancha (cable o DSL). La inversión inicial en equipo e instalación de la VPN es rápidamente recuperada por los ahorros mensuales obtenidos.

Variables. Para esto se asume que cada usuario sólo tendrá un tipo de acceso a Internet con el fin de reducir costos. Si se desea utilizar tanto acceso dial-up como de banda ancha para cada uno de los usuarios (en el caso de que cada uno de ellos utilice la VPN tanto en el hogar como cuando viaja) los costos aumentaran.

Administración de la VPN. La puesta en marcha y la administración de la solución VPN requieren de personal técnico altamente capacitado y de tiempo suficiente para diseñar la VPN cuidadosamente. Tales recursos pueden llegar a ser escasos y difíciles de implementar dentro de una organización.

Consecuentemente, las organizaciones buscan soluciones externas para administrar toda o parte de la infraestructura de la VPN. Un gran número de proveedores de servicios ofrecen servicios de administración de la VPN.[13] [10]

[13] www.cisco.com

A continuación se muestra un ejemplo de cuanto costara administrar la VPN de acceso remoto dentro de la organización con la administración externa por parte de un proveedor de servicios VPN.

Tabla 6.3: Comparación de costos administrativos de una VPN.

	Administración de la VPN internamente	Administración de la VPN externamente
	Porcentaje de ahorro de la VPN externa sobre una interna: 34 %	
Costo de mantenimiento mensual	$12,000	$0
Costo mensual de acceso a la VPN	$9,500	$14,000
Costos totales (de acceso a la VPN + Mantenimiento)	$21,500	$14,000

Costo de administración interno de la VPN. En este caso se ha estimado que costara aproximadamente $300 por usuario la administración.

Costo de administración externa de la VPN. Típicamente, los proveedores de servicios incorporan tarifas de mantenimiento dentro de los cargos mensuales por acceso a Internet. Por lo tanto, se ha estimado que el acceso a Internet dial-up costara $300/mes y el acceso a Internet de banda ancha costara $700/mes.

Los resultados obtenidos muestran un buen desempeño del sistema VPN, muestran una dinámica y rápida conexión que permite obtener una estimación muy buena de acceso remoto de un usuario móvil, existen muchos sistemas operativos para instalar una VPN en el mercado sin embargo uno de los mas utilizados debido a lo explicado en el proyecto es el Windows NT Server versión 4.0.

Al concluir este capitulo se cumplen todos los objetivos del trabajo de investigación, entregando valiosos resultados que muestran los grandes beneficios entregados a la empresa Logistic Meginter.

Conclusiones

La VPN representa una gran solución para Logistic Meginter S.A. de C.V. en cuanto a seguridad, confidencialidad e integridad de los datos y se ha vuelto un tema importante en la organización, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el único inconveniente que pudiera tener la VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no esta bien definido pueden existir consecuencias serias.

En el aspecto de las comunicaciones destaca su importancia la tendencia mundial, de dirigir las telecomunicaciones hacia una sola red global y la automatización total de ella, ya que en la medida que el sistema telefónico nacional evolucione con la mezcla de servicios se podrá observar un mejor desarrollo del país.

En conclusión, una Red Virtual Privada es el próximo futuro para nuevas compañías de telecomunicaciones que desean tener redes pequeñas capaces de tener los últimos adelantos de la tecnología, debido a que los beneficios de una red virtual privada son demasiados ya que es la seguridad ofrecida a organizaciones que no pueden afrontar la dedicación de líneas tradicionales usadas para conectar oficinas remotas.

Las soluciones de las VPN serán definidas por la cobertura de las características que ofrecen a los usuarios. Una plataforma VPN deberá ser segura contra intrusos, la misión de entrega de datos deberá ser de manera confiable y oportuna, y debe ser administrable a través de la empresa.

Ahora bien como se observa en la tabla 6.4, la VPN tiene ventajas importantes sobre las redes normales podríamos decir como primordial la recuperación de la inversión así como el costo operativo muy bajo así como la infinidad de funcionalidades, que hoy en días las compañías de telecomunicaciones buscan al invertir su capital en una red.

Las VPN hoy en día abarcan una pequeña parte dentro del mercado mundial, lo cual trae como consecuencia una gran dependencia del extranjero, siendo este un mercado importantísimo tanto política como tecnológicamente es altamente recomendable iniciar acciones que lleven a figurar en este mercado, aunque la tarea no sea nada fácil tomando en cuenta quienes son los actuales lideres del mercado.

Debido a lo anterior se hace urgente la necesidad de que al mismo tiempo que las redes se modernizan con equipo altamente tecnológico, también se cuente con un grupo de personal mexicano altamente calificado capaz de resolver cualquier problema y que no solo se dedique a recibir y estudiar tecnología extranjera, si no que también diseñe e implemente y desarrolle redes, mostrando al mundo que la ingeniería en México esta al nivel de cualquier otro en el mundo, evitando así la gran dependencia tecnológica que actualmente sufrimos.

Tabla 6.4: Ventajas de una VPN sobre una Red Normal

CARACTERÍSTICAS	VPN	RED NORMAL
INFRAESTRUCTURA PROPIA		X
SEGURIDAD	X	X
SERVICIOS	X	X
REDUCCIÓN DE CARGA ADMINISTRATIVA	X	
COSTOS ADMINISTRATIVOS MAS BAJOS	X	
COSTOS OPERACIONALES MAS BAJOS	X	
SIMPLIFICACIÓN DE TOPOLOGÍA DE RED	X	
ESCALABILIDAD	X	X
RECUPERACIÓN DE LA INVERSIÓN	MESES	AÑOS
TIEMPO DE IMPLEMENTACIÓN DE LA RED	INMEDIATA	6 MESES

Glosario

100Base-T: también conocido como Fast Ethernet o Ethernet de alta velocidad, se trata de un estándar de conexión Ethernet con una velocidad de transferencia de datos de hasta 100 Mbps.

10Base-T: estándar de conexión Ethernet más antiguo con una transferencia de datos de hasta 10 Mbps.

802.3: Especificación del IEEE (Institute of Electrical and Electronics Engineers) que describe las características de las conexiones Ethernet en redes de cableado.

A

Access point (Punto de acceso): Dispositivo que intercambia los datos entre los diferentes ordenadores de la red. Los puntos de acceso no suelen tener cortafuegos ni funciones de traducción de direcciones (NAT).

Adaptador de red: también se conoce como tarjeta de interfaz de red (NIC). Tarjeta de expansión o cualquier otro dispositivo utilizado para proporcionar acceso a un ordenador, impresora o cualquier otro componente de la red.

Adaptador USB: Dispositivo que se conecta al puerto USB.

Adaptador: también conocido como tarjeta de interfaz de red Ethernet (NIC), se trata de cualquier tarjeta de expansión u otro dispositivo que se utiliza para proporcionar acceso a la red en ordenadores, impresoras u otros periféricos.

Administrador: Persona responsable de la planificación, configuración y gestión de las operaciones diarias de la red. Entre otras tareas, el administrador se encarga de instalar nuevas estaciones de trabajo u otros dispositivos, añadir o eliminar personas de la lista de usuarios autorizados, archivar documentos, controlar las contraseñas de acceso y otras medidas de seguridad, supervisar el uso de los recursos compartidos y solucionar los problemas del sistema.

Ancho de banda: Cantidad de los datos o tamaño de los archivos que pueden transferirse a través de una conexión de red en un momento dado. Cuanto mayor es el ancho de banda la información se transmite con mayor rapidez.

Autenticación: Proceso de identificación mediante nombre de usuario y contraseña. En los sistemas de seguridad, la autenticación es una forma de autorización (proceso por el que se permite a los usuarios el acceso a los recursos del sistema según su identidad). La autenticación se limita a comprobar si el usuario es quien dice ser, pero no contempla los derechos de acceso.

B

Bridge (Puente): Dispositivo que reenvía paquetes o información de un segmento a otro de la red. Solo transfiere aquellos paquetes necesarios para la comunicación entre los segmentos.

Broadband connection (conexión de banda ancha): Es la conexión de alta velocidad en módems de cable o DSL con una velocidad de transferencia a partir de 256 Kbps.

Broadband modem (módem de banda ancha): Dispositivo que ofrece una conexión a Internet de banda ancha. Los dos tipos más habituales son los módems de cable, basados en la infraestructura de televisión por cable, y los módems DSL, que se sirven de las líneas telefónicas que funcionan a velocidad DSL.

Broadcast (Distribución): Con esta función se envía un mensaje a todos los usuarios de la red, mientras que con la multidifusion o multicasting se envía un mensaje solo a los miembros de una lista seleccionada.

Bus: líneas físicas que se utilizan para la transferencia de datos entre componentes de un ordenador. En otras palabras, es lo que permite compartir la información entre las diferentes partes del sistema. Los buses, por ejemplo, conectan la unidad de disco duro, la memoria o los puertos de entrada y salida al microprocesador.

C

Cable Cat. 5: Abreviatura de cable de categoría 5. Es un tipo de cable Ethernet que admite una velocidad de transferencia de datos de hasta 100 Mbps.

Cable cruzado: Tipo de cable que facilita las comunicaciones de red al interconectar dos ordenadores invirtiendo los contactos de sus respectivas patillas.

Cable de conexión directa: Tipo de cable que hace posible las comunicaciones de la red. Los cables Ethernet de conexión directa pueden ser de dos tipos: trenzado o coaxial. Ambos permiten una velocidad de transferencia de datos de 10 Mbps. A diferencia de los cables cruzados, los cables de conexión directa tienen los contactos de las patillas en la misma posición en ambos extremos del cable.

Cable Ethernet: Tipo de cable que facilita las comunicaciones de la red. Los cables Ethernet pueden ser de dos tipos: de par trenzado o coaxial. Ambos permiten una velocidad de transferencia de datos de 10 Mbps.

Cable modem (módem de cable): Dispositivo que ofrece una conexión a Internet de banda ancha. Los módems de cable utilizan la infraestructura de la televisión por cable. Es decir, que los datos se transmiten por las mismas líneas de la televisión. Canal: Ruta o enlace por el que pasa la información entre dos dispositivos.

Capa MAC: Abreviatura de Media Access Control layer (Capa de control de acceso a medios). Subcapa inferior de dos subcapas que forman la capa de conexión de datos (Data Link) en el modelo de referencia ISO/OSI. La capa MAC gestiona el acceso a la red física. Protocolos como Ethernet funcionan a este nivel.

Carpeta compartida: Carpeta de un ordenador que se pone a disposición de otros usuarios de la red.

CHAP: Challenge Handshake Authentication Protocol (Protocolo de autenticación por desafío mutuo). Es un tipo de autenticación donde el dispositivo que la realiza, normalmente el servidor de la red, envía un valor seleccionado al azar (una sola vez) y un valor identificativo al programa cliente. El emisor y el punto deben compartir una clave predefinida.

Cifrado: Trascripción de los datos mediante un código secreto. Es el método más efectivo de garantizar la seguridad de los datos. Para leer un archivo cifrado, es preciso tener acceso a la clave secreta o contraseña que permite descifrarlo.

Cliente: Cualquier ordenador o programa que se conecta o solicita los servicios de otro ordenador o programa de la red. Tanto en las redes locales (LAN) como en Internet, se considera un cliente a todo ordenador que utilice recursos de red compartidos proporcionados por un servidor.

Compartir: Poner los recursos asociados a un ordenador a disposición de los demás usuarios de la red.

Conector RJ-11: Clavija que se utiliza para conectar dispositivos, como un módem, a la línea telefónica o para conectar las líneas telefónicas externas.

Conector RJ-45: Clavija que se encuentra en los extremos de los cables Ethernet que realiza la conexión entre los ordenadores u otros dispositivos y el cable Ethernet.

Conector USB: Extremo del cable USB que se inserta o enchufa en el puerto USB. Tiene forma rectangular y es algo aplastado, con una altura algo menor de un centímetro.

Conmutación: Forma de comunicación se utiliza temporalmente para establecer un enlace o una ruta para enviar información entre dos dispositivos. En redes, la conmutación de mensajes o de paquetes permite el intercambio de información entre dos dispositivos. Los mensajes son encaminados o dirigidos a través de estaciones que funcionan como intermediarios entre el emisor y el receptor.

Controlador: En redes, mecanismo que funciona de mediador de las comunicaciones entre el ordenador y el adaptador de red instalado en el ordenador.

D

DHCP: Sigla de Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de hosts). Es un protocolo TCP/IP que asigna automáticamente direcciones IP temporales a los ordenadores de la red local (LAN). El USR8200 Firewall/VPN/NAS es compatible con el uso de DHCP, lo que le permite compartir la conexión a Internet con varios ordenadores de la red.

Dirección de la puerta de enlace: dirección IP que se utiliza al realizar una conexión externa a la red.

Dirección MAC: Media Access Control address (dirección de control de acceso a medios). Se utiliza para las comunicaciones entre los distintos adaptadores de red de una misma subred. Cada adaptador viene de fábrica con una dirección MAC exclusiva.

DMZ: Sigla de Demilitarized Zone (Zona desmilitarizada). Se trata de un conjunto de dispositivos y subredes ubicadas entre la red privada y la conexión a Internet que protegen a dicha red de accesos no autorizados.

DNS: Sigla de Domain Name System (sistema de nombres de dominio). Servicio de consulta de datos utilizado principalmente en la Red para traducir los nombres de los hosts en direcciones de Internet. La base de datos DNS traduce los nombres de dominios DNS a direcciones IP, de forma que los usuarios puedan localizar los ordenadores y servicios a través de nombres más sencillos.

Dominio de Internet: En redes, conjunto de ordenadores que comparten la base de datos de dominios y las directrices de seguridad. Cada dominio se gestiona como si fuera una unidad, con reglas y procedimientos comunes, y con un único nombre identificativo.

Dominio: En redes, conjunto de ordenadores que comparten la base de datos de dominios y las directrices de seguridad. Cada dominio se gestiona como si fuera una unidad, con reglas y procedimientos comunes, y con un único nombre identificativo.

DSL modem (módem DSL): Dispositivo que ofrece una conexión a Internet de banda ancha. Los módems DSL se sirven de las líneas telefónicas pero ofreciendo una gran velocidad de conexión.

DSL: Sigla de Digital Subscriber Line (línea digital de abonado). Conexión digital a Internet ininterrumpida y de alta velocidad que utiliza la infraestructura telefónica estándar.

Dúplex: Modo de conexión. La transmisión dúplex completa permite la transferencia simultánea de información entre el emisor y el receptor. La transmisión media dúplex solo permite enviar información en una dirección cada vez.

Dynamic IP address (dirección IP dinámica): dirección IP asignada a un dispositivo que la necesite mediante el protocolo DHCP. El ISP también puede asignar direcciones IP dinámicas a puertas de enlace o routers.

E

Ethernet: estándar de red que se sirve del cableado para proporcionar acceso a la red. Es la tecnología que más se utiliza para conectar ordenadores entre sí.

F

Firewall (Cortafuegos): Sistema de seguridad que protege la red de amenazas externas, como ataques de piratas informáticos. Un hardware de cortafuegos es un dispositivo de encaminamiento de conexión dispone de configuración de comprobación de datos específica con la que protege los dispositivos a los que está conectado.

Firmware: información de programas guardada en la memoria permanente del dispositivo.

FTP: File Transfer Protocol (Protocolo de transferencia de archivos). Protocolo de Internet estándar para la descarga o transferencia de archivos de un ordenador a otro.

G

Gateway (Puerta de enlace): Dispositivo que actúa como punto central de los dispositivos conectados y que se encarga de recibir y reenviar los mensajes transmitidos. El USR8200 Firewall/VPN/NAS puede conectar varios ordenadores a una misma red y compartir una conexión cifrada a Internet con dispositivos inalámbricos o con cables.

H

Hexadecimal: Sistema de numeración que utiliza 16 como base en lugar de 10 (sistema decimal) para la representación de números, por lo que también se le conoce como sistema de numeración de base 16. El sistema hexadecimal utiliza dígitos del 0 al 9 y las letras de la A a la F (tanto en mayúsculas como en minúsculas) para representar los números decimales del 0 al 15. así, por ejemplo, la letra hexadecimal D representa al número 13 del sistema decimal. Un dígito hexadecimal equivale a 4 bits y un 1 byte puede expresarse con dos dígitos hexadecimales.

Hub (Concentrador): Dispositivo con múltiples puertos que funciona como punto central de conexión para las líneas de comunicación entre todos los dispositivos de una red. Cuando la información llega a un puerto, esta se copia en los demás.

I

IEEE: Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos). Asociación profesional se encarga de desarrollar estándares para los sectores científicos relacionados con la electricidad, la electrónica y la informática. El IEEE es una asociación sin fines lucrativos que cuenta con más de 377.000 miembros en 150 países. El nombre completo es Institute of Electrical and Electronics Engineers, Inc., aunque la forma más habitual de referirse a ellos es con la sigla IEEE.

Impresora compartida: Impresora conectada a un único ordenador a la que tienen acceso otros usuarios de la red.

Intranet: Red dentro de una organización que se sirve de las tecnologías de Internet, como navegadores Web para ver la información, y protocolos, tales como TCP/IP, pero que solo está disponible para cierto tipo de usuarios, como los empleados de una empresa. también se conoce con el nombre de red privada. Algunas Intranets ofrecen acceso a Internet, que se controla mediante un cortafuegos.

IP address (dirección IP): Abreviatura de dirección del protocolo de Internet. IP es el protocolo dentro del binomio TCP/IP que se utiliza para enviar datos entre dos ordenadores a través de Internet. Una dirección IP es el número que se asigna a un ordenador concreto dentro de una red conectada a través de TCP/IP para poder identificar al ordenador. Este número está formado por cuatro segmentos separados por puntos, que van del 0 al 255, por ejemplo: 192.168.1.1.

IP: Sigla de Internet Protocol (Protocolo de Internet). Protocolo dentro del binomio TCP/IP que se utiliza para enviar datos entre dos ordenadores a través de Internet. Este protocolo, en concreto, es el que se encarga del encaminamiento de los mensajes de datos que se transmiten fragmentados en lo que se denomina como paquetes.

ISP: Internet Service Provider (proveedor de servicios de Internet). Empresa que proporciona acceso a Internet a usuarios individuales o a empresas.

K

Kbps: Abreviatura de Kilobits por segundo. Velocidad de transferencia de datos a través de un módem o de la red medida en múltiplos de 1.000 bits por segundo.

L

LAN: Sigla de Local Area Network (Red de área local). Conjunto de ordenadores y otros dispositivos en un área relativamente limitada, como por ejemplo un edificio, conectados entre sí por un sistema de comunicación que les permite interactuar entre ellos.

M

Mapeado: Procedimiento por el que un ordenador puede comunicarse con un recurso situado en otro ordenador de la red. Si se quiere acceder a una carpeta que se encuentra en otro ordenador, por ejemplo, hay que mapearla. Para ello, el ordenador en el que está ubicada debe estar configurado para compartir dicha carpeta.

Mascara de subred: Normalmente, una subred representa a todos los equipos ubicados en un espacio concreto (en un edificio, por ejemplo) o a los equipos de una misma red local (LAN). Al dividir la red de una organización en varias subredes, los ordenadores pueden utilizar una misma dirección de red para conectarse a Internet. Las mascaras de subred son parecidas a las direcciones IP que normalmente proporcionan los ISP. Una mascara de subred podrá ser, por ejemplo: 255.255.255.0.

Mbps: Abreviatura de Megabits por segundo. Unidad de medida del ancho de banda que define la velocidad a la que se transfiere la información a través de la red o de un cable Ethernet. Un megabyte equivale aproximadamente a 8 mega bits.

Memoria Flash: Tipo de memoria que mantiene los datos incluso después de apagar el dispositivo. La memoria Flash se utiliza como complemento o sustituto de los discos duros en los ordenadores portátiles. En estos casos, la memoria Flash o bien viene integrada en la unidad o puede añadirse mediante una tarjeta PC que se inserta en la ranura PCMCIA.

Modelo de referencia ISO/OSI: Modelo de referencia de interconexión a sistema abierto del Organismo Internacional de Estandarización (ISO). Este tipo de arquitectura estandariza los niveles de servicios y los tipos de interacción de los ordenadores que intercambian información a través de las redes de comunicación. El modelo de referencia ISO/OSI separa las comunicaciones entre ordenadores en siete capas de protocolos, que dependen de los estándares contenidos en los niveles inferiores. La capa más inferior de las siete solo trata las conexiones de hardware mientras que la última se ocupa de las interacciones del software. Se trata de una especie de boceto diseñado para guiar la creación de hardware y software para redes.

Módem: Dispositivo que envía y recibe información de un ordenador a otro.

MPPE: Sigla de Microsoft Point to Point Encryption (Cifrado punto a punto de Microsoft). Medio de cifrado de los paquetes del protocolo punto a punto (PPP).

Multicast (Multidifusion): envía mensajes a un grupo de destinatarios. Un ejemplo de multidifusion será el envío de un mensaje de correo electrónico a los miembros de una lista de correo. La teleconferencia y videoconferencia también serán otras formas de multidifusion, pero requieren redes y protocolos más sólidos.

N

NAT: Sigla de Network Address Translation (traducción de direcciones de red). Procedimiento de conversión de las direcciones IP utilizadas dentro de la red privada y en Internet. Permite compartir una única dirección IP entre todos los ordenadores de la red.

Nombre de host: Nombre DNS de un dispositivo de la red, que se utiliza para simplificar el proceso de localización de ordenadores en una red. Nombre de la red: Nombre dado a un conjunto de ordenadores conectados entre sí formando una red.

Nombre del dominio: dirección de una conexión de red que identifica al propietario con formato jerárquico: servidor.empresa.tipo. Por ejemplo, www.logistic meginter.com identifica el servidor Web de la Empresa Logistic Meginter.

Nombre del ordenador: Nombre que identifica a un único ordenador de la red para que todos sus recursos puedan compartirse con otros ordenadores de la red. No puede haber dos ordenadores con el mismo nombre o nombre de dominio en la red.

P

PAP: Sigla de Password Authentication Protocol (Protocolo de autenticación de contraseñas). Forma más básica de autenticación, en la que el nombre de usuario y la contraseña se transmiten por la red y se comparan con un cuadro de correspondencias de nombre de usuario y contraseña. Normalmente, las contraseñas se guardan en un cuadro cifrado. La función de autenticación básica integrada en el protocolo HTTP se sirve de PAP.

Paquete: Unidad de información que se transmite completa de un dispositivo a otro de la red.

Perfil: Registro de un ordenador que contiene la configuración de software de un usuario de la red y sus datos de identificación.

PING: Protocolo que comprueba si un ordenador está conectado a Internet enviando un paquete a la dirección IP del ordenador y esperando la respuesta.

PPPoE: Sigla de Point-to-Point Protocol over Ethernet (Protocolo punto a punto a través de Ethernet). Especificación que permite a los usuarios de una red Ethernet conectarse a Internet mediante banda ancha, normalmente a través de un módem DSL.

PPTP: Sigla de Point-to-Point Tunneling Protocol (Protocolo canalizado punto a punto). Tecnología desarrollada para la creación de redes privadas virtuales (VPN). Internet es una red abierta y este protocolo se utiliza para garantizar la seguridad de

los mensajes enviados de un nodo a otro de una red privada virtual. Con el PPTP, los usuarios pueden conectarse a la red de su empresa a través de Internet.

Protocolo: Conjunto de reglas que utilizan los ordenadores para comunicarse entre sí a través de la red.

Puertas de enlace del nivel de aplicación (ALG): Aplicaciones como: FTP, TFTP, PPTP y H323, requieren la utilización de módulos ALG específicos para funcionar en la red doméstica. Los paquetes de datos asociados a estas aplicaciones contienen información para su direccionamiento correcto. Las ALG se encargan de controlarlos y asegurarse de que llegan a su destino. El USR8200 Firewall/VPN/NAS viene equipado con una gran variedad de módulos ALG para facilitar un mejor rendimiento de la red doméstica.

Puerto USB: Ranura rectangular de un ordenador en el que se enchufa o inserta el conector USB.

Puerto: conexión física a través de la cual se transmiten los datos entre un ordenador y la red, otro ordenador u otros dispositivos, como el monitor, el módem o la impresora. También es un canal de software para las comunicaciones de la red.

R

Recurso: Cualquier tipo de hardware, como un módem o una impresora, o software, como aplicaciones, archivos o juegos, que los usuarios pueden compartir a través de la red.

Red cliente/servidor: Red compuesta por dos o más ordenadores que dependen de un servidor central para realizar conexiones o acceder a otros recursos del sistema. Esta dependencia del servidor es lo que diferencia a las redes cliente/servidor de las redes entre entidades pares.

Red conmutada: Red de comunicaciones que utiliza switchs o conmutadores para establecer las conexiones entre los diferentes dispositivos.

Red: Conjunto de dos o más ordenadores conectados entre sí por cables o tecnología inalámbrica. Estos ordenadores comparten el acceso a Internet y pueden utilizar los archivos, impresoras y cualquier otro equipo conectado a la red.

Redes entre entidades pares: Red entre dos o más ordenadores que se comunican sin mediación de ningún servidor central. Esta falta de dependencia del servidor diferencia a las redes entre entidades pares de las redes cliente/servidor.

Rendimiento: Velocidad de transferencia de datos de una red que se mide conforme al número de kilobytes transmitidos por segundo.

Restaurar valores predeterminados: Término que se utiliza para describir el proceso de eliminación de la configuración actual del equipo para restablecer la que venía de fábrica. Para ello, basta pulsar el botón Reset (Reinicio) y mantenerlo pulsado durante cinco segundos o un poco más. Hay que tener en cuenta que este proceso es diferente a reiniciar la estación base.

S

Samba: Conjunto de programas que permite compartir de forma ininterrumpida los archivos entre clientes SMB/CIFS.

Seguridad PPTP IP: Conjunto de protocolos desarrollados para realizar un intercambio seguro de paquetes en la capa IP. El protocolo IPSec se ha implantado en gran medida sobre todo en la creación de redes privadas virtuales (VPN).

Servidor virtual: Uno de los múltiples sitios Web que funcionan dentro un mismo servidor. Cada uno dispone de un único nombre de dominio y dirección IP.

Servidor: Ordenador, ofrece recursos compartidos, dispositivos de almacenamiento o capacidad de procesamiento, a los usuarios de la red.

SNTP: Sigla de Simple Network Time Protocol (Protocolo simple de hora de red). Protocolo que permite sincronizar los relojes de los ordenadores clientes con el del servidor a través de Internet.

Static IP address (dirección IP estática): dirección permanente de ordenador en Internet asignada por el ISP.

Subred: Red bien delimitada que forma parte de una red mayor. Las subredes están conectadas a través de routers y pueden compartir una misma dirección de red y la conexión a Internet.

Switch (Conmutador): Dispositivo central que funciona de forma parecida a un concentrador o hub y que se encarga de reenviar cada paquete a un puerto específico en lugar de distribuirlos todos a cada puerto. Resultan muy útiles en redes con un gran tráfico de datos.

T

TCP/IP: Transmission Control Protocol/Internet Protocol (Protocolo de control de transmisión/Protocolo de Internet). Protocolo de red que permite la comunicación entre ordenadores a través de la red o de Internet. Todos los ordenadores de Internet se comunican mediante el protocolo TCP/IP.

U

Unidad: Area de almacenamiento formateada con determinado sistema de archivos y al que se le ha asignado una letra. Esta area de almacenamiento puede ser un disquete (normalmente designado con la letra A), un disco duro (normalmente designado con la letra C) o un CD-ROM (normalmente designado con la letra D) entre otros tipos. Para ver el contenido de una unidad basta hacer clic en el icono en Windows Explorer o Mi PC. La unidad C, también conocida como disco duro, contiene el sistema operativo del ordenador y todos los demás programas instalados. también suele disponer de capacidad suficiente para guardar las carpetas y archivos que cree el usuario.

USB: Universal Serial Bus (Bus de serie universal). Se trata de una interfaz Plug and Play entre el ordenador y los demás periféricos, como reproductores de sonido, joysticks, teclados, teléfonos, escáneres o impresoras. Gracias al USB, los nuevos dispositivos pueden conectarse al ordenador sin necesidad de ninguna tarjeta adaptadora ni de

apagar el ordenador.

UTP: Sigla de Unshielded Twisted Pair (Par trenzado sin blindar) Cable con más de un par de hebras de alambre trenzadas sin ninguna cubierta protectora. Es más flexible y ocupa menos espacio que los cables de par trenzado blindado (STP) pero ofrecen un ancho de banda menor.

V

VPN: Virtual Private Network (Red privada virtual). Como su nombre indica, se trata de una red privada que se sirve de las infraestructuras de telecomunicaciones públicas pero que mantiene su privacidad mediante protocolos de canalizado y otras medidas de seguridad.

W

WAN: Wide Area Network (Red de area extensa). Red que abarca diferentes zonas geográficas y que puede incluir un gran numero de redes locales (LAN).

Bibliografía

[1] Redes de computadoras /Andrew S., Tanenbaum; traducción Elisa Núñez Ramos. México: Pearson Educación, c2003

[2] Redes de computadoras / Cornelio Robledo Sosa. México: IPN, 2002.

[3] Redes de computadoras Internet e interredes / Douglas E. Comer; traducción David Morales Peaje. México: Prentice-Hall Hispanoamérica, 1997.

[4] Redes de computadoras: Protocolos, normas e interfaces / Black, Uyless; Colombia: Alfaomega, c2000

[5] Redes de area local (LAN) / Neil Jenkins, Stan Schatt; traducción de Ricardo de la Barrera Ugalde. México: Prentice-Hall Hispanoamérica, c1996

[6] Redes locales y TCP/IP / José Luís Raya Cabrera, Cristina Raya Pérez. México: Alfaomega, c1997

[7] Redes Privadas Virtuales de Cisco Secure / Andrew G. Mason; traducción KME Sistemas. Madrid: Pearson Education, 2002

[8] IPSec: securing VPNs / Davis Carlton R ebrary, Inc; New York: Obsborne/McGraw Hill, c2001

[9] Check Point NG VPN-1/Firewall-1. / Rockland, Mass.: Syngress, 2003

[10] www.cisco.com/global/ES/solutions/ent/avvid solutions/vpn home.shtml [11] www.ugr.es/informatica/redes/vpn/vpn.htm

[12] www.microsoft.com/../windowsserver2003/es/library/serverhelp/b7ab88e6-9a6b 408a-a57b

[13] www.cisco.com/global/LA/productos/sol/emp/grandes/seguridad.shtml

[14] www.es.wikipedia.org/wiki/Red privada virtual