Universidad Autónoma del Estado de Hidalgo

Instituto de Ciencias Básicas e Ingeniería

Licenciatura en Ingeniería en Electrónica y Telecomunicaciones

Redes Privadas Virtuales

MONOGRAFÍA

Que para obtener el título de
Ingeniero en Electrónica y Telecomunicaciones

PRESENTA

P.D.L.I.E.T. Alexandro González Morales

Asesora: Ing. Sandra Luz Hernández Mendoza

Pachuca, Hidalgo; Mayo de 2006

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA

P.D.L.I.E.T. ALEXANDRO GONZÁLEZ MORALES
P R E S E N T E

Por este conducto le comunico que el Jurado que le fue asignado a su trabajo de titulación denominado **"REDES PRIVADAS VIRTUALES"**, y que después de revisarlo en reunión de sinodales han decidido autorizar la impresión, hechas las correcciones que fueron acordadas.

A continuación se anotan las firmas de conformidad de los integrantes del Jurado:

PRESIDENTE:	M. en C. Elías Varela Paz	_____
PRIMER VOCAL:	Ing. Sandra Luz Hernández Mendoza	_____
SEGUNDO VOCAL:	Ing. Alejandro Ayala Espinoza de los Monteros	_____
TERCER VOCAL:	Lic. Ángel Martínez Rodríguez	_____
SECRETARIO:	Lic. Clara Mercado Jarillo	_____
PRIMER SUPLENTE:	Ing. Arturo Austria Cornejo	_____
SEGUNDO SUPLENTE:	Ing. Jaime Barrera Rodríguez	_____

Sin otro particular, reitero a usted la seguridad de mi atenta consideración.

ATENTAMENTE
"AMOR, ÓRDEN Y PROGRESO"
Pachuca de soto, Hgo., a 27 de Marzo de 2006

_____
M. en C. Elías Varela Paz
Coordinador adjunto de la Lic. en Ingeniería en Electrónica y Telecomunicaciones

C.c.p. Integrantes del jurado.
" Expediente

Universidad Autónoma del Estado de Hidalgo
Instituto de Ciencias Básicas e Ingeniería
Ciudad Universitaria Carretera Pachuca - Tulancingo Km. 4.5 C.P. 42184
Col. Carboneras Mineral de la Reforma Hidalgo.
Tel. 017717172000 Ext. 6302 Fax ext. 6318
Edificio "D" del ICBI. Extensión de la coordinación: 6320
correo electrónico: evarela@uaeh.reduaeh.mx

A mis padres, por su apoyo a lo largo de mi vida

Agradecimientos

La realización de esta monografía no hubiera podido ser llevada a cabo sin el apoyo de las siguientes personas:

- Mis padres, que me dieron consejos sobre cómo organizarme para realizar este trabajo.
- La Ing. Sandra Luz Hernández que me orientó acerca del contenido de la monografía.
- Los integrantes del jurado, los cuales hicieron las correcciones necesarias
- Los profesores que impartieron clases relacionadas con las redes de telecomunicaciones, ya que de ahí nació mi interés sobre este tema.
- Mis amigos de la Universidad, con los cuales estudié y juntos pudimos aclarar muchas dudas acerca de los temas de esta carrera.

A todos ellos, mis más sinceros agradecimientos.

Redes Privadas Virtuales (VPN)

Índice de temas

Índice de figuras

Capítulo 1

Capítulo 2

Capítulo 3

Capítulo 4

Índice de tablas

Capítulo 1

Capítulo 2

Capítulo 3

Capítulo 4

Objetivo general

El objetivo de esta monografía es que el lector conozca los fundamentos de las Redes Privadas Virtuales (VPN), las bases de su funcionamiento y la importancia que tienen en muchas organizaciones hoy en día.

Objetivos específicos

- Definir qué es una red privada virtual
- Describir la importancia de las redes privadas virtuales
- Explicar como funciona una red privada virtual
- Explicar como se configura una red privada virtual

Justificación

El ser humano se encuentra en la llamada era de la Información. Mientras que en el pasado las únicas tecnologías para realizar comunicaciones eran el telégrafo y más tarde el teléfono, a partir de la segunda mitad del siglo XX, la computadora se ha convertido en el medio favorito para poder comunicarse.

Todo tipo de organizaciones, ya sea empresas grandes y pequeñas, universidades, institutos, gobierno, etc., requieren de métodos para poder transmitir información de forma rápida, eficiente, segura y a un precio razonable. Esto lleva al desarrollo continuo de tecnologías de la información y actualización de las ya existentes con el fin de satisfacer las necesidades de dichas organizaciones en este mundo globalizado.

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 implementar 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.

Introducción

La época en que vivimos se caracteriza por la creación y la implementación de toda clase de tecnologías de la información. Las necesidades de las empresas y organizaciones motivaron la creación de redes LAN, WAN, intranets y extranets y, por supuesto, Internet. Las corporaciones conectan su oficina central con sus sucursales utilizando diversos tipos de conexiones WAN. También instalan infraestructura para poder permitir el acceso a usuarios remotos. Ahora bien, el problema es que establecer y mantener una red privada de esa manera resulta la mayor parte de las veces algo muy costoso. La cuestión es ¿cómo reducir los costos de una WAN?

Si crear una red privada resulta ser muy caro, entonces podría pensarse que, puesto que las redes públicas resultan ser más económicas sería buena idea montar la red privada de una compañía en una red pública. Esto puede parecer una buena idea, pero está el problema de la seguridad. Una red pública como Internet está infestada de muchos usuarios malintencionados. La única forma de lograr que una red pública sea segura es utilizando métodos que garanticen el envío confidencial de los datos.

Así pues, se requiere una tecnología que permita el envío seguro y confidencial de los datos de una red privada a través de una red pública. ¿Qué tecnología realiza eso? La respuesta: Redes Privadas Virtuales (VPN, *Virtual Private Networks*).

La presente monografía se dedica a analizar de forma general a las VPN, sus características y funcionamiento, así como las tecnologías que utiliza para enviar los datos de forma segura a través de una red pública. Las VPN están cobrando cada vez mayor popularidad debido a las grandes ventajas que ofrece.

Debido a que no existe un estándar en la industria de las telecomunicaciones respecto a las VPN, el término se ha prestado ha diferentes interpretaciones, y en

ocasiones genera confusión, puesto que cada fabricante de dispositivos VPN o cada proveedor de servicios VPN ofrece soluciones que muchas veces difieren de sus competidores y en ocasiones hasta resultan contradictorias.

Al principio el término VPN se refería las tecnologías que se instalaban en redes ATM o *Frame Relay*. En la actualidad el término se aplica más a las redes IP. Y debido a que Internet es la red IP por excelencia, además de los reducidos costos económicos y de mantenimiento, el término VPN se está aplicando por lo general a las redes privadas que operan sobre Internet.

La seguridad es el aspecto más importante en una VPN. Debido a que se trata de información privada de las corporaciones circulando a través de una red pública, es necesario el uso de fuertes métodos de encriptación y autenticación de los datos con el fin de lograr el envío seguro de la información.

1

Fundamentos de las VPN

En este primer capítulo se da una breve introducción a las redes de computadoras y después se centra en lo que son las tecnologías WAN y el acceso remoto, los cuales son conceptos fundamentales en el mundo de las VPN.

1.1 Redes de computadoras

1.1.1 Definición de red de computadoras

Una red de computadoras es un grupo de computadoras interconectadas entre sí las cuales comparten información y recursos. La interconexión se puede realizar de diferentes maneras, ya sea cable de cobre, fibra óptica, rayos infrarrojos o microondas. Los recursos y la información que se pueden compartir pueden ser los siguientes:

- Archivos
- Aplicaciones
- Correo electrónico
- Impresoras[13]

Las redes de computadoras ofrecen muchas ventajas. Sin ellas todo el envío de la información tendría que hacerse de forma manual, por medio de diskettes o CDs. Esto haría el proceso algo muy lento. Con las redes no sólo se puede intercambiar información a nivel local, sino también a grandes distancias incluso mundiales y de forma instantánea.

1.1.2 Clasificación de las redes de computadoras

El mundo de las redes de computadoras es muy complejo, por lo que es necesario clasificarlas para facilitar su estudio, ya que existen muchos tipos de redes. Las redes pueden ser clasificadas en cuanto a cobertura, topología y propiedad.

1.1.2.1 Cobertura

La clasificación de las redes en cuanto a cobertura se refiere a la extensión que tiene una red dentro de un área geográfica. Utilizando este criterio, las redes de computadoras se pueden clasificar de acuerdo a la tabla 1.1: [21]

Distancia entre procesadores	Procesadores ubicados en el mismo	Clasificación
1 m	Metro cuadrado	Red de Área Personal (PAN)
10 m	Cuarto	Red de Área Local (LAN)
100 m	Edificio	
1 km	Campus	Red de Área Campus (CAN)
10 km	Ciudad	Red de Área Metropolitana (MAN)
100 km	País	Red de Área Amplia (WAN)
1000 km	Continente	
10000 km	Planeta	Internet

Tabla 1.1 *Clasificación de las redes en cuanto a cobertura*

Sin embargo, esencialmente las redes pueden clasificarse simplemente como Redes de Área Local (que abarcan desde un cuarto hasta un campus) y Redes de Área Amplia (que abarcan distancias mayores a un campus hasta abarcar todo el planeta). Resulta más práctico clasificarlas solamente así al momento de describir las tecnologías y dispositivos de redes.

Red de Área Local (LAN). Es aquella red donde todas las computadoras conectadas en red están dentro de una habitación, un edificio e incluso varios edificios dentro de una localidad pequeña. Las LAN realizan lo siguiente:

- Operan dentro de una zona geográfica limitada
- Permiten a los usuarios acceder a medios de gran ancho de banda
- Proporcionan conectividad de tiempo completo a los servicios locales
- Conectan físicamente dispositivos adyacentes

Las principales tecnologías LAN son las siguientes:

- Ethernet

- Token Ring
- FDDI [2]

Siendo *Ethernet* la más popular y más difundida de todas ellas.

Una LAN puede intercomunicarse por medio de un cableado que transmita señales punto a punto; o bien, por medio de una zona de influencia de un punto de acceso (*access point*) inalámbrico. La velocidad que se puede alcanzar en este tipo de red abarca desde los 10 Mbps hasta los 10 Gbps y se están desarrollando normas para 40 Gbps, 100 Gbps y 160 Gbps. [13]

Red de Área Amplia (WAN). Es aquella red que está formada por la interconexión de varias LAN. Una WAN abarca una gran área geográfica de varios kilómetros. Las WAN son útiles cuando los usuarios de una red necesitan acceder a los recursos de otra red. Esto ocurre por ejemplo cuando las oficinas principales de una compañía necesitan utilizar recursos de la red que se encuentra en alguna de sus fábricas ubicada a varios kilómetros de distancia. Las WAN realizan lo siguiente:

- Operan sobre grandes áreas geográficamente separadas
- Permiten que los usuarios mantengan comunicación en tiempo real con otros
- Proporcionan acceso a los recursos remotos de una LAN
- Ofrecen servicios de correo electrónico, web, transferencia de archivos y comercio electrónico

Las principales tecnologías WAN son:

- Módems
- Red Digital de Servicios Integrados (RDSI)
- Línea de Abonado Digital (DSL, *Digital Suscriber Line*)
- Frame Relay
- Modo de Transferencia Asíncrono (ATM, *Asynchronous Transfer Mode*)

- Portadoras T1, E1, etc
- Red Óptica Síncrona (SONET, *Synchronous Optical Network*) [2]

En la figura 1.1 se pueden observar distintas redes LAN conectadas a una red WAN que puede utilizar diferentes tecnologías.

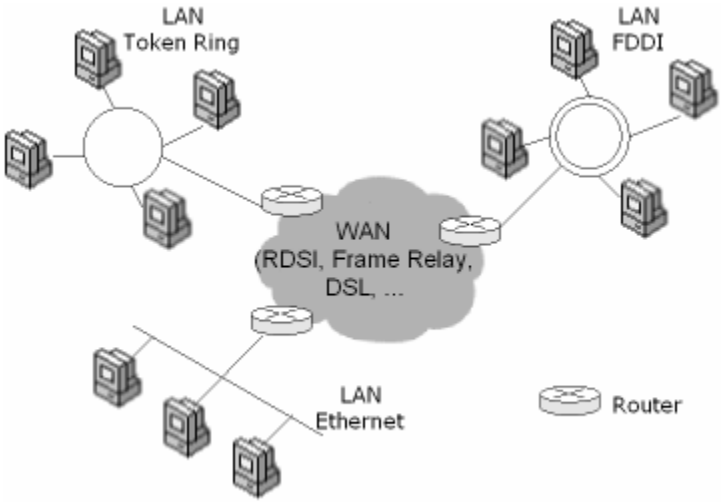

Figura 1.1 *LAN y WAN*

1.1.2.2 Topología

En cuanto a la topología, como se muestra en la figura 1.2, existen básicamente cuatro tipos de redes de las cuales se desprenden varias combinaciones. Estas topologías son:

- Red tipo bus
- Red tipo estrella
- Red tipo anillo
- Red tipo malla
- Red tipo híbrida

Red tipo bus. En esta topología se utiliza un cable o serie de cables como eje central al cual se conectan todas las computadoras. En este conductor se efectúan todas las comunicaciones entre las computadoras. Esta red conviene usarse si no son muchas las computadoras que se van a conectar. [13]

Red tipo estrella. Se caracteriza por tener un núcleo del cual se desprenden líneas hacia varias terminales. Fueron las primeras en utilizarse en el mundo de la computación. Esta topología es útil cuando se tiene una computadora central muy potente rodeada de máquinas de menor potencia. Esta topología es la más común porque es la que más utilizan las redes *Ethernet*. [13] [2]

Red tipo anillo. Aquí también se utiliza un bus como eje central para conectar todos los equipos, sin embargo, dicho bus forma un anillo. Esta topología es utilizada en redes *Token Ring* y FDDI además de que es favorecida por los principales proveedores de acceso a Internet. [13]

Red tipo malla. En esta topología, todos los dispositivos o algunos de ellos son conectados con todos los demás con el fin de conseguir redundancia y tolerancia a fallos. Si un enlace falla, la información puede fluir por otro enlace. Las redes de malla suelen implementarse solamente en redes WAN. [2]

Red tipo híbrida. La topología híbrida es una red que utiliza combinaciones de las topologías anteriores.

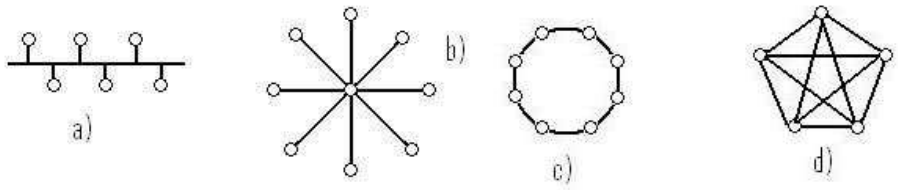

Figura 1.2 *Topología de redes: a) Bus b) Estrella c) Anillo d) Malla*

1.1.2.3 Propiedad

La clasificación de las redes en cuanto a propiedad se refiere a la forma de administración de la red. Así pues, como se muestra en la figura 1.3, las redes de computadoras se pueden clasificar de la siguiente forma:

- Redes privadas
- Redes públicas

Red privada. Es aquella red exclusiva de una sola compañía u organización en particular. La información no se comparte con otras compañías u organizaciones. En una red privada la información estará protegida, se podrá controlar el uso que se le da a la red y se podrá predecir el ancho de banda disponible. [5]

Red pública. Es una red a través de la cual circula información de muchas compañías y organizaciones. Una red pública siempre será menos segura que una red privada, pero resultan ser más económicas y no se requiere que un administrador de red local de mantenimiento a una de estas redes. Como ejemplo de red pública tenemos a Internet. [5]

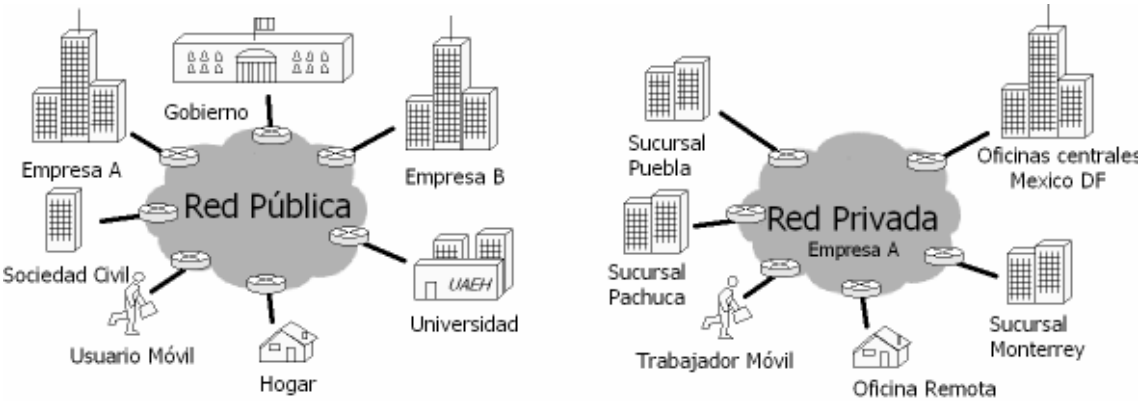

Figura 1.3 *Red pública y red privada*

1.1.3 Componentes de una red de computadoras

Una red de computadoras consta de varios equipos necesarios para el correcto funcionamiento de la red. Entre los componentes de una red podemos encontrar el cableado y dispositivos de red como aparece en la figura 1.4.

1.1.3.1 Sistema de cableado

Éste se refiere al medio físico que se usa para conectar entre sí las estaciones de trabajo de los usuarios y con otros dispositivos o nodos de la red para lograr un intercambio de información. La elección del sistema de cableado depende de varios factores, como los que se mencionan a continuación:

- Tipo de ambiente donde se va a instalar
- Tipo de equipo por conectar
- Tipo de aplicación y requerimiento
- Capacidad económica (relación costo/beneficio)

Se utilizan tres tipos de cables para instalar redes de cómputo, de los cuales los dos primeros son alámbricos y el tercero es óptico:

- Par trenzado
- Cable coaxial
- Fibra óptica.

El cable par trenzado es el medio de transmisión más utilizado actualmente. Se trata cuatro pares de dos conductores de cobre forrados con plástico, torcidos entre sí y protegidos por una cubierta de plástico. Existen dos clases de par trenzado: el UTP, que es el que más se usa y que tiene diferentes categorías que van desde la categoría 3 hasta la 7 con velocidades desde 10 Mbps hasta 1 Gbps y el STP, el cual tiene mayor resistencia al ruido y del cual hay cuatro tipos diferentes.

El cable coaxial es utilizado cada vez menos debido al auge del UTP. Existen dos tipos de cable coaxial: el delgado, el cual tiene un grosor de 6 mm. y puede transportar señales a distancias de hasta 185 m. y el grueso, el cual tiene un diámetro de 12 mm. y puede transportar señales a distancias de hasta 500 m.

La fibra óptica consiste en un núcleo central muy delgado de vidrio con alto índice de refracción de la luz. Alrededor del núcleo hay un revestimiento de vidrio pero con un índice de refracción más bajo que protege al núcleo de contaminación. La fibra óptica posee un ancho de banda muy grande y poca pérdida de señal, lo que las hace ideales para transmitir un gran volumen de datos y a grandes distancias. La desventaja es que su instalación es muy costosa todavía. [6]

1.1.3.2 Dispositivos de interconexión de redes

Los dispositivos de interconexión de redes conectan a los dispositivos terminales de redes para formar la red y controlar el flujo de la información. Estos son:

- Concentrador (*hub*)
- Conmutador (*switch*)
- Enrutador (*router*)

Concentrador o *hub*: Es un dispositivo que conecta varios cables de red que llegan desde computadoras cliente a la red. Existen concentradores de diferente tamaño en los cuales se puede conectar desde dos computadoras hasta más de 60 equipos. La información que llega al nodo de un *hub* es retransmitida a todos los demás nodos conectados a este equipo, lo que puede afectar el desempeño de una red.

Conmutador o *switch*: Se trata de un dispositivo que conmuta de forma dinámica sus distintos puertos para crear las conexiones. Un *switch* es un equipo semejante a un *hub* con la diferencia de que todas las conexiones de red tienen su propio dominio de colisión, esto hace que cada conexión de red sea privada, lo cual incrementa el desempeño de una red.

Enrutador o *Router:* Es un equipo que direcciona los paquetes de datos de una red a otra. Las dos redes se conectan al *router* usando sus propios cableados y tipos de conexión. Este dispositivo puede determinar cuál es la ruta más corta de un paquete hacia su destino, además de que también pueden optimizar el ancho de banda de la red y ajustarse de manera dinámica a problemas de patrones de tráfico cambiantes dentro de la red. Para que un *router* funcione de manera correcta, necesita ser programado, esto se puede realizar conectando una PC a una terminal del *router* y utilizando algún software de terminal o un programa en modo gráfico. [5]

1.1.3.3 Dispositivos terminales de redes o de usuario final

Los dispositivos terminales de redes o de usuario final son aquellos que son conectados por los dispositivos de interconexión de redes y son los puntos finales de una red que transmiten o envían la información. Estos dispositivos son:

- Estación de trabajo (*host*)
- Servidor
- Tarjeta de Interfaz de Red (NIC)

Estación de trabajo. Son las computadoras que componen la red. Permiten a los usuarios crear, compartir y obtener información. A las estaciones de trabajo también se les denomina *hosts* y el término incluye a las impresoras en red.

Servidor. Es aquella computadora que proporciona funciones o servicios a otras computadoras. Existen diferentes tipos de servidores de acuerdo a la función que realizan como servidores de archivos, de red, de acceso remoto, de Internet, etc.

Tarjeta de Interfaz de Red (NIC, *Network Interface Card).* Es un dispositivo electrónico que permite a un ordenador o impresora acceder a una red y compartir recursos entre dos o más equipo. [36][15]

Figura 1.4 *Componentes de una red de computadoras*

1.2 El modelo OSI

1.2.1 Definición del modelo OSI

El modelo OSI (Sistemas Abiertos de Interconexión) define los métodos y protocolos necesarios para lograr la comunicación entre los equipos en una red. Fue desarrollado por la Organización Internacional de Estandarización (ISO) con el fin de proporcionar un modelo de referencia para la normalización y quedó definido en la norma ISO 7498.

El modelo divide las funciones en un conjunto jerárquico de capas. Cada capa realiza un conjunto de tareas necesarias para lograr la comunicación con otros sistemas. Cada capa se sustenta en la inmediatamente inferior, la cual realiza funciones más primitivas ocultando los detalles a las capas superiores. El modelo define en términos generales las funciones que se deben realizar en cada capa. El modelo OSI consta de siete capas, e idealmente, cada sistema debe poseer las siete capas. Estas capas se muestran en la figura 1.5.

Figura 1.5 *Las siete capas del modelo OSI*

1.2.2 Las capas del modelo OSI

1.2.2.1 Capa física

La capa física se encarga de la interfaz física entre los dispositivos, así como las reglas que rigen la transmisión de los bits. Esta capa tiene cuatro características importantes:

- Mecánicas
- Eléctricas
- Funcionales
- De procedimiento

Las características mecánicas definen las propiedades físicas de la interfaz con el medio de transmisión, como por ejemplo la especificación del conector que transmite las señales a través de los conductores. Las características eléctricas especifican la forma en como se representan los bits, tales como niveles de voltaje, así como su velocidad de transmisión. Las características funcionales especifican las funciones que realiza cada uno de los circuitos de la interfaz física entre el sistema y el medio de transmisión. Por último, las características de procedimiento definen la secuencia de eventos que se llevan a cabo en el intercambio del flujo de bits a través del medio físico.

1.2.2.2 Capa de enlace de datos

La capa de enlace de datos proporciona los medios para activar, mantener y desactivar el enlace, así como intentar hacer que el enlace físico sea fiable. Uno de los principales servicios de esta capa es proporcionar detección y corrección de errores. Los elementos de información que circulan por esta capa se denominan tramas. En la mayor parte de los sistemas, los controladores de las NIC realizan el trabajo de esta capa.

Esta capa se divide normalmente en dos subcapas las cuales son LLC (Control de Enlace Lógico) y MAC (Control de Acceso a Medios). LLC realiza establecimiento y terminación de conexión, además de la transferencia de datos. MAC controla el ensamble y fragmentación de tramas, detección y corrección de errores, y direccionamiento. Los protocolos MAC más importantes son:

- 802.3 Ethernet
- 802.5 Token Ring
- 802.7 Banda Ancha
- 802.11 Inalámbrico
- 802.12 100BaseVBG [20]

1.2.2.3 Capa de red

La capa de red realiza la transferencia de información entre sistemas finales a través de algún tipo de red de comunicación. Aquí es donde se define la forma en que los paquetes llegan de un punto a otro dentro de una red y lo que lleva cada paquete. Esta capa define distintos protocolos de transmisión de paquetes. Estos protocolos definen las direcciones fuente y destino. Además, en esta capa se realizan las funciones de conmutación y enrutamiento de los paquetes. Los protocolos más importantes de esta capa son IP, IPX, *AppleTalk* y NetBIOS. [20][5]

1.2.2.4 Capa de transporte

En la capa de transporte se proporciona un mecanismo para intercambiar datos entre sistemas finales. El servicio de transporte orientado a conexión asegura que los datos se entregan libres de errores, en orden y sin pérdidas ni duplicaciones. En esta capa se realiza también una optimización de los servicios de red. Algunos de los protocolos de transporte son TCP y UDP. [20]

1.2.2.5 Capa de sesión

Esta capa proporciona los mecanismos para controlar el diálogo entre las aplicaciones de los sistemas finales, es decir, se define la conexión de un usuario en un servidor de red o desde un punto de una red hasta otro punto. Estas conexiones virtuales se conocen como sesiones e incluyen la negociación entre el cliente y el anfitrión, la transferencia de información del usuario y la autenticación en la red. [20][5]

1.2.2.6 Capa de presentación

La capa de presentación se encarga de definir el formato de los datos que se intercambian entre las aplicaciones y además ofrece un conjunto de servicios para transformar dichos datos. En esta capa se define la sintaxis utilizada entre las aplicaciones y proporciona los medios para seleccionar y modificar la representación utilizada. Las funciones que se realizan en esta capa pueden incluir el cifrado y la compresión de los datos. [5]

1.2.2.7 Capa de aplicación

Esta capa proporciona a los programas de aplicación los medios necesarios para que accedan al entorno OSI, es decir, controla la forma en que el sistema operativo y sus aplicaciones interactúan con la red. En esta capa se encuentran las aplicaciones dedicadas a la transferencia de archivos (FTP), el correo electrónico (SMTP), el acceso remoto, etc. [20]

1.3 Protocolo TCP/IP

El Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP, *Transmission Control Protocol/Internet Protocol*) es un conjunto de protocolos que permiten la comunicación a través de varias redes diferentes. TCP/IP fue creado por el Departamento de Defensa de Estados Unidos y se diseñó porque se quería un protocolo que fuera capaz de transmitir información en cualquier momento y bajo cualquier condición. Este protocolo tan popular dio origen a Internet, el cual ha posibilitado la interconexión de toda clase de redes a nivel mundial. [2]

1.3.1 El modelo TCP/IP

TCP/IP fue diseñado en base un modelo de cuatro capas. Este modelo precedió al modelo OSI y fue muy importante. Aunque los nombres de algunas capas del modelo TCP/IP son iguales a las del modelo OSI no se debe confundirlas. Las funciones que realizan son diferentes. Estas capas se muestran en la figura 1.6.

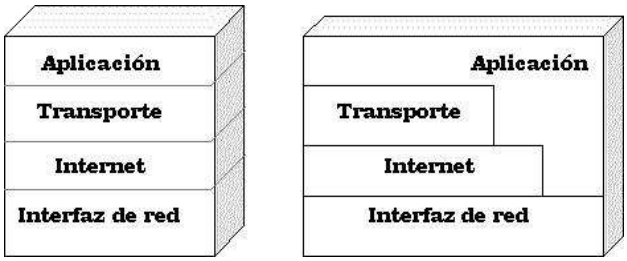

Figura 1.6 *Las cuatro capas del modelo TCP/IP*

1.3.1.1 Las capas del modelo TCP/IP

Capa de aplicación. Esta capa proporciona servicios que pueden ser utilizados por otras aplicaciones utilizadas para acceso remoto, correo electrónico, transferencia de archivos y administración de la red. La capa de aplicación de TCP/IP utiliza servicios de las tres capas superiores del modelo OSI (aplicación, presentación y sesión). Como podemos apreciar en la figura 1.7, TCP/IP no utiliza una estructura de capas rígida, ya que la capa de aplicación puede operar

directamente sobre las capas de transporte, Internet y red. Los protocolos de la capa de aplicación son los siguientes: [11]

- Protocolo de Transferencia de Hipertexto (HTTP, *HyperText Transfer Protocol*)
- Protocolo Trivial de Transferencia de Archivos (TFTP, *Trivial File Transfer Protocol*)
- Protocolo de Transferencia de Archivos (FTP, *File Transfer Protocol*)
- Sistema de Archivos de Red (NFS, *Network File System*)
- Protocolo Simple de Transferencia de Correo (SMTP, *Simple Mail Transfer Protocol*)
- Emulación de Terminal (Telnet)
- Protocolo Simple de Administración de Redes (SNMP, *Simple Network Management Protocol*)
- Sistema de Nombres de Dominio (DNS, *Domain Name System*)

Capa de transporte. La capa de transporte se encarga de controlar las conexiones lógicas entre las computadoras o *hosts*. Los protocolos de esta capa segmentan y reensamblan los datos que las aplicaciones de la capa superior envían. Los protocolos de la capa de transporte son los siguientes:

- Protocolo de Control de Transmisión (TCP, *Transmission Control Protocol*)
- Protocolo de Datagrama de Usuario (UDP, *User Datagram Protocol*) [2]

Capa de Internet. Gestiona la transferencia de información a lo largo de varias redes mediante el uso de *routers*. La capa de Internet de TCP/IP es equivalente a la capa de red del modelo OSI, ya que se encarga de la transferencia de paquetes entre computadoras conectadas a distintas redes. En esta capa se determina la mejor ruta a seguir y la conmutación de paquetes. Los protocolos de la capa de Internet son los siguientes: [11]

- Protocolo de Internet (IP, *Internet Protocol*)
- Protocolo de Mensajes de Control en Internet (ICMP, *Internet Control Message Protocol*)

- Protocolo de Resolución de Direcciones (ARP, *Address Resolution Protocol*)
- Protocolo de Resolución Inversa de Direcciones (RARP, *Reverse Address Resolution Protocol*) [2]

IP es un protocolo que funciona en la capa de red del modelo OSI el cual define la forma en que se asignan las direcciones a los datos que van del origen hasta el destino y la secuencia en que los datos deben ser reensamblados en el otro extremo de la transmisión. En la figura 1.7 se puede apreciar la forma en que está estructurado un datagrama IP. [5]

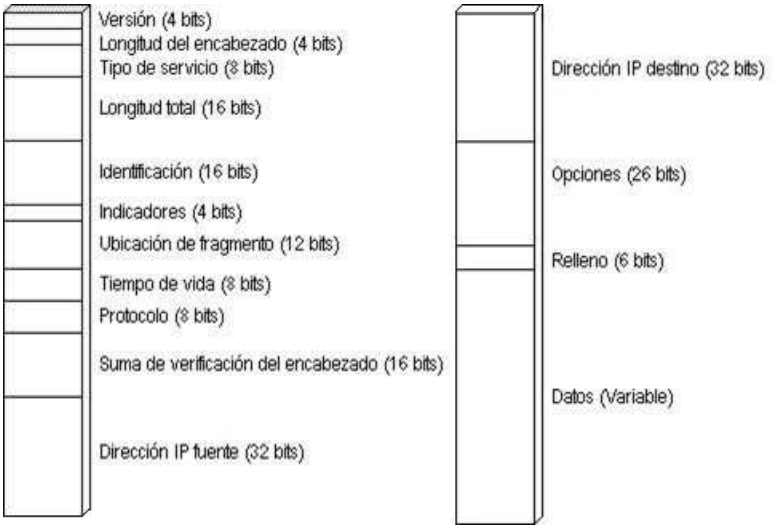

Figura 1.7 *Estructura de un datagrama IP*

Capa de interfaz de red. Se encarga de todo lo relacionado con la transferencia de paquetes dependientes de la red. Realiza funciones que pertenecen a parte de la capa de enlace de datos y la capa física del modelo OSI. Se ocupa de los métodos utilizados para que un paquete IP pueda obtener un enlace físico con el medio de red. Los protocolos de la capa de interfaz de red son: [11]

- Tecnologías LAN (Ethernet, Fast Ethernet, FDDI)
- Tecnologías WAN (ATM, Frame Relay)
- Protocolo Punto a Punto (PPP, *Point-to-Point Protocol*)
- ARP y RARP [2]

1.4 Acceso remoto y conexiones WAN

1.4.1 Internet, intranets y extranets

Internet es una red de redes que ha proporcionado muchas ventajas a toda clase de organizaciones. A las empresas les aporta muchos beneficios económicos el hecho de conectarse a Internet y poder realizar ahí toda clase de negocios. Las corporaciones han descubierto también que llevar la tecnología sobre la cual se basa Internet a sus propias redes privadas les trae muchos beneficios a todos sus usuarios, de ahí el surgimiento de las intranets. Finalmente, las empresas requieren estar conectadas con sus socios y clientes, por lo que pronto surgen las extranets. Internet, intranet y extranet son conceptos muy importantes en el mundo de las VPN y no puede hablarse de una VPN sin antes conocer en qué consisten dichos conceptos.

1.4.1.1 Internet

Internet conecta decenas de millones de computadoras en todo el mundo, permitiéndoles comunicarse entre sí y compartir recursos. Internet es una colección de redes organizada en una estructura multinivel las cuales usan toda una variedad de tecnologías para interconectarse. En el nivel más bajo se encuentra algunas decenas o cientos de computadoras conectadas a un *router*, formando una LAN. Otras computadoras se conectarán a un *router* a través de la red telefónica usando un módem. Una empresa o universidad podrá tener varios *routers* enlazados a un *router* principal. Estos *routers* se encuentran conectados mediante líneas alquiladas a un router de un Proveedor de Servicios de Internet (ISP, *Internet Service Provider*). A su vez, el proveedor conecta sus *routers* a una WAN de alta velocidad llamada *backbone*. Un país puede tener varios *backbones* que conectan a todos los ISP. Finalmente, los *backbones* de todos los países se interconectan en una malla usando líneas internacionales. Todo esto es lo que finalmente forma Internet.

La base de Internet es TCP/IP. El éxito de las redes basadas en IP se debe precisamente a Internet. Dos conceptos definen la tecnología de Internet: los paquetes y la forma de direccionamiento.

Paquetes. Internet transporta toda la información en unidades llamadas paquetes. Un paquete consta de dos partes: la información que contiene, la cual se llama carga útil y la información acerca de la información, llamada cabecera. La cabecera contiene información acerca de las direcciones origen y destino, longitud de los datos y tipo de éstos. [10]

Direccionamiento. Las direcciones de la cabecera permiten el envío de la información a través de Internet. Los *routers* se encargan de realizar esto. Los paquetes recorren diferentes caminos para llegar a su destino y eventualmente pueden ser almacenados dentro del *router*. [10]

1.4.1.2 Intranet

Una intranet es una Internet orientada a una organización en particular. Los servidores *web* intranet difieren de los servidores *web* públicos en que estos últimos no tienen acceso a la intranet de la empresa sin los permisos y las contraseñas adecuadas. Una intranet está diseñada para que accedan a ellas sólo los usuarios con los debidos permisos de acceso a una red interna de una empresa. Una intranet reside dentro de un *firewall* y éste impide el acceso a los usuarios no autorizados. [2]

1.4.1.3 Extranet

Una extranet es una intranet orientada a las personas u organizaciones que son externas a su empresa, pero necesitan acceder a alguna información, así se les permite el acceso a este contenido adicional, siempre bajo un sistema de autenticación y control de acceso. [66]

La diferencia entre una intranet y una extranet es el método de acceso, siendo similares en cuanto a las facilidades y funciones, el tipo de recurso que utiliza y su filosofía general, de proporcionar acceso fácil, rápido y seguro a la información requerida.

El concepto extranet nace cuando una empresa quiere dar acceso a unas determinadas personas o grupos de personas a una determinada información de su intranet. Sin hacerla pública, la hace accesible a otras personas que puedan necesitarla o con quien mantienen relaciones comerciales. El ejemplo más claro es la accesibilidad que una empresa da a una parte de sus clientes o proveedores. [66]

1.4.2 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.

1.4.2.1 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. [57]

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

De acuerdo a la figura 1.8, existen diferentes tipos de usuarios dependiendo de 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 clasificados 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. [5]

Usuarios de oficina remota. Son aquellos que acceden a la red corporativa desde una ubicación fija distante como puede ser una pequeña oficina o el hogar. El teletrabajo 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. [5] [4] [37]

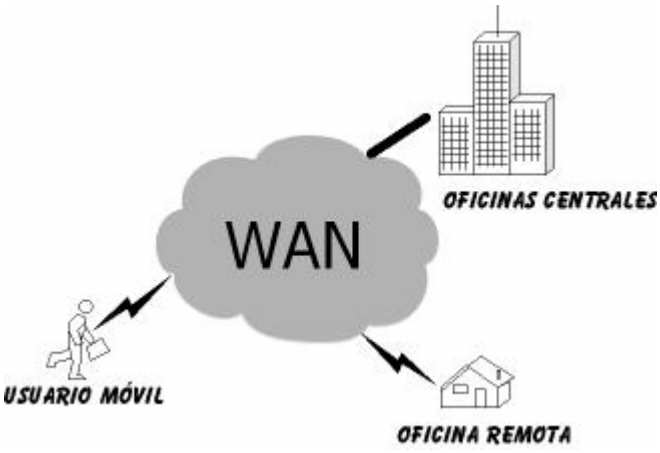

Figura 1.8 *Acceso remoto*

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, el siguiente paso 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.

1.4.2.2 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 hacía una llamada para estar en conexión con la red corporativa. En redes donde

no hay muchos usuarios remotos se pueden agregar sólo 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 1.9. [5]

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. [19] [23]

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.

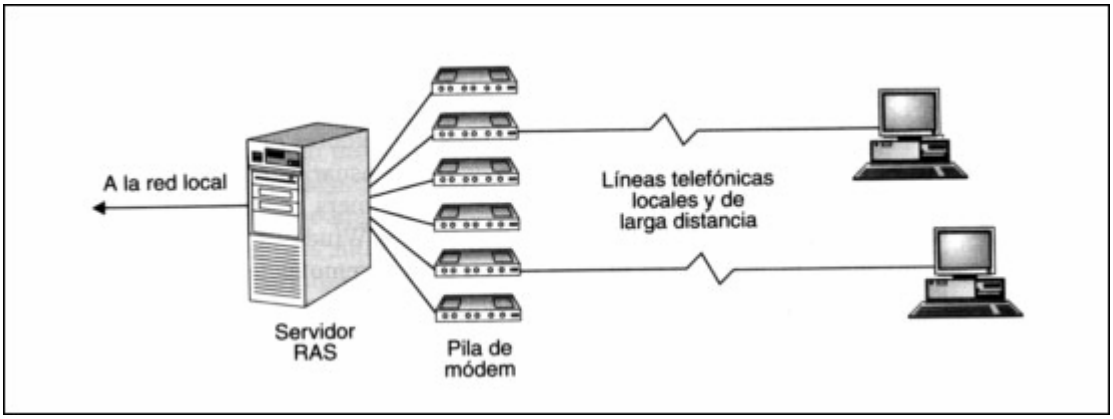

Figura 1.9 *Acceso remoto sin una VPN* [53]

1.4.3 Conexiones WAN

Existen diversas tecnologías o conexiones para poder unir diferentes LAN y crear una WAN. Un enlace WAN puede ser conmutado o dedicado. Por conmutado se entiende que es aquel que no está disponible todo el tiempo, la conexión se establece sólo cuando es necesaria. Un ejemplo de esto es una conexión de acceso telefónico a redes a través de un módem. Por otra parte, un enlace dedicado es aquel donde la conexión siempre estará disponible, incluso cuando no se esté utilizando. Como ejemplo podemos mencionar una conexión que utiliza tecnología xDSL. Las conexiones WAN se pueden clasificar de la siguiente manera: [5]

- Servicios de conmutación de circuitos
- Servicios de conmutación de paquetes
- Servicios de conmutación de celdas
- Servicios digitales dedicados
- Servicios de marcación, cable e inalámbricos

1.4.3.1 Servicios de conmutación de circuitos

La conmutación de circuitos es un método en el que se establece, mantiene y termina un circuito físico dedicado a través de una red de proveedor para cada sesión de comunicación. Los servicios de circuitos conmutados utilizan Multiplexación por División del Tiempo (TDM) y son síncronos (utilizan STM). Los dos servicios de circuitos conmutados son POTS y RDSI.

Servicio Telefónico Analógico Convencional (POTS, *Plain Old Telephone Service).* Se trata de la red telefónica, también llamada Red Pública Telefónica Conmutada (PSTN, *Public Switched Telephone Network*). Aunque no es propiamente un servicio de datos de computadora, muchas de sus tecnologías son parte de la creciente infraestructura de datos y es una red de telecomunicaciones fiable, fácil de usar y de área amplia. [2]

Red Digital de Servicios Integrados (RDSI o ISDN, *Integrated Services Digital Network).* Se trata del primer servicio de conexión telefónica digital. Es un sistema diseñado para integrar voz y datos en una sola conexión. Existen dos tipos principales de RDSI:

- Interfaz de servicio básico (BRI)
- Interfaz de servicio primario (PRI)

La interfaz de servicio básico (BRI) es una conexión que se puede tener en cualquier hogar o pequeña oficina. Consiste en dos conexiones simultáneas que pueden ser una mezcla de voz datos y fax. Cuando es usado como una conexión de datos BRI ofrece dos canales (llamados canales B) de 64 kbps o 128 kbps cuando se combinan en una sola conexión.

La interfaz de servicio primario (PRI) ofrece 24 o 30 canales de 64 kbps dando un total de 1.536 o 1920 kbps respectivamente. Al igual que en BRI, cada canal puede conectarse para un propósito diferente o combinarse para incrementar el ancho de banda.

Tanto BRI como PRI poseen un tercer canal llamado D el cual contiene la información de configuración de los canales B. El medio de transmisión más común para una red RDSI es el cable de cobre de par trenzado. [35]

1.4.3.2 Servicios de conmutación de paquetes

La conmutación de paquetes es un método que enruta pequeñas unidades de datos denominadas paquetes a través de una red en base a la dirección de destino contenida en el paquete. Los dos servicios de paquetes conmutados son X.25 y *Frame Relay*. [2]

X.25. Aunque se trata de una tecnología antigua, todavía sigue utilizándose en muchos lugares. X.25 tiene capacidades extensivas de comprobación de errores

debido a que al principio las WAN eran muy propensas a fallar a causa de un error en la transmisión de información. Esto hace que sea una tecnología fiable, pero debido a esto su ancho de banda queda limitado lo que lo hace más lento que *Frame Relay*. El ancho de banda que puede alcanzar es de hasta 2 Mbps. X.25 es orientado a conexión y la comprobación de errores trabaja en las capas 2 y 3 del modelo OSI. El medio de transmisión más común para una red X.25 es el cable de cobre de par trenzado. El costo de X.25 es moderado. [30]

Retransmisión de tramas (*Frame Relay*). Es una tecnología WAN de alto desempeño que opera en las capas 1 y 2 del modelo OSI y es de las tecnologías de redes más populares. Es una versión de paquetes conmutados del RDSI ya que originalmente fue diseñado para trabajar sobre este tipo de redes, aunque actualmente se utiliza en redes muy variadas. *Frame Relay* ofrece sus servicios en la capa 2, a diferencia de X.25 que también proporciona servicios en la capa 3. Esto permite que las redes *Frame Relay* sean mucho más rápidas que las X.25. [2] [28]

Una red *Frame Relay* consta de dos tipos de dispositivos principales, tal como aparece en la figura 1.10. Estos son:

- Equipos Terminales de Datos (DTE, *Data Terminal Equipment*)
- Equipos Terminadores de Circuitos de Datos (DCE, *Data Circuit-Terminating Equipment*)

Los DTEs son considerados como equipos terminales de una red específica y están localizados en los dominios del cliente (corporaciones). De hecho, las corporaciones pueden ser propietarias de estos equipos. Ejemplos de DTEs son terminales, computadoras personales, *routers* y *switches*.

Los DCEs son dispositivos de redes portadores. El propósito de un DCE es proporcionar servicios de sincronización y conmutación en una red. Son

dispositivos que transmiten datos a través de la WAN. Para el caso de *Frame Relay*, se trata de dispositivos de conmutación de paquetes.

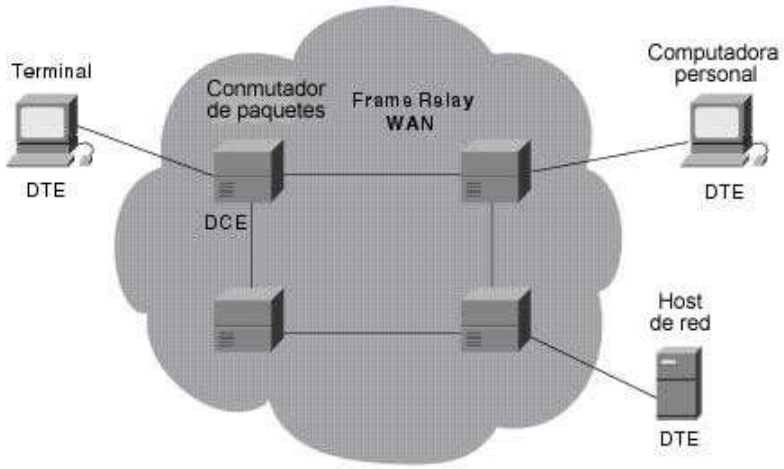

Figura 1.10 *Red Frame Relay*

Frame Relay proporciona comunicación orientada a conexión en la capa de enlace de datos. Esto significa que una comunicación determinada existe entre cada par de dispositivos y que estas conexiones están asociadas con un identificador de conexión. Este servicio es implementado utilizando un circuito virtual, el cual es una conexión lógica creada entre dos DTEs a través de una red *Frame Relay*.

Los circuitos virtuales *Frame Relay* se dividen en dos categorías:

- Circuitos Virtuales Conmutados (SVC, *Switched Virtual Circuits*)
- Circuitos Virtuales Permanentes (PVC, *Permanent Virtual Circuits*)

Los SVCs son conexiones temporales utilizadas en situaciones que requieren sólo una transferencia de datos esporádica entre los DTEs a través de la red *Frame Relay*. Para transmitir datos se realiza una llamada y cuando se termina de transmitir la llamada es terminada.

Los PVCs son conexiones que son establecidas permanentemente las cuales son utilizadas cuando se desea transferencia de datos de forma continua entre los DTEs a través de la red *Frame Relay*. Un PVC no requiere el establecimiento y fin de llamadas como en los SVC.

Los circuitos virtuales *Frame Relay* son identificados por los Identificadores de Conexión de Enlace de Datos (DLCI, *Data-Link Connection Identifiers*). Los DLCI son asignados comúnmente por los proveedores de servicio *Frame Relay*. [28]

El medio de transmisión más común para una red *Frame Relay* es el cable de cobre de par trenzado y la fibra óptica y el costo de este tipo de redes es de moderado a bajo.

1.4.3.3 Servicios de conmutación de celdas

Los servicios de conmutación de celdas proporcionan una tecnología de conmutación de conexión dedicada que organiza los datos digitales en unidades de celda y las transmite entonces por el medio físico utilizando tecnología de señal digital. Los dos servicios de celdas conmutadas son ATM y SMDS.

Modo de Transferencia Asíncrono (ATM, *Asynchronous Transfer Mode).* ATM surgió debido a las necesidades de crear un RDSI de banda ancha. Es un método de multiplexación y conmutación que permite varios servicios. Se trata de una técnica de conmutación de celdas orientada a conexión y el cual combina varias de las características de la conmutación de paquetes y la conmutación de circuitos al utilizar TDM. ATM realiza un control dinámico del ancho de banda. De esta manera, si una fuente de datos deja de enviar información, el canal de comunicación se reasigna a otra fuente. El ancho de banda máximo que soporta es de 622 Mbps, pero se está trabajando para ofrecer soporte a velocidades más elevadas. En la figura 1.11 se muestra una red ATM típica. [11]

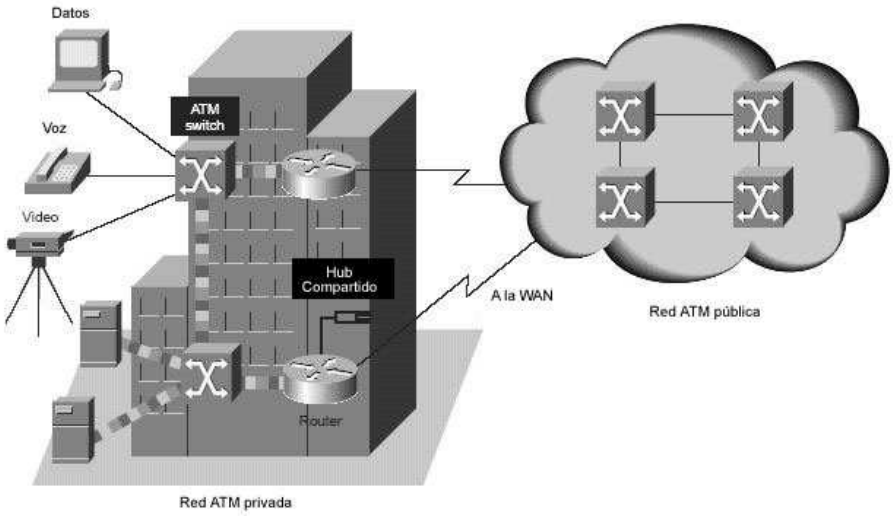

Figura 1.11 *Red ATM*

ATM convierte todo el tráfico que fluye en la red a bloques de 53 bytes llamados celdas, de los cuales 48 son de carga útil y 5 son de la cabecera que contiene la información de destino de la celda, de acuerdo a la figura 1.12. [27]

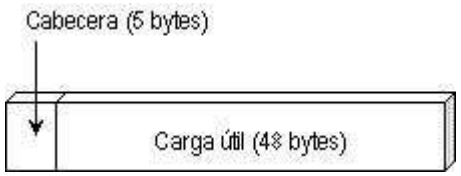

Figura 1.12 *Estructura de una celda ATM*

ATM no está limitada por la velocidad o distancia, la conmutación le permite operar a través de las LAN y redes de banda ancha mundiales a grandes. Estas velocidades permiten a ATM transportar voz, datos y video por lo que puede ofrecer soporte a una red de servicios integrados. [11]

Al igual que *Frame Relay*, ATM proporciona dos tipos básicos de conexiones:

- Circuitos Virtuales Permanentes (PVC)
- Circuitos Virtuales Conmutadas (SVC)

El medio de transmisión más común para una red ATM es el cable de cobre de par trenzado y la fibra óptica. El costo de este tipo de redes es alto.

Servicio de Datos Multimegabit Conmutado (SMDS, *Switched Multimegabit Data Service).* Es una tecnología muy relacionada con ATM y por lo general se utiliza en redes metropolitanas (MAN). Es una tecnología poco común, el medio de transmisión más común para una red SMDS es el cable de cobre de par trenzado y la fibra óptica. El costo de este tipo de redes es alto.

1.4.3.4 Servicios digitales dedicados

Los servicios digitales dedicados también proporcionan servicios de circuitos conmutados. Sin embargo, se trata de una conexión dedicada; es decir, siempre está disponible. Las series T y E, xDSL y SONET son las tecnologías de servicios digitales dedicados. [2]

Series T y E (T1, T3, E1, E3,…). La serie T de Estados Unidos, Canadá y Japón y la serie E de Europa y resto del mundo son de las tecnologías WAN más utilizadas. Los Laboratorios Bell desarrollaron una jerarquía de sistemas que pueden transportar señales digitales de voz.

En la capa más baja de esta jerarquía se encuentra una conexión llamado DS0 que transporta datos a 64 Kbps. 24 canales DS0 forman una conexión llamada DS1 o T1 a una velocidad de 1.544 Mbps. Adicionalmente, existe una T1-C la cual opera a 3.152 Mbps. Existe también una T2 a 6.312 Mbps. Hay una T3, operando a 44.736 Mbps y finalmente, una T4 a 274.176 Mbps. El ancho de banda es de 2.048 Mbps para E1 y 34.368 Mbps para E3. [5]

La jerarquía T se muestra en la figura 1.13:

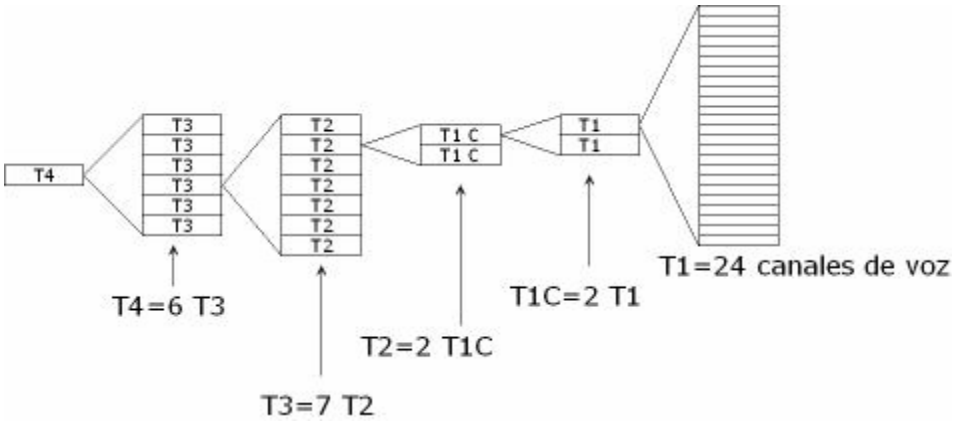

Figura 1.13 *Jerarquía T*

En la tabla 1.2 se resume la jerarquía T y E:

Nivel de Señal (portadora)	**Número de T1**	**Canales de Voz**	**Velocidad**
DS0	1/24	1	64 Kbps
DS1(T1)	1	24	1.544 Mbps
DS1C (T1C)	2	48	3.152 Mbps
DS2 (T2)	4	96	6.312 Mbps
DS3 (T3)	28	672	44.736 Mbps
DS3C (T3C)	56	1344	89.472 Mbps
DS4 (T4)	168	4032	274.176 Mbps
Portadora	**Velocidad**		
E1	2 Mbps		
E2	8 Mbps		
E3	34 Mbps		
E4	139 Mbps		
E5	555 Mbps		

Tabla 1.2 *La jerarquía T y E*

Una trama T1 se compone de 193 bits, de los cuales 192 son para datos y 1 bit extra llamado bit de trama es utilizado para sincronizar. El aspecto fundamental de una trama T1 se muestra en la figura 1.14. [65]

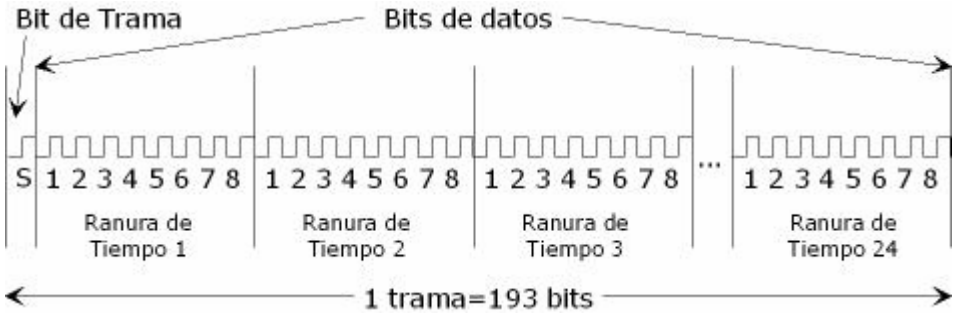

Figura 1.14 *Estructura de una trama T1*

T1 ha sido especificado por AT&T y por ANSI. El equivalente europeo, E1, es un estándar del Sector de Normalización de las Telecomunicaciones (UIT-T). E1 no utiliza un reloj maestro. En Estados Unidos, las tres portadoras mayores tienen cada una un reloj T1 maestro del cual se derivan las demás. Con estas tecnologías se pueden construir diferentes dispositivos tales como PBX, multiplexores T1, T1 fraccional, etc.

Las series T y E operan en la capa 1 y 2 del modelo OSI. Estas series utilizan TDM para asignar franjas de tiempo a la transmisión de datos. El medio de transmisión más común para las redes T y E es el cable de cobre de par trenzado y la fibra óptica y el costo de este tipo de redes es moderado. [2]

Línea de Abonado Digital (DSL, *Digital Suscriber Line).* Es un conjunto de tecnologías y estándares utilizados para la transmisión de datos a alta velocidad utilizando el cableado telefónico normal. Para lograr las altas velocidades, DSL hace uso de todo el espectro de frecuencias que se pueden transmitir por una línea de cobre. La voz sólo utiliza bajas frecuencias por lo que las altas frecuencias son aprovechadas para la transmisión de datos. Los rangos de frecuencias son separados por un dispositivo especial (*splitter*) o por una serie de filtros que se conectan a cada *socket* en el que se va a conectar un teléfono. Para lograr la conexión se utiliza un módem DSL. Existen diferentes tecnologías DSL, siendo algunas más útiles para la conexión a Internet y otras para interconectar dos o más LAN remotas. DSL se compone de las siguientes tecnologías: [55]

- DSL Asimétrico (ADSL, *Asymmetric DSL*)
- DSL de Alta Velocidad (HDSL, *High-bit-rate DSL*)
- DSL de Velocidad Adaptable (RADSL, *Rate Adaptable DSL*)
- DSL Simétrico o de Línea Única (SDSL, *Single-line DSL*)
- DSL de muy Alta Velocidad (VDSL, *Very-high-data-rate DSL*)

ADSL es la tecnología más popular actualmente, debido a su amplio uso doméstico. Ofrece distintas velocidades que pueden alcanzar hasta 8 Mbps en recepción y 1 Mbps en envío de datos, aunque lo más común es una velocidad de 1.5 Mbps para la recepción y 256 kbps para el envío. El costo de las redes DSL es moderado pero se está reduciendo cada vez más. [5]

Red Óptica Síncrona (SONET, *Synchronous Optical Network).* Es un conjunto de tecnologías de capa física de alta velocidad diseñadas especialmente para la fibra óptica, aunque también pueden ser implementadas en cable de cobre de par trenzado. SONET define una tecnología para transportar muchas señales de diferentes capacidades a través de una jerarquía óptica, flexible y síncrona. Esto se cumple a través de un esquema de multiplexación de difusión de bytes. Esto simplifica la multiplexación y proporciona una administración de la red de punto a punto.

El primer paso en el proceso de la multiplexación SONET involucra la generación del nivel más bajo de la señal base. En SONET esta señal base es llamada Señal de Transporte Síncrono Nivel 1 (STS-1, *Synchronous Transport Signal*), la cual constituye el nivel eléctrico utilizado en los dispositivos de hardware. Las señales de niveles mayores son múltiplos enteros de STS-1, la cual crea toda una familia de señales STS-N. Una señal STS-N se compone de N señales STS de difusión de bytes. La parte óptica para cada señal STS-N se denomina Portadora Óptica Nivel N (OC-N, *Optical Carrier*), la cual es utilizada en las transmisiones por fibra óptica.

En la tabla 1.3 se muestra la jerarquía de señales SONET, su velocidad así como la equivalencia con la serie T.

Nivel de Señal (Portad. óptica)	Velocidad	Capacidad
STS-1 (OC-1)	51.840 Mbps	28 DS1o 1 DS3
STS-3 (OC-3)	155.520 Mbps	84 DS1 o 3 DS3
STS-12 (OC-12)	622.080 Mbps	336 DS1 o 12 DS3
STS-48 (OC-48)	2.488 Gbps	1344 DS1 o 48 DS3
STS-192 (OC-192)	9.953 Gbps	5376 DS1 o 192 DS3
STS-768 (OC-768)	39.813 Gbps	21504 DS1 o 768 DS3

Tabla 1.3 *La jerarquía de señales SONET*

El formato de una señal STS-1 se muestra en la figura 1.15. En general, la trama puede ser dividida en dos áreas principales: cabecera de transporte y Envoltura de Carga útil Síncrona (SPE, *Synchronous Payload Envelope*). El SPE se puede dividir también en dos partes: cabecera de ruta STS y la carga útil.

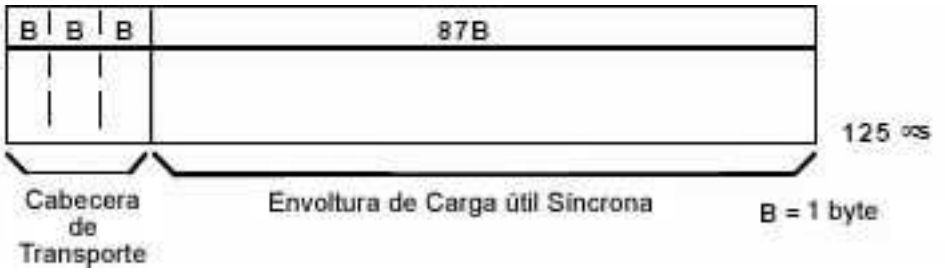

Figura 1.15 *Estructura de una trama SONET*

La carga útil tiene la capacidad de transportar arriba de 28 DS1s, 1DS3 o 21 señales de 2.048 Mbps o combinaciones de las anteriores. STS-1 es una secuencia específica de 810 bytes (6480 bits). Con una longitud de trama de 125 µs (8000 tramas por segundo), STS-1 tiene una tasa de bits de 51.840 Mbps. El formato de una trama STS se compone de 9 filas de 90 columnas de bytes, es decir, 810 bytes. El orden de transmisión es de fila por fila, de izquierda a derecha. [61]

Las redes SONET obtienen una alta velocidad de datos utilizando Multiplexación por División de Longitud de Onda (WDM, *Wavelength Division Multiplexing*). WDM es una tecnología que sincroniza los láseres a colores diferentes, lo que

proporciona diferentes longitudes de onda y así poder enviar enormes cantidades de datos. SONET se utiliza principalmente en las entidades *backbone* de Internet. El costo de esta tecnología es alto. [2]

1.4.3.5 Servicios de marcación, cable e inalámbricos

Existen otros servicios WAN diferentes a los explicados anteriormente. Se trata de los módems de marcación, los módems de cable y las redes WAN inalámbricas.

Módem de marcación. Esta tecnología funciona con la red telefónica existente. Su uso es extremadamente popular, sin embargo está limitado en velocidad, ya que su ancho de banda máximo es de 56 kbps. El costo de esta tecnología es bajo.

Módem de cable. Esta tecnología coloca las señales de datos en el mismo cable que las señales de televisión. Es utilizado en zonas que poseen cable coaxial para televisión ya instalado. El ancho de banda máximo que puede alcanzar es de 10 Mbps, sin embargo esta velocidad disminuye con el número de usuarios conectados a un mismo segmento de red. El costo de esta tecnología es relativamente bajo.

Redes WAN inalámbricas. Transmiten los datos por medio de ondas electromagnéticas que viajan por el aire. Los enlaces WAN inalámbricos se dividen en terrestres y satelitales. Los enlaces terrestres suelen utilizar microondas. El costo de esta tecnología es relativamente bajo y su uso es moderado. Los enlaces satelitales son utilizados por usuarios móviles en una red telefónica celular o por usuarios alejados de cualquier sistema de cableado. El costo de esta tecnología es alto pero es ampliamente utilizado. [2]

1.4.3.6 Implementación de una WAN antes de las VPN

Implementar una WAN requiere de una cuidadosa planeación debido a los costos ya a los tiempos requeridos para su instalación. Se debe analizar las aplicaciones que se le van a dar a la WAN con el fin de poder elegir una solución que pueda satisfacer las necesidades de una organización. Entre los aspectos que se deben analizar al elegir una solución WAN están los siguientes:

- Ubicación de las localidades (sucursales, oficinas remotas)
- Cantidad de datos a transmitir
- Velocidad de transferencia de la información
- Transmisión de datos en tiempo real (síncronos) o en un momento determinado (asíncronos)
- Restricciones [5]

Algo muy importante a tomar en cuanta al crear una WAN es el costo. Tener una WAN implica costos de instalación y posteriormente gastos mensuales. Mantener un enlace WAN resulta costoso también porque las necesidades de ancho de banda se van incrementando con el tiempo. Entre más grande sea una red y más potentes sean sus componentes, mayores serán los costos de tener la red. Es necesario establecer un equilibrio entre el rendimiento de la red y los costos de ésta. Los costos de instalar un *backbone* privado por lo general van de los $100,000 a $1’000,000[1] dependiendo del tráfico y de las distancias geográficas. [2] [23]

Como se puede ver, el alto costo necesario para implementar y mantener redes privadas está llevando a éstas a una situación muy difícil. Las tecnologías WAN tradicionales, representan una serie de necesidades diarias. El personal de soporte necesario para gestionar estas tecnologías complejas conlleva un crecimiento continuo tanto en el número de personas como en su experiencia.

[1] A lo largo de esta monografía, los precios son aproximados y están en pesos mexicanos utilizando la equivalencia 1 dólar estadounidense = 10 pesos mexicanos

Igualmente, la dependencia de aplicaciones de red requiere un aprovisionamiento separado de respaldo además de una expansión de la infraestructura de la red privada ya existente. [57]

A continuación se presenta un ejemplo de la implementación de una tecnología WAN.

Implementación de una red *Frame Relay*. Una forma típica de implementar una red privada *Frame Relay* es equipando un multiplexor T1 con interfaces *Frame Relay* y también con interfaces que no lo sean. El tráfico *Frame Relay* circula a través de la interfaz *Frame Relay* y es dirigido a la LAN. El tráfico que no es *Frame Relay* es enviado a la aplicación o servicio apropiado, como puede ser un PBX (*Private Branch Exchange*) para servicio telefónico o una aplicación de videoconferencia, como se muestra en la figura 1.16.

Una red típica *Frame Relay* consta de cierto número de dispositivos DTE, como pueden ser *routers*, conectados a puertos remotos de equipos multiplexores a través de servicios tradicionales punto a punto como pueden ser T1, T1 fraccional o módems. [28]

Una red *Frame Relay* puede ser implementada de forma pública o privada. En una red *Frame Relay* pública, un proveedor de servicios de telecomunicaciones ofrece los servicios de transmisión a sus clientes. Todos los equipos de conmutación están ubicados en las instalaciones del proveedor de servicios. Los suscriptores (corporaciones) pagan una tarifa basada en el uso de la red pero se libran del hecho de tener que administrar y mantener los equipos de la red, ya que los DCE pertenecen al proveedor e incluso los DTE podrían pertenecer a él.

En una red *Frame Relay* privada, la compañía es propietaria de los equipos *Frame Relay*. La administración y mantenimiento de la red son responsabilidad de la

empresa. Tener una red privada así resulta ser mucho más caro que tenerla de forma pública. [2]

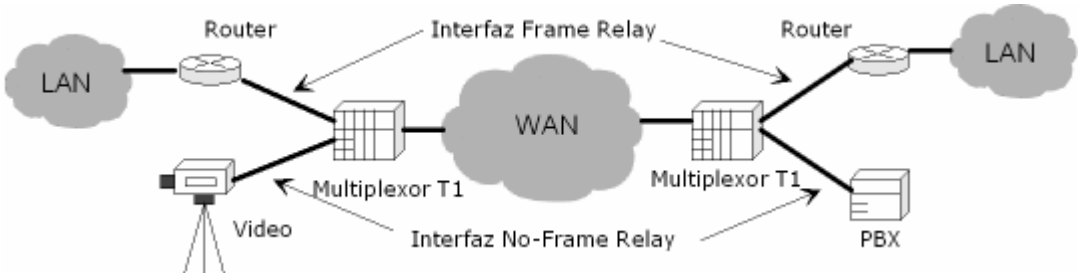

Figura 1.16 *WAN convencional que usa T1 y Frame Relay*

1.4.4 Protocolo Punto a Punto (PPP)

Las conexiones en una red están controladas por protocolos que realizan sus funciones en la Capa 2 del modelo OSI. En una LAN, para trasladar datos de un nodo a otro y controlar el flujo correcto de los datos se utilizan tecnologías de Capa 2 como Ethernet, Token Ring o FDDI. En una WAN, para lograr esto se utiliza el Protocolo Punto a Punto (PPP, *Point to Point Protocol*).

PPP proporciona conexiones fiables de *router* a *router* y de *host* a red sobre circuitos síncronos (como RDSI) y asíncronos (como las conexiones telefónicas por módem). PPP es el protocolo WAN más utilizado y conocido. Entre sus características principales tenemos:

- Controlar la configuración del enlace de datos
- Proporcionar asignación dinámica de direcciones IP
- Multiplexación del protocolo de red
- Configuración del enlace y verificación de la calidad de éstos
- Detección de errores
- Opciones de negociación para prestaciones como la dirección de capa de red y compresión de datos [3]

PPP permite características avanzadas, no disponibles en su antecesor llamado SLIP. PPP acepta varios métodos de autenticación, así como compresión y cifrado

de datos. En la mayor parte de las implementaciones de PPP, se puede automatizar todo el proceso de inicio de sesión. También admite múltiples protocolos de LAN. Con este protocolo es posible utilizar TCP/IP, IPX o NetBEUI como protocolo de red. PPP es el estándar principal para la mayor parte de los procesos de equipos de acceso remoto. PPP resulta ser muy importante en una VPN, ya que es la base de los protocolos PPTP y L2TP. [50]

1.4.4.1 Formato de una trama PPP

El formato de una trama PPP se muestra en la figura 1.17 y se describe a continuación:

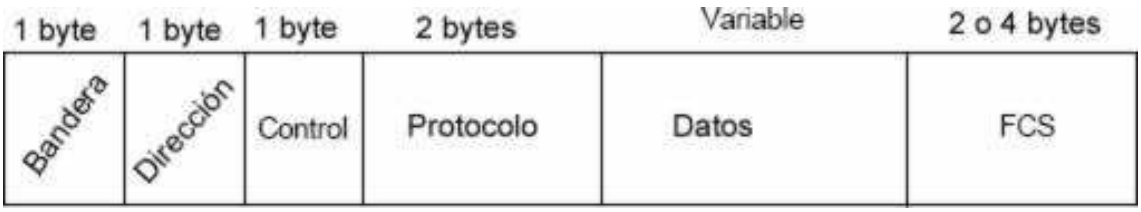

Figura 1.17 *Formato de una trama PPP*

- **Bandera.** Byte que describe el principio o final de la trama. Consiste en la secuencia 01111110.
- **Dirección.** Byte que contiene la secuencia 11111111 la cual es una dirección de transmisión estándar.
- **Control.** Byte con la secuencia 00000011, el cual llama a una transmisión de datos de usuario.
- **Protocolo.** 2 bytes que identifican el protocolo encapsulado en el campo de información de la trama
- **Datos.** 0 o más bytes que contienen el datagrama del protocolo especificado en el campo protocolo. La longitud máxima de este campo es de 1500 bytes.
- **Comprobación de Secuencia de Trama (FCS, *Frame Check Sequence*)**. 2 o 4 bytes que detectan errores en la trama.

1.4.4.2 Componentes de PPP

PPP proporciona tres componentes principales para lograr la conectividad con Internet.

- **Control de Enlace de Datos de Alto Nivel (HDLC, *High Data Link Control).*** Es un método para encapsular datagramas sobre enlaces punto a punto.
- **Protocolo de Control de Enlace (LCP, *Link Control Protocol).*** Este protocolo establece, configura y prueba la conexión de enlace de datos.
- **Protocolo de Control de Red (NCP, *Network Control Protocol).*** Es un conjunto de protocolos que establecen y configuran los distintos protocolos de capa de red. Como ya se mencionó, PPP está diseñado para soportar no sólo IP, sino también otros protocolos de red como AppleTalk e IPX.

1.4.4.3 Establecimiento de sesiones PPP

PPP proporciona un método para establecer, configurar, mantener y terminar una conexión punto a punto. Este procedimiento se lleva a cabo en cuatro fases las cuales son:

- Fase 1.- Establecer el enlace y negociar la configuración
- Fase 2.- Determinar la calidad del enlace y autenticar
- Fase 3.- Negociar la configuración del protocolo de capa de red
- Fase 4.- Terminar el enlace

Fase 1.- Establecer el enlace y negociar la configuración: En esta fase, cada dispositivo PPP envía paquetes LCP para configurar y establecer el enlace de datos. Antes de que se puedan intercambiar los datagramas de la capa de red, LCP debe abrir la conexión y negociar los parámetros de configuración. La fase queda completada cuando se ha enviado y recibido una trama de acuse de recibo de la configuración.

Fase 2.- Determinar la calidad del enlace y autenticar: LCP permite una fase para poder determinar la calidad del enlace y negociación de la configuración. En esta fase, el enlace se prueba para determinar si la calidad de éste es lo suficientemente aceptable como para que se pueda acceder a los protocolos de red.

Una vez que se ha establecido el enlace, se lleva a cabo la autenticación del usuario. Si se usa la autenticación, ésta tiene lugar antes de que se configure el protocolo de la capa de red. Esto se hace con el fin de garantizar que el usuario tiene el permiso para establecer la conexión. PPP soporta los protocolos de autenticación PAP, CHAP y EAP, de los cuales CHAP y EAP son los más utilizados porque ofrecen mayor seguridad. PAP está basado en autenticación simple por contraseña, por lo que no es recomendable.

Fase 3.- Negociar la configuración del protocolo de capa de red: Después de que se determinó la calidad del enlace y se autenticó, los protocolos de capa de red podrán ser configurados por los NCP adecuados. En esta fase, los dispositivos PPP envían paquetes NCP para elegir y configurar uno o más protocolos de capa de red. Cuando se han configurado, los datagramas podrán ser enviados por el enlace.

Fase 4.- Terminación del enlace: LCP puede terminar el enlace en cualquier momento. Esto puede ocurrir por una petición del usuario, o a causa de un evento físico, como la pérdida del proveedor de servicios o la expiración del tiempo. [3]

2

Funcionamiento de las VPN

En este capítulo se explica la definición, arquitecturas, tipos y topologías de una VPN. También se presenta el concepto de tunneling, que es la tecnología más importante sobre las que operan las VPN y se explican los métodos de seguridad (cifrado de datos, autenticación) que son utilizados para proteger los datos

2.1 Introducción a las VPN

2.1.1 Definición de Red Privada Virtual (VPN)

Como se pudo leer en el capítulo anterior, los métodos tradicionales de acceso remoto y creación de WAN privadas resultan ser bastante costosos. Puesto que las redes públicas resultan ser mucho más económicas que las privadas, se buscaron maneras de poder establecer una red privada dentro de una red pública. El resultado fue el surgimiento de las Redes Privadas Virtuales (VPN) las cuales han ofrecido ventajas muy amplias a las corporaciones siendo la principal de ellas la reducción de costos de instalación y mantenimiento de forma muy significativa. Se puede definir a una VPN de la siguiente manera:

> Una Red Privada Virtual (VPN, *Virtual Private Network*) es una red privada que utiliza la infraestructura de una red pública para poder transmitir información.

Una VPN combina dos conceptos: redes virtuales y redes privadas. En una red virtual, los enlaces de la red son lógicos y no físicos. La topología de esta red es independiente de la topología física de la infraestructura utilizada para soportarla. Un usuario de una red virtual no será capaz de detectar la red física, el sólo podrá ver la red virtual. [19]

Desde la perspectiva del usuario, la VPN es una conexión punto a punto entre el equipo (el cliente VPN) y el servidor de la organización (el servidor VPN). La infraestructura exacta de la red pública es irrelevante dado que lógicamente parece como si los datos se enviaran a través de un vínculo privado dedicado. Esto se puede apreciar en la figura 2.1. [52][51][48]

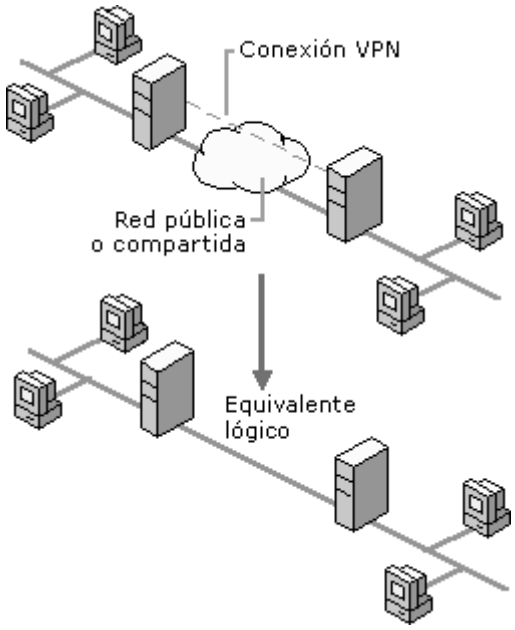

Figura 2.1 *VPN: una red virtual*

Las redes privadas son definidas como redes que pertenecen a una misma entidad administrativa. Un ejemplo típico de esta clase de red es una intranet corporativa, la cual puede ser utilizada sólo por los usuarios autorizados. De los conceptos de red privada y red virtual es como nace el concepto de red privada virtual. [19]

Debido al hecho de ser una red privada que utiliza una red pública, la cuestión de la seguridad en una VPN es muy importante, ya que la información que circula en una red pública puede ser vista por cualquiera si no se toman las debidas precauciones. Y en una red pública como Internet existen muchas personas malintencionadas que siempre están dispuestas a robar información. Es por eso que una VPN debe de poseer excelentes mecanismos de autenticación y de encriptación de la información para que ésta viaje segura a través de una red pública.

2.1.1.1 Historia del término VPN

Resulta confuso definir el término VPN. El problema radica en que cada fabricante o proveedor de servicios VPN define a las VPN de diferentes maneras. No existen estándares que definan los componentes de software o hardware de una VPN o las tecnologías VPN, por lo que cada fabricante ofrece los servicios VPN que más se adaptan a sus propias plataformas de hardware y aplicaciones de software. Como la tecnología no está estandarizada, se ofrecen VPN en toda clase de formas diferentes, como pueden ser *firewalls*, sistemas operativos, etc.[2] Respecto a la confusión para definir VPN un empresario de una importante empresa de telecomunicaciones mencionó: "Las VPN tienden a ser ahora lo que el mercado dice que son". [60] [3] [16]

El tiempo también ha modificado el concepto de VPN. El término VPN comenzó a aplicarse a las redes *Frame Relay* o ATM públicas, o a un servicio de acceso remoto basado en la red pública de telefonía conmutada (PSTN). En el capítulo anterior se explicó que las redes *Frame Relay* pueden implementarse de forma pública o privada. Pues bien, a las redes públicas *Frame Relay* se les dio el nombre de VPN, así como también a las redes públicas ATM. Estos servicios de VPN eran proporcionados por un proveedor de servicios, el cual conectaba las redes de diferentes organizaciones a su red ATM o *Frame Relay*. [42]

Otros proveedores utilizan el término en referencia a los servicios provistos sobre sus redes de datos privadas (como es el caso de Telmex, Avantel y Alestra). Pero las expectativas creadas por la utilización de Internet y de IP en general como medio de transporte son tan altas que incluso algunos expertos han redefinido el concepto de VPN como una red que soporta transporte de datos privados sobre infraestructura IP pública. Y la infraestructura IP por excelencia es Internet, la red

[2] Ver tipos de VPN para consultar las distintas soluciones VPN que se ofrecen

de datos más pública que existe. De esta forma, el término VPN se está aplicando cada vez más a las redes privadas que transportan datos utilizando Internet.[3] [46]

2.1.1.2 Componentes de una VPN

Los componentes básicos de una VPN aparecen en la figura 2.2 y son:

- Servidor VPN
- Túnel
- Conexión VPN
- Red pública de tránsito
- Cliente VPN

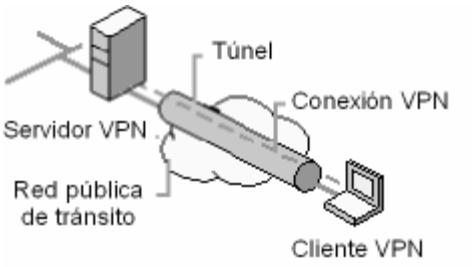

Figura 2.2 *Componentes de una VPN* [51]

Para emular un vínculo punto a punto en una VPN, los datos se encapsulan o empaquetan con un encabezado que proporciona la información de enrutamiento que permite a los datos recorrer la red pública hasta alcanzar su destino. Para emular un vínculo privado, los datos se cifran para asegurar la confidencialidad. Los paquetes interceptados en la red compartida o pública no se pueden descifrar si no se dispone de las claves de cifrado. La parte de la conexión en la cual los datos privados son encapsulados es conocida como túnel. La parte de la conexión en la que se encapsulan y cifran los datos privados se denomina conexión VPN. [52] [51]

[3] En adelante, esta monografía se centrará en las VPN basadas en redes IP, como Internet

2.1.1.3 Utilizar Internet para crear una VPN

El uso de Internet como una VPN permitió a los usuarios remotos acceder a la red corporativa utilizando a un ISP. Puesto que ahora muchos ISP ofrecen acceso ilimitado a Internet por un precio de $200 en promedio al mes para conexiones de módem, el uso de Internet puede proporcionar muchos beneficios económicos comparados con las tarifas de hacer llamadas de larga distancia. Por ejemplo, si la llamada de larga distancia cuesta $1 por minuto, una hora de acceso por día para un usuario viajero resultaría en un costo de $60 por día o $1200 al mes si se trabajan 20 días al mes. Por lo tanto, un costo de $200 pesos al mes por tener acceso ilimitado a Internet claramente demuestra el ahorro considerable de dinero que se obtiene con el uso de una VPN.

Cuando una VPN es utilizada como un mecanismo para reemplazar redes privadas, también se pueden obtener bastantes beneficios económicos. La figura 2.3 muestra a dos sucursales conectadas con la oficina corporativa. En el inciso a) se muestra una red privada típica mientras que en el inciso b) se muestra una VPN que usa Internet como red pública.

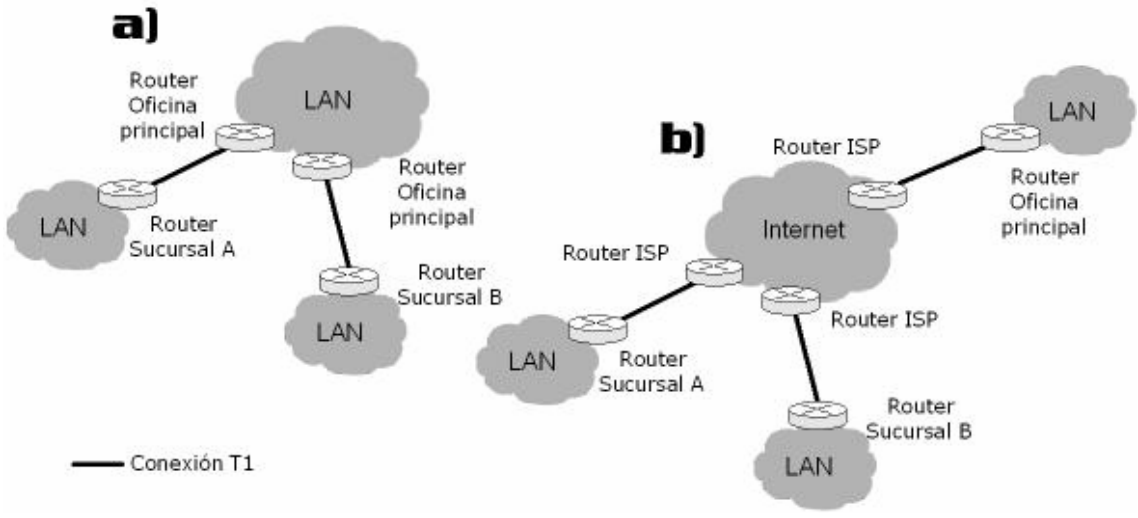

Figura 2.3 *El uso de Internet para crear una VPN*

En el inciso b) se muestra que cada LAN de la empresa se conecta a Internet a través de un ISP local usando tres conexiones T1. La mayoría de los ISP tienen

presencia en varias ciudades y cobrarán una tarifa de $10000 al mes por una conexión T1. Tanto las sucursales como la oficina principal utilizan una conexión T1 a Internet a través de un ISP con el fin de interconectar sus redes LAN a través de Internet.

Desde una perspectiva económica, se puede comparar el costo de usar Internet con el costo de mantener una red privada con dos conexiones T1 como aparece en el inciso a). Si se supone que cada red LAN se encuentra a 500 millas (804.67 Km.) de la otra, se requerirá de 1000 millas (1609.34 km.) de conexión T1 para interconectar los tres sitios.

Aunque el costo de los circuitos T1 puede variar por distintos factores, un costo de $30 por milla (1.61 km.) proporciona una aproximación razonable. De esta forma, interconectar tres sitios como aparece en el inciso a) con dos conexiones T1 costaría $30000, si existe una distancia de 500 millas entre sitios. Hay que notar que este costo iguala al costo de interconectar tres sitios utilizando Internet como aparece en el inciso b).

Sin embargo, si se asume ahora que cada uno de esos tres sitios se encuentran a una distancia de 3500 millas (5632.70 Km.) entre ellos; a un costo mensual de $30 por milla, el costo de dos líneas T1 para interconectar tres sitios como en el inciso a) se incrementaría en 3500*30, o $105,000. Ahora si se asume que cada sitio se interconecta con los otros usando la VPN del inciso b), el costo de conectar cada sitio seguiría siendo de $10000 al mes, puesto que cada sitio se conecta con el ISP local. Por lo tanto, el costo de usar la VPN del inciso b) permanecería en $30000, mientras que con la red privada del inciso a) el costo sería de $105,000. Está claro que con la VPN se lograría un ahorro de $75000. [8]

2.1.2 Arquitectura de una VPN

Existen básicamente dos tipos de arquitectura para una VPN. Estos son:

- VPN de acceso remoto
- VPN de sitio a sitio

La VPN de sitio a sitio también puede ser llamada VPN LAN a LAN o VPN POP a POP. Las VPN de sitio a sitio se dividen a su vez en VPN extranet y VPN intranet. Las VPN de acceso remoto se dividen en VPN Dial-up y VPN directas. [19]

2.1.2.1 VPN de acceso remoto

Esta VPN proporciona acceso remoto a una intranet o extranet corporativa. Una VPN de acceso remoto permite a los usuarios acceder a los recursos de la compañía siempre que lo requieran. Con el cliente VPN instalado en un dispositivo, el usuario es capaz de conectarse a la red corporativa, no importa donde se encuentre. La figura 2.4 muestra una VPN de acceso remoto. [63] [3]

Las VPN de acceso remoto ahorran costos a las empresas ya que los usuarios sólo necesitan establecer una conexión con un ISP local, pagándose solamente la llamada local y olvidándose de realizar llamadas de larga distancia. El cliente de acceso remoto inicia una conexión VPN a través de Internet con el servidor VPN de la compañía. Una vez que se ha establecido el enlace, el usuario puede acceder a los recursos de la intranet privada de la empresa. [51]

De acuerdo a la tecnología utilizada para establecer la conexión, las VPN de acceso remoto se puede dividir en VPN dial-up y VPN directas.

VPN dial-up. En esta VPN, el usuario realiza una llamada local al ISP utilizando un módem. Aunque se trata de una conexión lenta es todavía muy común. El uso de este tipo de VPN se da más entre los usuarios móviles, ya que no en todos los

lugares a donde se viaja se pueden tener disponibles conexiones de alta velocidad.

VPN directa. En esta VPN, se utilizan las tecnologías de conexión a Internet de alta velocidad, tales como DSL y módem de cable las cuales ya ofrecen muchos ISP. Este tipo de VPN se puede encontrar principalmente entre los teletrabajadores. Actualmente se pueden obtener conexiones a Internet desde el hogar utilizando estas tecnologías. [5]

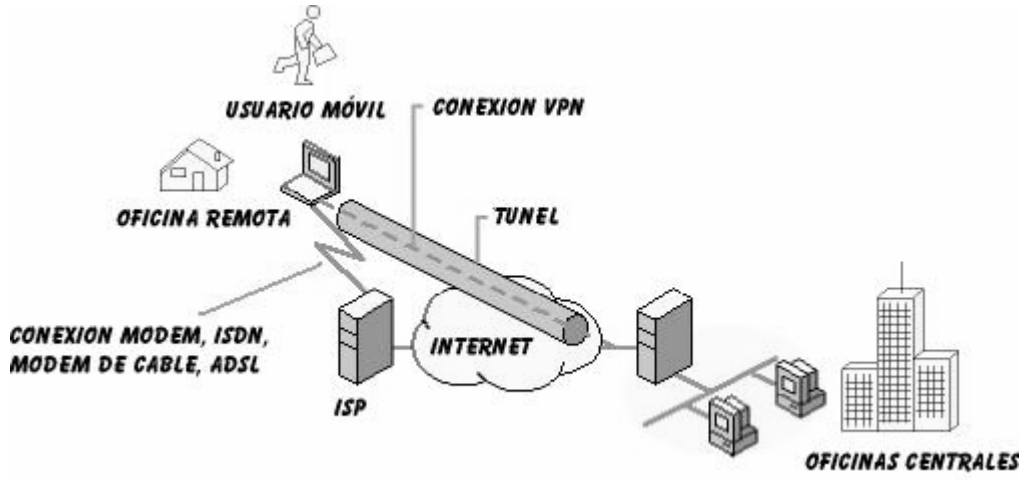

Figura 2.4 *VPN de acceso remoto*

2.1.2.2 VPN de sitio a sitio

Las VPN de sitio a sitio son utilizadas para conectar sitios geográficamente separados de una corporación. Como ya se explicó anteriormente, en las redes tradicionales las distintas oficinas de una corporación son conectadas utilizando tecnologías como T1, E1, ATM o *Frame Relay*.

Con una VPN, es posible conectar las LAN corporativas utilizando Internet. El envío de información se realiza a través de una conexión VPN. De esta forma, se puede crear una WAN utilizando una VPN. Una empresa puede hacer que sus redes se conecten utilizando un ISP local y establezcan una conexión de sitio a sitio a través de Internet. [52][51] [54]

Los costos de la comunicación se reducen enormemente porque el cliente sólo paga por el acceso a Internet. Las oficinas remotas se conectan a través de túneles creados sobre Internet. Con el uso de la infraestructura de Internet, una empresa puede desechar la difícil tarea de tener que estar administrando los dispositivos como los que se utilizan en las WAN tradicionales. [19] [23]

En base a lo problemas comerciales que resuelven, las VPN de sitio a sitio pueden subdividirse a su vez en VPN intranet y VPN extranet.

VPN intranet. Las VPN intranet se utilizan para la comunicación interna de una compañía, como aparece en la figura 2.5. Enlazan una oficina central con todas sus sucursales. Se disfrutan de las mismas normas que en cualquier red privada. Un enrutador realiza una conexión VPN de sitio a sitio que conecta dos partes de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la que está conectado el servidor VPN. [63] [52] [3]

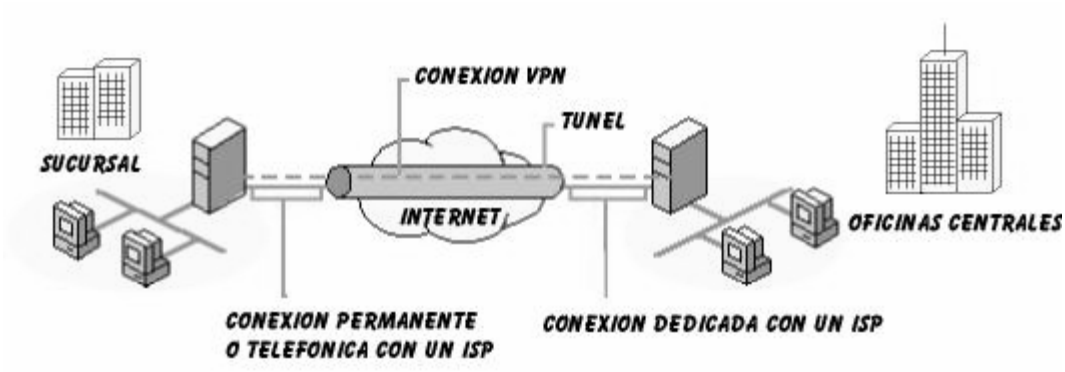

Figura 2.5 *VPN intranet*

VPN extranet. Estas VPN enlazan clientes, proveedores, socios o comunidades de interés con una intranet corporativa, como se muestra en la figura 2.6. Se puede implementar una VPN extranet mediante acuerdo entre miembros de distintas organizaciones. Las empresas disfrutan de las mismas normas que las de una red privada. Sin embargo, las amenazas a la seguridad en una extranet son mayores que en una intranet, por lo que una VPN extranet debe ser

cuidadosamente diseñada con muchas pólizas de control de acceso y acuerdos de seguridad entre los miembros de la extranet. [3] [63] [19]

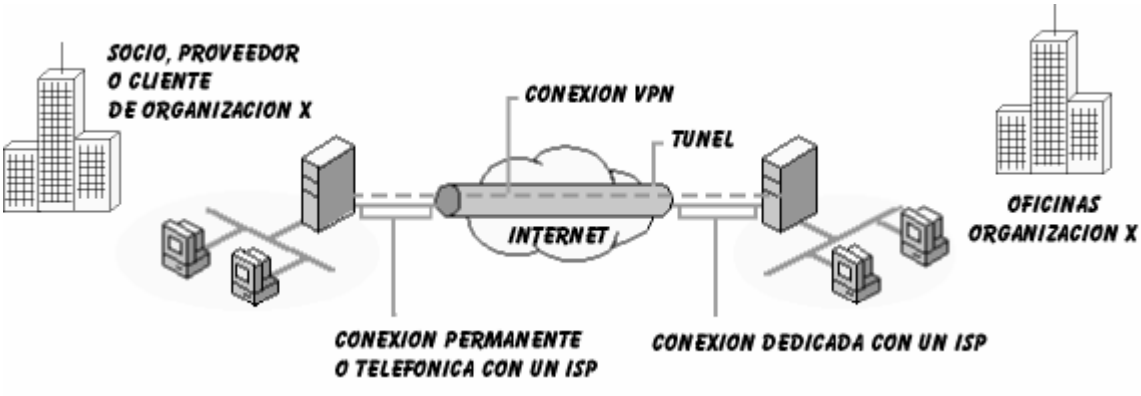

Figura 2.6 *VPN extranet*

2.1.3 Tipos de VPN

Existen diferentes formas de que una organización puede implementar una VPN. Cada fabricante o proveedor ofrece diferentes tipos de soluciones VPN. Cada corporación tendrá que decidir la que más 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

2.1.3.1 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. [1] 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. [33]

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 sólo 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. [16]

2.1.3.2 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 diseñado 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. [2]

Este dispositivo está especialmente diseñado para las VPN, por lo que se trata de la solución VPN más rápida. Resulta ser más 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.

2.1.3.3 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 además 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 más para el acceso remoto. [16]

2.1.3.4 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 Infotecs. [16] [44]

La desventaja es que estas VPN no soportan una gran cantidad de usuarios y son mucho más 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. [16]

2.1.3.5 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.[4]

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. [14]

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]

[4] Ver el Anexo 1 para consultar un listado de algunos proveedores de servicios VPN

2.1.4 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 híbrida

Para las VPN de acceso remoto:

- 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.

2.1.4.1 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 2.7. 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.

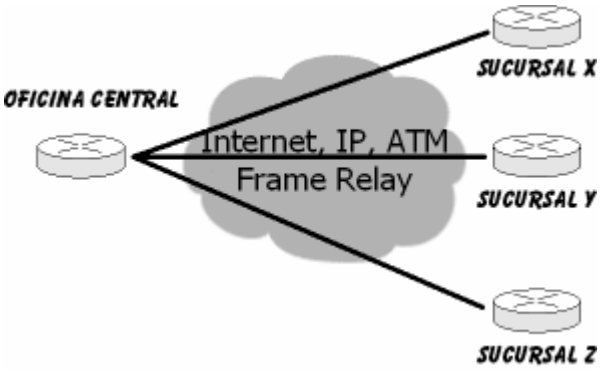

Figura 2.7 *Topología radial*

2.1.4.2 Topología de malla completa o parcial

Esta topología 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. Dependiendo de sus necesidades, una empresa puede utilizar una topología de malla completa si todas las LAN se comunican entre sí 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 2.8 muestra una topología de malla:

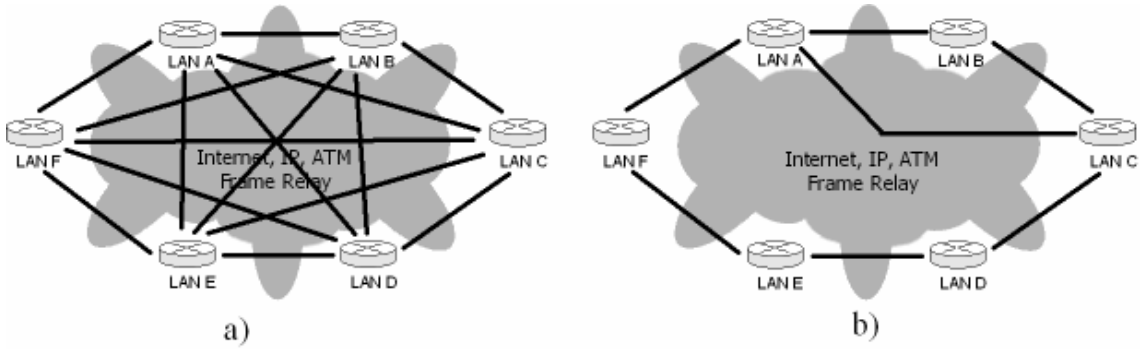

Figura 2.8 *Topología de malla: a) completa b) parcial*

2.1.4.3 Topología híbrida

Las redes VPN grandes combinan la topología radial con 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.

2.1.4.4 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 más común IP, sobre el enlace PPP entunelado e intercambian paquetes de datos sobre él. [14]

2.1.5 Requerimientos de una VPN

Una VPN debe de contar con ciertos requerimientos que permitan que valga la pena el uso de esta tecnología. Sin estos requerimientos, las VPN no podrán ofrecer la calidad necesaria que requieren las organizaciones para un desempeño óptimo. Una solución VPN debe ofrecer los siguientes requerimientos:

- Autenticación de usuarios
- Control de acceso
- Administración de direcciones
- Cifrado de datos
- Administración de claves
- Soporte a protocolos múltiples
- Ancho de banda

2.1.5.1 Autenticación de usuarios

La autenticación es uno de los requerimientos más importantes en una VPN. Cada entidad participante en una VPN debe de identificarse a sí misma ante otros y viceversa. La autenticación es el proceso que permite a los diversos integrantes de la VPN verificar las identidades de todos.

Existen muchos mecanismos de autenticación pero el más popular de todos ellos es la Infraestructura de Claves Públicas (PKI, *Public Key Infraestructure*), el cual es un sistema basado en la autenticación por medio de certificados. Cada integrante de una VPN se autentica intercambiando los certificados de cada uno, los cuales están garantizados por una autoridad de certificación (CA, *Certification Authority*) en la que todos confían.

El proceso de autenticación también involucra el intercambio de información secreta, como una clave o un desafío ante un Servidor de Acceso a Red (NAS, *Network Access Server*), el cual consultará a un servidor RADIUS. Un servidor RADIUS administra la autenticación en una red que lo requiere.

2.1.5.2 Control de acceso

El control de acceso en una red está definido como el conjunto de pólizas y técnicas que rigen el acceso a los recursos privados de una red por parte de usuarios autorizados. Una vez que un usuario ha sido autenticado, se debe definir a qué recursos de la red puede tener acceso dicho usuario. Los diferentes tipos de VPN, ya sea de *firewalls*, sistemas operativos, etc; son responsables de gestionar el estado de la conexión del usuario. La VPN debe administrar el inicio de una sesión, permitir el acceso a ciertos recursos, continuar una sesión, impedir el acceso de recursos y terminar una sesión.

El conjunto de reglas y acciones que definen el control de acceso se denomina póliza de control de acceso. Un servidor RADIUS puede administrar el control de acceso basándose en la póliza. Un ejemplo de una regla de control de acceso sería que el servidor permitiera el acceso sólo los usuarios de acceso remoto que no han rebasado un determinado uso de horas de la red.

El principal propósito de una VPN es permitir acceso seguro y selectivo a los recursos de una red. Con un buen sistema de cifrado y autenticación pero sin

control de acceso, la VPN sólo protege la integridad del tráfico transmitido y evita que usuarios no autorizados ingresen a la red, pero los recursos de ésta no quedan protegidos. Es por eso que el control de acceso es importante.

2.1.5.3 Administración de direcciones

Un servidor VPN debe de asignar una dirección IP al cliente VPN y asegurarse de que dicha dirección permanezca privada. Está claro que IP no es un protocolo seguro y se puede ver esto en la inseguridad de Internet. Las direcciones deben ser protegidas con fuertes mecanismos de seguridad, esto es, deben usarse técnicas que permitan la ocultación de la dirección privada dentro de una red pública.

La tecnología más utilizada para ocultar la información es el *tunneling*. El *tunneling* es una técnica que encapsula los datos (incluyendo la dirección destino privada) dentro de otro conjunto de datos. Así, el contenido de los paquetes encapsulados se vuelve invisible para una red pública insegura como Internet. Existen muchas tecnologías de *tunneling*, cada una de ellas con sus ventajas y desventajas. Otra tecnología alterna al *tunneling* es MPLS, donde se hace uso de un sistema de etiquetas para transmitir información. MPLS es una tecnología que realizará grandes cambios a los métodos tradicionales de enrutamiento y de la forma de crear túneles.[5] [19]

2.1.5.4 Cifrado de datos

Cifrar o encriptar los datos es una tarea esencial de una VPN. Aunque se puedan encapsular los datos dentro de un túnel, estos todavía pueden ser leídos si no se implementan fuertes mecanismos de cifrado de la información. El cifrado es un conjunto de técnicas que intentan hacer inaccesible la información a personas no

[5] Esta monografía se centrará sólo en los protocolos de *tunneling* convencionales como PPTP y L2TP por ser los más populares

autorizadas. El texto sin cifrar se le denomina *texto nativo*, mientras que el texto cifrado se le denomina *texto cifrado*. Antes de enviar la información, el servidor VPN cifra la información convirtiéndolo en *texto cifrado*. El receptor de la información descifra la información y la convierte en *texto nativo*. [49] [23]

Al principio los algoritmos de encriptación se mantenían en secreto. Sin embargo, cuando el algoritmo era roto, toda la información protegida con dicho algoritmo se volvía vulnerable. Por consiguiente, actualmente los algoritmos se hacen públicos. Existen muchos tipos de algoritmos de cifrado muy fuertes utilizados en las VPN entre los que podemos encontrar 3DES, *Diffie-Hellman*, MD5, RSA y SHA-1.

Puesto que el algoritmo de cifrado es conocido por todos, es necesario implementar técnicas para poder mantener los datos seguros. Esto se logra mediante el uso de claves. Una clave es un código secreto que el algoritmo de encriptación utiliza para crear una única versión de texto cifrado. Mientras la longitud en bits de esta clave sea más grande, más difícil será descifrar una información.

Las VPN requieren del uso de claves con una cierta longitud, de tal manera que resulta prácticamente imposible descifrar los datos (teóricamente tardaría millones de años, a no ser que se posean cientos de procesadores trabajando al mismo tiempo para encontrar la clave y aunque ésta se encontrara, los algoritmos están diseñados de forma que no se garantizaría totalmente el éxito). Aunque de hecho, el uso de claves muy largas no es recomendable porque se afecta mucho el rendimiento de un procesador. Para eso se utilizan métodos como el uso de claves simétricas y asimétricas. [23]

Con una clave simétrica, se usa la misma clave para cifrar y descifrar la información que viaja por un túnel. Tanto el emisor como el receptor de los datos poseen la misma clave privada. Con una clave asimétrica, la información se cifra con una clave y se descifra con otra diferente. Una de las claves sólo es conocida

por el usuario, la cual es conocida como clave privada. La otra clave es conocida por todos y se le llama clave pública.

Las claves públicas permiten el uso de firmas digitales para autenticar información. Una clave pública es distribuida libremente a cualquiera que requiera enviar información cifrada o firmada. La clave privada debe ser bien resguardada por el usuario y no darla a conocer nunca.

2.1.5.5 Administración de claves

En una VPN, es importante la administración de claves. Para asegurar la integridad de una clave pública, ésta es publicada junto con un certificado. Un certificado es una estructura de datos firmada digitalmente por una organización conocida como autoridad de certificación (CA) en la cual todos confían. Una CA firma su certificado con su clave privada. Un usuario que utiliza la clave pública de la CA podrá comprobar que el certificado le pertenece a dicha CA y por lo tanto, la clave pública es válida y confiable. [51]

En una VPN pequeña no es muy necesario establecer una infraestructura de administración de claves. Sin embargo, las grandes compañías obtendrán muchos beneficios si hacen crean una Infraestructura de Claves Públicas (PKI) para poder crear y distribuir certificados. Una corporación puede crear su propia CA o confiar en una CA de terceros. Una PKI es muy útil en aquellas organizaciones que requieren de mucha seguridad y acceso limitado a sus usuarios. [23]

2.1.5.6 Soporte a protocolos múltiples

Para que una solución VPN sea viable, es necesario también que ésta pueda ofrecer soporte a múltiples protocolos. Esto incluye el soporte a protocolos de red que no sean IP como pueden ser *AppleTalk*, IPX y NetBEUI. PPTP soporta varios protocolos de red. IPSec sólo puede ser utilizado en redes basadas en IP, pero

siempre es posible encapsular los protocolos no compatibles dentro de un paquete IP, de modo que puedan ser transportados. En cuanto a L2TP, este protocolo VPN no sólo puede ser implementado en redes IP, sino también en ATM y *Frame Relay*.

2.1.5.7 Ancho de banda

El ancho de banda es también un requerimiento importante en una VPN. En el mundo de las redes existe un concepto que define la forma de administrar el ancho de banda con el fin de que el tráfico de una red fluya de forma eficiente. Dicho concepto es la Calidad de Servicio (QoS, *Quality of Service*). La QoS es una característica muy importante de una VPN. Una solución VPN no estará completa si no proporciona formas para el control y administración del ancho de banda. [29]

La calidad del servicio también se refiere al número de conexiones simultáneas (la cantidad de túneles que pueden ser establecidos entre un sitio remoto y el sitio central) que puede soportar una VPN y la forma cono ésta afecta al rendimiento de la VPN. [64]

Es preciso también asegurarse que una VPN puede cifrar y descifrar los paquetes transmitidos a una velocidad adecuada, ya que algunos algoritmos de cifrado son lentos y si no se tiene un buen procesador el rendimiento se verá afectado. Es importante mencionar que el valor nominal de velocidad de los dispositivos de redes (por ejemplo 100 Mbps) nunca se cumple en la realidad y que eso habrá que tomarse en cuenta a la hora de implementar una VPN. [9]

La calidad de las conexiones a Internet también es importante. Las técnicas de encriptación incrementan el deterioro del rendimiento de la comunicación por las sobrecargas. Las pérdidas de paquetes y la latencia en conexiones a Internet de baja calidad afecta más al rendimiento, que la carga añadida por la encriptación. [34]

2.2 Tunneling

2.2.1 Definición de *tunneling*

El *tunneling*[6] es un método utilizado para encapsular paquetes (conocidos como datos de usuario) dentro de otros paquetes los cuales son enviados utilizando la tecnología de la red por la que viaja. Esto ofrece grandes ventajas, ya que permite el transporte de protocolos con diferente esquema de direccionamiento y que por lo tanto no son compatibles con una red que utiliza otros protocolos de direccionamiento dentro de paquetes que sí reconoce la red. [19]

2.2.1.1 Funcionamiento del *tunneling*

Por ejemplo, un paquete IPX o *AppleTalk* no puede ser transportado en una red basada en IP, como Internet. Sin embargo, si este paquete es encapsulado dentro de un paquete IP, entonces podrá ser transportado como cualquier otro paquete IP. Lo que hace este proceso es simplemente agregarles un encabezado adicional.

Después de agregar el encabezado, se envía el paquete encapsulado a través de una ruta lógica denominada túnel. El túnel es la ruta de información lógica a través de la cual viajan los paquetes encapsulados. Para los interlocutores de origen y de destino originales, el túnel suele ser transparente y aparece simplemente como otra conexión punto a punto en la ruta de acceso a la red. A estos puntos que están en cada extremo del túnel se les denomina interfaces de túnel. Los interlocutores desconocen los *routers*, *switches*, servidores *proxy* u otras puertas de enlace de seguridad que pueda haber entre los extremos del túnel.

[6] Se podría traducir al español como “entunelamiento”

Cuando el paquete llega a su destino, éste es desencapsulado para que pueda ser utilizado. En resumen, el *tunneling* es un proceso que consta de los siguientes pasos:

- Encapsulación
- Transmisión
- Desencapsulación

El uso de un túnel abarca todo el proceso de encapsulación, enrutamiento y desencapsulación. El túnel envuelve, o encapsula, el paquete original dentro de un paquete nuevo. Este paquete nuevo puede contener nueva información de direccionamiento y enrutamiento, lo que le permite viajar por la red. Si el túnel se combina con la confidencialidad de datos, los datos del paquete original (así como el origen y el destino originales) no se muestran a quienes observen el tráfico en la red. Cuando los paquetes encapsulados llegan a su destino, se quita la encapsulación y se utiliza el encabezado original del paquete para enrutar éste a su destino final. [48]

2.2.1.2 Protocolo pasajero, encapsulador y portador

El proceso de *tunneling* involucra tres protocolos diferentes (Ver Figura 2.9):

- **Protocolo pasajero:** Representa el protocolo que debe encapsularse. Como ejemplos de protocolos pasajeros tenemos PPP y SLIP.
- **Protocolo de encapsulamiento:** Es el que será empleado para la creación, mantenimiento y destrucción del túnel. Ejemplos de protocolo de encapsulamiento son L2F, L2TP, PPTP.
- **Protocolo portador:** Es el encargado de realizar el transporte del protocolo de encapsulamiento. El principal ejemplo de protocolo portador es IP puesto que este tiene amplias capacidades de direccionamiento y es en el que está basado Internet. [31]

Figura 2.9 *Estructura general de un paquete de tunneling*

2.2.2 *Tunneling* y VPN

Cuando el uso de túneles se combina con el cifrado de los datos, puede utilizarse para proporcionar servicios de VPN. Las VPN utilizan el *tunneling* para poder ofrecer mecanismos seguros de transporte de datos. Dentro del contexto de las VPN, el *tunneling* involucra tres tareas principales:

- Encapsulación
- Protección de direcciones privadas
- Integridad de los datos y confidencialidad de éstos

Para que el proceso del *tunneling* pueda ser llevado a cabo, existen diversos protocolos llamados protocolos de túnel los cuales se encargan de encapsular y desencapsular los datos que viajan dentro de una red privada virtual. Los protocolos de túnel usados por las VPN como PPTP y L2TP son usados para encapsular tramas de la capa de enlace de datos (PPP). Protocolos de túnel como IP sobre IP e IPSec en modo túnel son utilizados para encapsular paquetes de la capa de red.

Es posible colocar un paquete que utiliza una dirección IP privada dentro de un paquete que usa una dirección IP global única para poder extender una red privada sobre una red pública como Internet. Puesto que los contenidos del paquete entunelado sólo pueden ser interpretados por las interfaces de túnel, las direcciones IP privadas pueden ser ocultadas completamente de las redes IP públicas.

Los mecanismos de integridad y confidencialidad garantizan que ningún usuario no autorizado pueda alterar los paquetes entunelados durante la transmisión sin que el ataque pueda ser detectado y que los contenidos del paquete permanecen protegidos de acceso no autorizado. Además, el *tunneling* opcionalmente puede proteger la integridad de la cabecera del paquete IP externo, mediante técnicas de autenticación. Por ejemplo, si se utiliza IPSec los protocolos AH y ESP pueden proporcionar autenticación de los paquetes transmitidos. [19]

Tres protocolos de túnel son los más usados para la creación de una VPN:

- Protocolo de Túnel punto a punto (PPTP)
- Protocolo de Túnel de Capa 2 (L2TP)
- Protocolo de Seguridad IP [9]

Los protocolos PPTP y L2TP se enfocan principalmente a las VPN de acceso remoto, mientras que IPSec se enfoca mayormente en las soluciones VPN de sitio a sitio. La figura 2.10 resume cómo se lleva a cabo el *tunneling* en una VPN. [62]

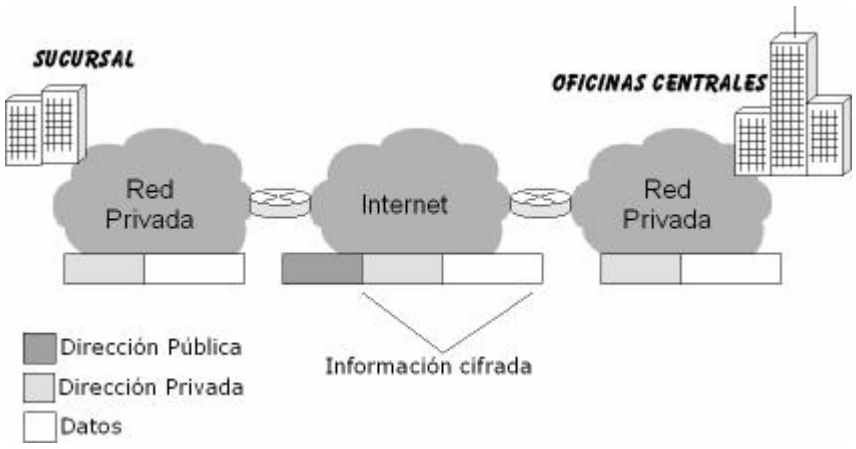

Figura 2.10 *Tunneling en una VPN*

2.2.3 Tipos de túneles

Los túneles se clasifican de acuerdo a cómo se establece la conexión entre dos *hosts*. En base a esto, existen dos tipos de túneles. Éstos son:

- Túnel voluntario
- Túnel obligatorio

2.2.3.1 Túnel voluntario

Un equipo usuario o cliente puede emitir una petición VPN para configurar y crear un túnel voluntario. En este caso, el equipo del usuario es un extremo del túnel que funciona como cliente de túnel. El túnel voluntario se produce cuando una estación de trabajo o un *router* utilizan software de cliente de túnel para crear una conexión VPN con el servidor de túnel de destino. Para ello, debe instalar el protocolo de túnel correspondiente en el equipo cliente. Un túnel voluntario puede ser creado de dos maneras a través de una conexión dial-up o a través de una LAN. La figura 2.11 muestra un túnel voluntario.

A través de una conexión dial-up. En este caso, el usuario primero hace una llamada a su ISP para conectarse a Internet y entonces posteriormente podrá ser creado el túnel. Esta suele ser la situación más común. La conexión a Internet es un paso preliminar para crear el túnel pero no forma parte del proceso de creación del túnel. [52]

A través de una LAN. En este caso, el cliente ya posee una conexión a la red, por lo que el túnel puede ser creado con cualquier servidor túnel deseado. Este es el caso de un usuario de una LAN que crea un túnel para acceder a otra LAN. [51]

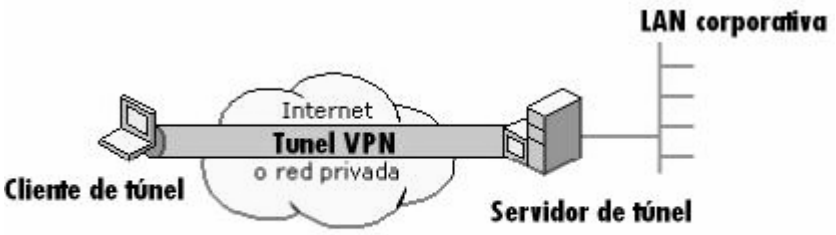

Figura 2.11 *Túnel voluntario*

2.2.3.2 Túnel obligatorio

El túnel obligatorio es la creación de un túnel seguro por parte de otro equipo o dispositivo de red en nombre del equipo cliente. Los túneles obligatorios se configuran y crean automáticamente para los usuarios sin que éstos intervengan ni tengan conocimiento de los mismos. Con un túnel obligatorio, el equipo del usuario no es un extremo del túnel. Lo es otro dispositivo entre el equipo del usuario y el servidor de túnel que actúa como cliente de túnel.

Algunos proveedores que venden servidores de acceso telefónico facilitan la creación de un túnel en nombre de un cliente de acceso telefónico. El dispositivo que proporciona el túnel para el equipo cliente se conoce como procesador cliente (FEP) o PAC en PPTP, concentrador de acceso (LAC) de L2TP en L2TP o puerta de enlace (*gateway*) de Seguridad IP en IPSec. Para realizar su función, el dispositivo que proporciona el túnel debe tener instalado el protocolo de túnel adecuado y debe ser capaz de establecer el túnel cuando el equipo cliente intenta establecer una conexión. [52]

Esta configuración se conoce como túnel obligatorio debido a que el cliente está obligado a utilizar el túnel creado por el dispositivo que proporciona el túnel. Una vez que se realiza la conexión inicial, todo el tráfico de la red de y hacia el cliente se envía automáticamente a través del túnel. En los túneles obligatorios, la computadora cliente realiza una conexión única PPP y, cuando un cliente se conecta en el NAS, se crea un túnel y todo el tráfico se enruta automáticamente a través de éste. Se puede configurar un el dispositivo que proporciona el túnel para hacer un túnel a todos los clientes hacia un servidor específico del túnel. De manera alterna, el dispositivo que proporciona el túnel podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.

A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel entre el dispositivo que proporciona el túnel y el servidor del túnel puede

estar compartido entre varios clientes. Cuando un segundo cliente se conecta al dispositivo que proporciona el túnel para alcanzar un destino para el cual ya existe un túnel, no hay necesidad de crear una nueva instancia del túnel entre el dispositivo que proporciona el túnel y el servidor del túnel. El tráfico de datos para el nuevo cliente se transporta sobre el túnel existente. Ya que puede haber varios clientes en un túnel único, el túnel no se termina hasta que se desconecta el último usuario del túnel. [47]

Una compañía puede contratar a un ISP para que implemente un conjunto de dispositivos que proporcionen túneles por todos los territorios donde existan LAN de la compañía. Estos dispositivos pueden establecer túneles a través de Internet hasta un servidor VPN conectado a la red privada de la organización, consolidando así las llamadas de zonas geográficamente dispersas en una sola conexión a Internet en la red de la organización.

Existen dos formas de crear túneles obligatorios. En la primera forma, el túnel se crea antes de autenticar al cliente de acceso. Una vez creado el túnel, el cliente de acceso se autentica en el servidor de túnel. En la segunda forma, el túnel se crea después de que el dispositivo que proporciona el túnel autentica al cliente de acceso. La figura 2.12 muestra cómo se compone un túnel obligatorio.

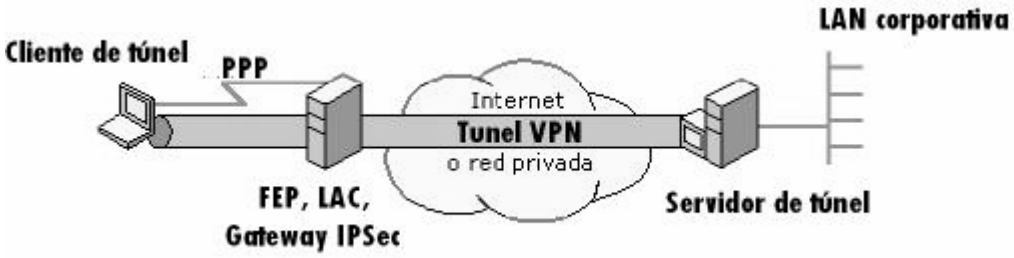

Figura 2.12 *Túnel obligatorio* [52]

2.3 Seguridad en una VPN

2.3.1 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, toda 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 las redes. [1]

La seguridad cobra especial importancia al momento de implementar una VPN. Puesto que la información privada de una 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 una VPN debe ir más allá que simplemente controlar el acceso seguro a los recursos de una red. También debe proveer mecanismos para administrar la implementación de pólizas de seguridad que garanticen el desarrollo exitoso de una 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

debe cumplir el equipo remoto que desea conectarse a la red corporativa debe ser lo más 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 teletrabajador en su ámbito doméstico. [37]

La autenticación de usuarios y la encriptación de datos son características de seguridad muy fuertes. Y en una VPN la tecnología que podrá ofrecer mejor seguridad será IPSec.

2.3.2 Ataques a la seguridad de las redes

2.3.2.1 Clasificación de las amenazas a redes

Existen cuatro posibles amenazas a la seguridad de las redes las cuales son descritas a continuación.

Amenazas no estructuradas. Esta clase de amenazas suelen ser originadas por personas inexpertas que utilizan herramientas de piratería en Internet. Aunque algunos actúan de forma malintencionada, la gran mayoría de ellos lo hace por puro reto intelectual. Se les conoce comúnmente como *script kiddies*.

A pesar de que no se trata de profesionales de las redes ni grandes programadores, son una amenaza muy seria para la seguridad. Pueden ser capaces de introducir un virus o caballo de Troya a una red sin saber exactamente lo que hacen y provocar graves pérdidas económicas.

Amenazas estructuradas. Estas amenazas son causadas por personas que sí tienen conocimientos de redes. Saben cómo están constituidas y conocen sus puntos débiles. Como conocen mucho de programación pueden crear programas que penetren en los sistemas. Son conocidos como *hackers* y si tienen malas intenciones se les llama *crackers*. Estas personas pueden ser contratadas por el crimen organizado para cometer robos y fraudes, por una empresa para dañar a la competencia o por agencias de inteligencia con el fin de desestabilizar un gobierno enemigo.

Amenazas externas. Son las amenazas causadas por personas ajenas a la red de una empresa. Son personas no autorizadas a ingresar a estos sistemas, pero pueden entrar a través de Internet o por medio de un RAS.

Amenazas internas. Son amenazas causadas por personas que sí tienen acceso autorizado a la red. Puede ocurrir que algún empleado despedido o descontento con la compañía introduzca un virus a la red como venganza. Este tipo de amenazas son las más frecuentes que existen. [1]

2.3.2.2 Clasificación de los ataques a redes

Husmeadores (*sniffers*) de red. Este ataque tiene lugar cuando el usuario no autorizado utiliza un programa llamado husmeador o *sniffer* el cual puede leer todos los paquetes que circulan por una red con lo que se puede tener acceso a información privada. Si los paquetes no están cifrados, el *sniffer* proporciona una vista completa de los datos contenidos en el paquete. Incluso los paquetes encapsulados (enviados por un túnel) se pueden abrir y leer si no están cifrados.

Integridad de datos. Una vez que un atacante ha leído los datos entonces podrá tener la capacidad de modificarlos. Este ataque tiene lugar cuando alguien modifica o corrompe los datos que circulan por una red. Un atacante puede modificar los datos de un paquete sin que el remitente ni el receptor lo adviertan.

Incluso cuando no se esté enviando información importante, nadie desea que la información enviada sea modificada en su camino.

Ataques de contraseña (diccionario). Un problema típico de seguridad tiene que ver con el control de acceso basado en contraseñas. El problema es que un sistema no puede saber quien está frente al teclado escribiendo la contraseña. Una forma de obtener una contraseña es si los nombres de usuario y contraseña no son cifrados al enviarse por una red, cualquier atacante podría apoderarse de ella y obtener acceso a una red haciéndose pasar por un usuario legítimo. Otra forma que se utiliza para obtener una contraseña es utilizar ciertas técnicas de criptoanálisis llamadas ataques de diccionario o fuerza bruta. [16]

Ataque de denegación de servicio (DoS). Este ataque tiene lugar cuanto un atacante desactiva o corrompe las redes, los sistemas o los servicios para denegar el servicio a los usuarios. Se puede lograr enviando datos no válidos a aplicaciones o servicios de red, lo que puede hacer que el servidor se bloquee. Otro ataque DoS consiste en inundar de tráfico toda una red hasta hacer que se sature y sea imposible utilizarla o también se puede estropear un *router* con el fin de que los usuarios legítimos no puedan acceder a la red. [16] [1]

Ataque hombre en medio. Este ataque se produce cuando alguien se interpone entre dos usuarios que se están comunicando. El atacante observa activamente, captura y controla los paquetes sin que los usuarios lo adviertan. Por ejemplo, un atacante puede negociar claves de cifrado con ambos usuarios. A continuación, cada usuario enviará datos cifrados al atacante, quien podrá descifrarlos.

Spoofing. Este ataque se basa en el uso de las direcciones IP. La mayoría de las redes y sistemas operativos utilizan la dirección IP para identificar un equipo como válido en una red. En algunos casos, es posible utilizar una dirección IP falsa. Esta práctica se conoce como suplantación. Un atacante podría utilizar programas especiales para construir paquetes IP que parezcan provenir de direcciones

válidas dentro de la intranet de una organización. Una vez obtenido el acceso a la red con una dirección IP válida, el atacante podrá modificar, desviar o eliminar datos.

Ataque de clave comprometida. Una clave es un código o un número secreto necesario para cifrar, descifrar o validar información protegida. Averiguar una clave es un proceso difícil y que requiere grandes recursos por parte del atacante, pero no deja de ser posible. Cuando un atacante averigua una clave, ésta se denomina clave comprometida. El atacante puede utilizar la clave comprometida para obtener acceso a una comunicación protegida sin que el remitente ni el receptor lo perciban. La clave comprometida permite al atacante descifrar o modificar los datos. El atacante también puede intentar utilizar la clave comprometida para calcular otras claves que podrían suponer el acceso a otras comunicaciones protegidas. [48]

2.3.3 Seguridad de los datos

Todas las tecnologías de seguridad en las redes se basan en técnicas criptográficas. Para dar seguridad a los datos, tres aspectos deben de proporcionar estas técnicas.

- Confidencialidad
- Integridad
- Autenticación.

Por confidencialidad se entiende como el hecho de ocultar los datos de usuarios no autorizados. Por integridad se refiere al hecho de asegurar que los datos no sean modificados mientras son transmitidos y la autenticación se refiere al hecho de poder comprobar que los datos provienen del lugar del que se supone deben venir. El cifrado simétrico, el cifrado de clave pública y las funciones de dispersión (*hash*) son las técnicas utilizadas para proteger la información de todos los tipos de ataques ya mencionados.

2.3.3.1 Criptografía y criptoanálisis

Criptografía. Es la ciencia que trata del enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente. La criptografía abarca el uso de mensajes encubiertos, códigos y cifras así como el uso de algoritmos matemáticos para poder proteger la información. La criptografía es el fundamento de todas las tecnologías de seguridad de las redes. [49]

Criptoanálisis. Es la ciencia que analiza los algoritmos criptográficos, con el fin de poder obtener el texto nativo a partir de un texto cifrado. Hay ciertos algoritmos simples que son fáciles de romper, sin embargo un buen algoritmo de encriptación sólo puede ser roto por medio de ataques de fuerza bruta o de diccionario. [9]

El ataque de fuerza bruta consiste en probar cada posible clave sobre un fragmento de texto cifrado hasta que se obtenga un mensaje legible de texto nativo. Por otra parte, el ataque de diccionario se basa en estudiar la naturaleza del algoritmo junto a algún conocimiento de las características generales del texto nativo con el fin de deducir un texto nativo concreto o encontrar la clave que se esté utilizando. Si la clave es descubierta, todos los mensajes cifrados con esta clave quedan seriamente amenazados. [20]

2.3.3.2 Cifrado simétrico o de clave privada

La técnica más utilizada históricamente para dar privacidad a los datos transmitidos es el cifrado simétrico o de clave privada. En el cifrado simétrico, las entidades de comunicación establecen y comparten una clave secreta que se utiliza después para cifrar y descifrar los mensajes. Un esquema de cifrado simétrico tiene los siguientes elementos (Ver figura 2.13): [12]

- **Texto nativo:** Es el mensaje original que va a ser cifrado y que constituye la entrada del algoritmo.
- **Algoritmo de cifrado:** Es un algoritmo que realiza varias transformaciones del texto nativo en base a operaciones simples sobre patrones de bits.
- **Clave secreta:** Es una entrada del algoritmo de cifrado. Los cambios que realice el algoritmo al texto nativo dependen de la clave.
- **Texto cifrado:** Es el mensaje alterado que produce el algoritmo de cifrado. Claves diferentes producen cifrados diferentes para un mismo mensaje.
- **Algoritmo de descifrado:** Es esencialmente el algoritmo de cifrado ejecutado inversamente. [20]

Figura 2.13 *Modelo de cifrado simétrico*

Una clave es un código secreto que utiliza el algoritmo de encriptación para crear una única versión de texto cifrado. Mientras mayor sea la longitud de la clave, será más difícil averiguar ésta. Por ejemplo una clave de 56 bits puede proporcionar 2^{56} diferentes combinaciones. [23]

Los algoritmos de encriptación simétrica más importantes son los llamados cifradores de bloque. Un cifrador de bloque procesa una entrada de texto nativo en bloques de tamaño fijo y produce un texto cifrado de igual tamaño por cada bloque de texto nativo. Los principales algoritmos de este tipo son DES y 3DES.

Estándar de Cifrado de Datos (DES, *Data Encryption Standard).* Creado en 1977, este algoritmo utiliza una clave simétrica de 56 bits para encriptar datos en

bloques de 64 bits. Una computadora personal común tardaría años en probar todas las combinaciones usando la fuerza bruta. Sin embargo, utilizando computadoras especiales es posible romper la encriptación en cuestión de segundos. Esto hace que DES ya no sea considerado un algoritmo seguro y no se debería usar en una VPN.

Estándar de Cifrado de Datos Triple (3DES). Debido a su debilidad, DES fue reforzado y se creó 3DES. Este algoritmo repite el algoritmo básico DES tres veces. Esto es, un texto es cifrado tres veces usando tres claves distintas. La longitud de la clave es de 168 bits. La desventaja de este algoritmo es que es lento, sin embargo da buena seguridad y es muy utilizado por IPSec para cifrar los datos. [20]

2.3.3.3 Cifrado asimétrico o de clave pública

El cifrado asimétrico o de clave pública fue propuesto por Diffie y Hellman en 1976. El cifrado asimétrico es un método donde cada usuario posee una pareja de claves relacionadas matemáticamente, donde se utiliza una clave para cifrar la información y la otra para descifrarla. Una de las claves se denomina clave pública, la cual puede darse a conocer ante todos los que quieran intercambiar información de forma segura con el usuario. La otra es la clave privada, la cual el usuario es dueño y no debe darla a conocer. Un esquema de cifrado asimétrico tiene los siguientes elementos: [12]

- Texto nativo.
- Algoritmo de cifrado
- Clave pública y privada
- Texto cifrado.
- Algoritmo de descifrado.

El procedimiento para cifrar mensajes utilizando claves públicas se muestra en la figura 2.14 y es explicado a continuación.

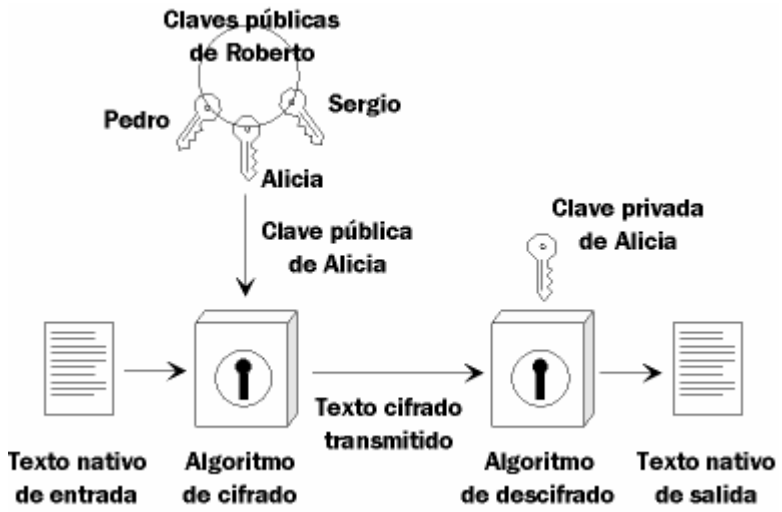

Figura 2.14 *Modelo de cifrado de clave pública*

1. Cada usuario genera un par de claves que van a ser utilizadas para el cifrado y descifrado de los mensajes.
2. Cada usuario publica una de las dos claves de cifrado en un registro público. Esta clave se convierte en pública y la otra permanece privada. Cada usuario puede tener las claves públicas de todos los usuarios con los que mantiene comunicación.
3. Si un usuario (*Roberto*) desea enviar un mensaje cifrado a otro (*Alicia*), él cifra el mensaje utilizando la clave pública de *Alicia*.
4. Cuando *Alicia* recibe el mensaje, lo descifra utilizando su clave privada. Nadie más puede descifrar el mensaje, ya que solamente *Alicia* conoce su propia clave. [20]

Así, todos los participantes tienen acceso a las claves públicas y cada uno de ellos genera localmente su propia clave privada. Mientras la clave privada permanezca en secreto, las comunicaciones serán seguras.

Los algoritmos de cifrado de clave pública más importante son el RSA y Diffie-Hellman.

Rivest Shamir Adleman (RSA). Es un algoritmo de clave pública creado en 1977 por Ron Rivest, Adi Shamir y Len Adleman. Este algoritmo goza de mucha popularidad. La longitud de su clave varía desde 512 a 2048 bits haciendo que sea un algoritmo de encriptación muy seguro.

Este algoritmo utiliza un número conocido como módulo público para conseguir las claves pública y privada. Este número se forma multiplicando dos números primos. La seguridad de este algoritmo se encuentra en el hecho de que aunque encontrar números primos grandes es relativamente fácil, hacer factor del resultado de multiplicar dos números primos resulta ser muy difícil. Si los números primos usados son muy grandes, el problema llega a ser computacionalmente imposible. RSA es ampliamente utilizado en certificados, los cuales utilizan muchas VPN para autenticar usuarios. [16]

Diffie-Hellman (D-H). Es un método de encriptación de clave pública el cual permite a dos partes que se comunican usando IPSec establecer una clave simétrica que sólo ellos conocen, aunque se estén comunicando sobre un canal inseguro.

Con Diffie-Hellman, cada par genera una clave pública y otra privada. La clave privada se mantiene secreta y nunca es compartida. La clave pública se calcula de la clave privada por cada parte y se intercambia sobre el canal inseguro. Cada par combina la clave pública del otro con su propia clave privada y calcula el mismo número secreto compartido. El número secreto compartido es convertido entonces en una clave secreta compartida. Esta clave nunca se intercambia sobre el canal inseguro.

D-H es muy importante porque la clave secreta compartida es utilizada para cifrar datos usando los algoritmos de encriptación de clave secreta especificados en las SA de IPSec, tales como DES o MD5. [45]

2.3.3.4 Funciones de dispersión (*hash*) unidireccionales

Las funciones de dispersión unidireccionales (*one-way hash function*) son muy utilizadas para la autenticación de datos, para la creación de firmas digitales y también son muy utilizadas por las tecnologías de autenticación de usuarios. Un conjunto de datos está autenticado si verdaderamente proviene del lugar de origen pretendido. La autenticación verifica que el mensaje sea auténtico y que no haya sido alterado.

Existen tres formas para autenticar un mensaje. La primera es utilizando cifrado simétrico. Si se supone que sólo el emisor y el receptor comparten la clave, se asegura la autenticación. El resumen del mensaje se puede cifrar usando cifrado de clave pública. Esto proporciona una firma digital, así como la autenticación de los mensajes y no requiere distribuir las claves a las partes que se comuniquen. La tercer forma es utilizando una función de dispersión. [21]

Las funciones de dispersión operan sobre un mensaje de longitud variable y produce un resumen del mensaje de longitud fija (*hash signature*). Estas funciones crean una huella digital electrónica única para un mensaje dado. Para autenticar un mensaje se envía con él un resumen del mensaje de forma que el resumen sea auténtico. Una función de dispersión tiene las siguientes propiedades y atributos:

1. La función puede ser aplicada a un bloque de datos de cualquier tamaño.
2. La función produce una salida de longitud fija.
3. Para cualquier valor dado, es relativamente fácil calcular su función por lo que la función se puede implementar en software y hardware.
4. La función es unidireccional porque es fácil generar un código dado un mensaje, pero prácticamente imposible generar un mensaje a partir de un código. De esta forma, el mensaje se mantiene secreto.
5. No se puede encontrar un mensaje alternativo que produzca el mismo valor que un mensaje dado. Con esto se impide la falsificación de un mensaje.

6. Una función de dispersión es fuerte si resiste un ataque llamado “ataque del cumpleaños”. [20]

Las funciones de dispersión más importantes son MD5 y SHA-1.

Resumen de Mensaje versión 5 (MD5, *Message Digest version 5).* Es un algoritmo de dispersión que autentica los datos de los paquetes. Tuvo versiones anteriores llamadas MD2 y MD4. Este algoritmo toma un mensaje de longitud variable y produce un resumen del mensaje (*hash*) de 128 bits. MD5 es muy utilizado por IPSec para la autenticación de datos. [56]

Algoritmo de Dispersión Segura versión 1 (SHA-1, *Security Hash Algorithm).* Es un algoritmo de dispersión el cual fue publicado como estándar en 1993. En 1995 se publicó una versión revisada conocida como SHA-1. Este algoritmo toma como entrada un mensaje con una longitud máxima de 2^{64} bits y produce un resumen del mensaje (*hash*) de 160 bits. La entrada se procesa en bloques de 512 bits. IPSec y los certificados utilizan ampliamente SHA-1 para la autenticación y las firmas digitales.

2.3.3.5 Firma digital

Una firma digital es utilizada con las claves públicas y se trata de un medio por el que los autores de un mensaje, archivo u otro tipo de información codificada digitalmente enlazan su identidad a la información. El proceso de firmar información digitalmente implica la transformación de la misma y de algunos datos secretos que guarda el remitente en una etiqueta denominada firma. [21]

Una firma digital es el equivalente electrónico de una firma manuscrita y tiene el mismo propósito. Las firmas digitales no deben ser falsificables, los receptores deben ser capaces de verificarlas y los firmantes no deben poder negarlas después. Una diferencia entre una firma manuscrita y una firma digital electrónica

es que ésta última no debe ser constante y debe ser función de los datos que acompaña, de lo contrario una misma firma podría ser utilizada en cualquier mensaje y también se podría alterar cualquier mensaje firmado. [12]

El cifrado de clave pública puede operar en conjunción con las funciones de dispersión unidireccionales para poder crear una firma digital. El proceso de creación de una firma digital y la verificación de su autenticidad usando estas técnicas criptográficas se muestra en la figura 2.15:

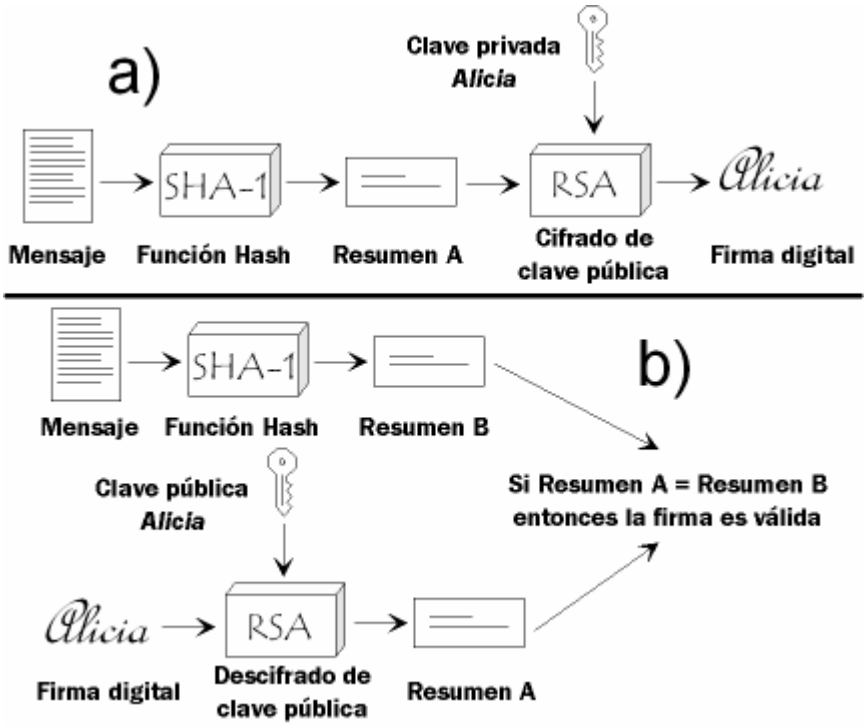

Figura 2.15 *Firma digital a) Creación b) Validación*

El inciso a) muestra la creación de la firma digital. *Alicia* crea la firma cifrando el resumen del mensaje producido por la función de dispersión usando su clave privada. En el inciso b) se muestra la validación de la firma. Cuando *Alicia* le envía un mensaje firmado a *Roberto*, éste lo valida comparando el resumen del mensaje que él genera localmente con el resumen obtenido al descifrar la firma usando la clave pública de *Alicia*. Si ambos resúmenes son exactamente iguales, entonces la firma es válida. [7]

Es necesario tomar en cuenta que una firma digital no ofrece privacidad, ya que un mensaje firmado puede ser leído por cualquier persona. Incluso si se cifra el mensaje completo, cualquier intruso puede descifrar el mensaje utilizando la clave pública del autor. Lo único que hace la firma digital es demostrar que el mensaje pertenece al verdadero autor que lo creó. [21]

2.3.4 Sistemas de autenticación de usuarios

Existen muchos mecanismos de autenticación de usuarios. Cada sistema de autenticación tiene sus ventajas y desventajas. Un sistema de autenticación es aquel donde un usuario se identifica ante un servidor remoto. En un VPN es muy importante identificar a los usuarios de la red para poder garantizar la seguridad. De los sistemas de autenticación aquí mencionados el más recomendable y utilizado en una VPN es PKI.

2.3.4.1 Autenticación basada en contraseña

La autenticación basada en contraseña es la más utilizada por los sistemas computacionales. En este mecanismo de autenticación, un usuario se identifica a sí mismo ante un servidor remoto al inicio de una sesión mediante una contraseña. La contraseña es un secreto compartido entre el usuario y el servidor remoto. El usuario recuerda la contraseña y el servidor almacena o una copia de ella o un valor calculado de la contraseña.

Aunque se trata de un método fácil de implementar y de usar, también resulta ser el más inseguro de todos. Si un intruso obtiene la contraseña, se puede hacer pasar como un usuario legítimo y entonces obtener todos los privilegios de acceso a la red que tenía el usuario legítimo. Cuando un usuario proporciona su nombre y su contraseña, cualquier atacante que esté observando (usando un *sniffer*) puede obtener la contraseña. Hasta que el usuario legítimo no cambie su contraseña, el

atacante podrá hacer todo lo que quiera. Es por eso que muchas organizaciones insisten en que sus usuarios cambien continuamente de clave.

Una autenticación basada en contraseña no proporciona autenticación mutua. La contraseña de un usuario lo autentica ante el servidor. Si el servidor necesitara autenticarse ante el usuario, se necesitaría otra contraseña. El hecho de que no exista autenticación mutua proporciona otra ventaja a un atacante, ya que éste puede crear un servidor falso que se haga pasar por el legítimo y así obtener todas las contraseñas de los usuarios que se autentican con el servidor. El principal protocolo de autenticación por contraseña es PAP el cual es utilizado por PPP.

2.3.4.2 Autenticación basada en desafíos

En este tipo de autenticación, el servidor genera un conjunto de datos aleatorio denominado desafío y se lo envía al usuario que desea autenticarse. En lugar de responder con una contraseña, el usuario cifra el desafío con una clave compartida sólo por el servidor y el usuario. El usuario envía su nombre y el texto cifrado al servidor. El servidor realiza la misma encriptación y entonces compara el texto cifrado enviado por el usuario con el texto cifrado generado localmente. Si ambos son iguales, la autenticación se lleva a cabo con éxito, de lo contrario el usuario será rechazado. [7]

Se pueden utilizar las funciones de dispersión para este tipo de autenticación. Este mecanismo permite que un usuario se autentique ante un servidor y se basa en la existencia previa de un secreto compartido previamente por ambos como puede ser una contraseña. El usuario presenta su nombre y el servidor genera un desafío. Entonces el usuario combina el desafío con la clave, le aplica una función de dispersión y devuelve el resultado. El servidor repite el cálculo usando su propia versión del secreto compartido. Si ambos son iguales, se autentica al usuario y sin necesidad de enviar la contraseña. [9]

Para prevenir los ataques de *sniffers*, este sistema de autenticación utiliza un secreto diferente por cada intento de autenticación. Este método es mejor que la contraseña porque un desafío diferente es enviado cada vez y así un atacante no podrá utilizar más de una vez el texto cifrado generado por el usuario para hacerse pasar por éste. Para que exista autenticación mutua, se requiere de un segundo desafío y su respectiva respuesta. El usuario puede proporcionar el segundo desafío junto con el primer desafío cifrado. Los protocolos de autenticación basados en este método son CHAP, MS-CHAP y EAP-MD5. [7]

2.3.4.3 Kerberos

Kerberos es un conjunto de servicios que proporcionan un sistema de autenticación basado en un Centro de Distribución de Claves (KDC, *Key Distribution Center*). Un KDC determina a qué sistemas se les permite comunicarse entre ellos. Cuando a dos sistemas se les permite comunicarse entre ellos, el KDC proporciona una clave de sesión para esa conexión. *Kerberos* fue diseñado para las redes TCP/IP y se basa en el cifrado simétrico. Además, comparte una clave secreta diferente con cada entidad en la red. [21] [17]

Kerberos fue creado en el Instituto Tecnológico de Massachussets (MIT) en 1980 para un proyecto denominado Atenea. *Kerberos* es muy popular principalmente en escuelas y universidades y apenas está ingresando en el mundo de las empresas. La versión utilizada actualmente es *Kerberos* 5, el cual corrige ciertas deficiencias respecto al *Kerberos* original: *Kerberos* 4. Se puede utilizar *Kerberos* como forma de autenticación para IPSec en lugar de utilizar una PKI. [9]

En un sistema *Kerberos* existen clientes y servidores. Los clientes pueden ser usuarios, sin embargo también pueden ser aplicaciones que requieran de privilegios para acceder a un determinado sistema. *Kerberos* mantiene una base de datos de los clientes y de sus claves secretas. En el caso de un usuario se trata

de una contraseña cifrada. Cualquiera que requiera autenticación necesita registrar su secreto con *Kerberos*. [17]

Debido a que *Kerberos* conoce los secretos de todos, puede crear mensajes que convenzan a un usuario que en realidad se está autenticando con el servidor con el que pretende autenticarse. *Kerberos* también crea claves de sesión que les son dadas a cada cliente y al servidor (o a dos clientes) y a nadie más. Una clave de sesión es utilizada para cifrar mensajes entre las dos partes que se comunican, después de la cual es destruida. [17]

2.3.4.4 Infraestructura de Claves Públicas (PKI)

Una Infraestructura de Claves Públicas (PKI, *Public Key Infraestructure*) basa su funcionamiento en el uso de certificados como sistema de autenticación de usuarios. Este es uno de los métodos de autenticación más utilizados en una VPN. Dada una clave pública, un usuario necesita saber quién posee la clave privada que está relacionada con dicha clave pública con el fin de poder comunicarse con él. La respuesta a este problema está en los certificados. La figura 2.17 muestra cómo se lleva a cabo la autenticación basada en certificados.

Una PKI consta de varios componentes que facilitan su administración. Cada componente tiene asignada una tarea específica y deben estar presentes en cualquier PKI. Los componentes de una PKI son:

- Certificados
- Autoridad de Certificación (CA, *Certification Authority*)
- Autoridad de Registro (RA, *Registration Authority*)
- Repositorio
- Archivo [7]

Certificados: Un certificado es un objeto digital que relaciona una clave pública con una persona u organización. Con el fin de distribuir claves públicas de una forma segura y asegurar su integridad, se certifican las claves públicas que pertenecen a las personas, empresas y toda clase de organizaciones que se encuentran en Internet. Al usar certificados, un usuario puede estar seguro de que está utilizando la clave pública de otro usuario y que por lo tanto, ese usuario firmó el mensaje. [7] [21]

Un certificado contiene el nombre del usuario y su clave pública. El certificado puede indicar la organización a la cual pertenece el usuario, así como también su correo electrónico. El certificado también posee la fecha de activación y la fecha en que caduca. También posee el nombre de la organización confiable que creó el certificado. Esta organización incluye un número de serie que identifica a cada certificado de manera única. Por último, la organización confiable firma digitalmente el certificado usando su propia clave privada. Un ejemplo de un certificado se muestra en la figura 2.16. [7]

Figura 2.16 *Ejemplo de un certificado*

Los certificados son muy importantes dentro de una VPN. Cuando un cliente inicia una sesión en la red de una empresa desde un sitio remoto a través de una VPN, el servidor VPN puede presentar un certificado de servidor para establecer su identidad. Dado que la entidad raíz corporativa es de confianza y la entidad

emisora de certificados de raíz corporativa emitió el certificado del servidor VPN, el equipo cliente puede proseguir con la conexión y el empleado sabe que su equipo está realmente conectado al servidor VPN de su organización.

El servidor VPN también tiene que poder autenticar al cliente VPN antes de empezar a intercambiar datos sobre la conexión VPN. Se puede dar la autenticación a nivel de equipo con el intercambio de certificados de equipo o la autenticación a nivel de usuario a través de un método de autenticación Protocolo punto a punto (PPP).

El certificado del equipo cliente puede servir para varios propósitos, la mayor parte de los cuales están basados en la autenticación, permitiendo que el cliente utilice muchos recursos organizativos sin la necesidad de certificados individuales para cada recurso. Por ejemplo, el certificado de cliente podría permitir conectividad VPN además de acceso al sitio intranet de la compañía, a servidores de productos y a una base de datos.

El certificado del servidor VPN también podría servir para varios propósitos. El mismo certificado podría tener el propósito de comprobar la identidad de servidores de correo electrónico, servidores Web o servidores de aplicaciones. La entidad emisora de certificados que emite el certificado determina el número de propósitos de cada certificado. [48]

Para estandarizar el formato de los certificados, se ha diseñado un estándar conocido como X.509 el cual es ampliamente utilizado en Internet. X.509 es una forma de describir certificados. Lo hace utilizando varios campos entre los más importantes se encuentran en la tabla 2.1. [21]

Campo	Significado
Versión	La versión del X.509
Número de serie	El número que identifica al certificado de forma única
Algoritmo de firma	El algoritmo utilizado para firmar el certificado
Emisor	El nombre X.500 de la CA
Valido desde	Fecha de inicio de validez del certificado
Valido hasta	Fecha de fin de validez del certificado
Asunto	La entidad cuya clave se está certificando
Clave pública	La clave pública del sujeto y el ID del algoritmo usado para crearla
Emisor	Un ID opcional que identifica de forma única al emisor del certificado
Sujeto	Un ID opcional que identifica de manera única al ID del certificado
Extensiones	Existen varias extensiones
Firma digital	La firma del certificado firmada por la clave privada de la CA

Tabla 2.1 *Campos de un certificado según el estándar X.509*

Un certificado puede ser revocado cuando termina su validez o si una persona u organización hace un mal uso de él o si alguna clave privada se ha expuesto. La herramienta que utiliza una PKI para comprobar si un certificado es válido o no es la Lista de Revocación de Certificados (CRL, *Certificate Revocation List*) La CRL contiene la lista de todos los números de serie de certificados que ya han expirado o que ya no son confiables. La entidad confiable se encarga de publicar la CRL de forma frecuente para que cualquiera pueda verla.

Autoridad de Certificación (CA, *Certification Authority).* Es el componente más importante de una PKI. Una CA es la entidad confiable encargada de crear, firmar y distribuir certificados. Una CA es el conjunto de software, hardware y las personas que la operan.

Una CA tiene seis responsabilidades fundamentales que debe cumplir. La primera y la más importante es proteger su clave privada utilizando software o hardware como tarjetas inteligentes o de lo contrario la seguridad se verá comprometida. La segunda es verificar la información de un certificado antes de que sea distribuido, es decir, los datos del poseedor del certificado. La tercera es asegurar que todos los certificados y CRL cumplen con su perfil, esto es, si por ejemplo una CA sólo

distribuye certificados para correo electrónico, no podrá existir un certificado de esa CA donde se autorice su uso para firmar un contrato. La cuarta es mantener una lista de los certificados que ya no son confiables, es decir que han expirado o han sido revocados. La quinta es distribuir los certificados y CRL para que puedan ser utilizados por los usuarios. La sexta y última responsabilidad es mantener un archivo de todos los certificados que ha tenido la CA. Las principales CA son las siguientes:

- Entrust
- GTE Cybertrust
- Network Associates PGP
- Baltimore
- Microsoft
- Verisign

Autoridad de Registro (RA, *Registration Authority).* Es la entidad que verifica el contenido de un certificado. El contenido de un certificado debe reflejar la información presentada por la entidad que solicita el certificado. Por ejemplo, una compañía puede solicitar un certificado para un usuario de cierto departamento y darle la autoridad para que firme algún contrato. Entonces la RA escribe en el certificado la información de la compañía, el departamento y la autoridad que tiene el usuario. Después, la RA proporciona esta información a la CA.

Repositorio. Un repositorio distribuye los certificados y las listas de revocación. Un repositorio acepta los certificados y CRL de una o varias CA y los hace disponibles a las organizaciones que los requieren para implementar servicios de seguridad.

Archivo. Se encarga de almacenar la información de los certificados de la CA. El archivo permite demostrar que la información es confiable al momento de recibirla y que no ha sido modificada mientras está en el archivo. [7]

Figura 2.17 *Autenticación basada en certificados*

2.3.4.5 Servidores RADIUS

El Servicio de Usuario de Marcación para Autenticación Remota (RADIUS, *Remote Authentication Dial-In User Service*) es un estándar para un sistema de autenticación de acceso remoto. Provee la funcionalidad de autenticación, autorización y contabilidad (AAA, *Authentication, Authorization, Accounting*) la cual es muy importante para el control de acceso.

RADIUS por si mismo no provee buenos métodos de autenticación, sin embrago, RADIUS puede utilizar diferentes protocolos de autenticación para proveer mejor servicio como PAP, CHAP, MS-CHAP y EAP.

RADIUS es un protocolo y software cliente-servidor, el cual es utilizado por los dispositivos o aplicaciones NAS y servidores VPN para autenticar usuarios remotos y autorizarlos para que puedan acceder a los recursos de la red. Un servidor que ejecuta el servicio RADIUS es comúnmente conocido como servidor RADIUS. RADIUS es utilizado frecuentemente como Sistema de Autenticación Central el cual provee la autenticación, autorización y control para los usuarios remotos. [58]

El servidor de RADIUS recibe una solicitud de conexión de usuario desde el NAS y autentifica al cliente contra su base de datos de autenticación. Asimismo, un servidor RADIUS mantiene una base de datos de almacenamiento central de otras propiedades relevantes de usuario. Además de la simple respuesta de sí/no a una solicitud de autenticación, RADIUS puede informar al NAS sobre otros parámetros de conexión aplicables para el usuario, tales como el tiempo máximo de sesión, asignación de dirección IP estática, e información de llamada de respuesta.

RADIUS puede responder a las solicitudes de autenticación basada en su propia base de datos, o puede ser un componente frontal para otro servidor de base de datos, como lo son el servidor genérico de conectividad de base de datos abierta o el controlador de dominio primario. Este último servidor puede ubicarse en la misma máquina del servidor RADIUS, o puede centralizarse en otra parte. Además, un servidor RADIUS puede actuar como un cliente proxy para un servidor RADIUS remoto.

EAP y RADIUS. Cuando se utiliza EAP junto con RADIUS se requieren cambios tanto para NAS como para RADIUS. Para la autenticación tradicional, la interacción NAS/RADIUS es un intercambio único de solicitud/respuesta. Pero en una autenticación EAP, NAS no puede recopilar información del cliente para la autenticación EAP a través de RADIUS, debido a que la información que RADIUS ha habilitado por EAP necesita estar oculta desde el NAS. Para resolver este problema, los administradores del sistema pueden configurar al NAS para que envíe un mensaje de identidad EAP al cliente, el cual a su vez envía el nombre de usuario y los datos de dominio al NAS. NAS presenta estos datos a RADIUS en una solicitud EAP- START, y luego se vuelve transparente para el resto del proceso de autenticación. RADIUS envía y contesta los mensajes EAP a través de NAS al cliente hasta que la autenticación sea satisfactoria o falle. [32]

2.3.4.6 Protocolos de autenticación

Protocolo de autenticación de contraseña (PAP, *Password Authentication Protocol).* El PAP es un protocolo de autenticación simple en el que el nombre de usuario y la contraseña se envían al servidor de acceso remoto como texto simple (sin cifrar). No se recomienda utilizar PAP, ya que las contraseñas pueden leerse fácilmente a partir de los paquetes de PPP intercambiados durante el proceso de autenticación. PAP suele utilizarse únicamente al conectarse a servidores de acceso remoto antiguos basados en UNIX que no admiten otros métodos de autenticación.

Protocolo de autenticación de contraseña de Shiva (SPAP, *Shiva Password Authentication Protocol).* El SPAP es un protocolo simple de autenticación de contraseña cifrada compatible con servidores de acceso remoto de Shiva. Con SPAP, el cliente de acceso remoto envía una contraseña cifrada al servidor de acceso remoto. SPAP utiliza un algoritmo de cifrado bidireccional. El servidor de acceso remoto descifra la contraseña y utiliza el formato sin cifrar para autenticar al cliente de acceso remoto.

Protocolo de Autenticación por Desafío (CHAP, *Challenge Authentication Protocol).* CHAP es un método de autenticación muy utilizado en el que se envía el conocimiento de la contraseña del usuario, no la propia contraseña. Con CHAP, el servidor de acceso remoto envía una cadena de desafío al cliente de acceso remoto. El cliente de acceso remoto utiliza la cadena de desafío y la contraseña del usuario, y calcula un resumen MD5. El resumen MD5 se envía entonces al servidor de acceso remoto. El servidor de acceso remoto, que tiene acceso a la contraseña del usuario, realiza el mismo cálculo del resumen y compara el resultado con el resumen enviado por el cliente. Si coinciden, las credenciales del cliente de acceso remoto se consideran auténticas.

Protocolo de Autenticación por Desafío de Microsoft (MS-CHAP, *Microsoft Challenge Authentication Protocol).* Microsoft creó MS-CHAP para autenticar estaciones de trabajo Windows remotas, proporcionando la funcionalidad a la que los usuarios de redes LAN están habituados e integrando los algoritmos de dispersión utilizados en las redes Windows. Al igual que CHAP, MS-CHAP utiliza un mecanismo de desafío y respuesta para evitar el envío de la contraseña durante el proceso de autenticación.

MS-CHAP utiliza el algoritmo de dispersión Resumen del Mensaje 4 (MD4) y DES para generar el desafío y la respuesta, y ofrece mecanismos para informar de errores de conexión y para cambiar la contraseña del usuario. El paquete de respuesta está en un formato diseñado específicamente para funcionar con productos de redes en sistemas operativos Windows. [48]

Protocolo de autenticación extensible (EAP, *Extensible Autenthication Protocol).* EAP fue diseñado originalmente para proveer una interfase estándar para opciones de autenticación adicionales para PPP. EAP admite métodos de autenticación arbitrarios que utilizan intercambios de credenciales e información de longitudes arbitrarias. EAP se desarrolló como respuesta a una creciente demanda de métodos de autenticación que utiliza otros dispositivos de seguridad y ofrece una arquitectura estándar para permitir métodos de autenticación adicionales dentro de PPP. [58] [48]

Al utilizar EAP, se pueden agregar varios esquemas de autenticación conocidos como tipos de EAP, entre los que se incluyen tarjetas de identificación, contraseñas de un solo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros. EAP, junto con los tipos de EAP seguros, es un componente tecnológico crítico para las conexiones VPN seguras. Los tipos de EAP seguros, como los basados en certificados, ofrecen mayor seguridad frente a ataques físicos o de diccionario, y de investigación de contraseñas, que otros

métodos de autenticación basados en contraseña, como CHAP o MS-CHAP. Existen dos tipos de EAP: [58] [48]

- EAP-MD5
- EAP-TLS.

EAP-MD5 es un protocolo de autenticación que es semejante en su funcionamiento a CHAP.

EAP-TLS es utilizado para autenticación basada en certificados de usuario. Se trata de un método de autenticación mutua, lo que significa que tanto el cliente como el servidor deben demostrar sus identidades uno a otro. Durante el intercambio EAP-TLS, el cliente de acceso remoto envía su certificado de usuario y el servidor de acceso remoto envía su certificado de equipo. Si el certificado no se envía o no es válido, se termina la conexión. [48]

3

Tecnologías de las VPN

En este capítulo se explican los protocolos más importantes que hacen que una VPN pueda funcionar. Existen varios, pero los más importantes son PPTP, L2TP e IPSec. Cada protocolo tiene sus ventajas y desventajas, así que corresponde al diseñador y administrador de la VPN determinar cual es el más conveniente para una organización en particular.

3.1 Protocolo de Túnel Punto a Punto (PPTP)

3.1.1 Definición de PPTP

El Protocolo de Túnel Punto a Punto (PPTP, *Point-to-Point Tunneling Protocol*) es un protocolo de red creado por Microsoft, Ascend Communications y US Robotics el cual permite la realización de transferencias seguras desde clientes remotos a servidores emplazados en redes privadas, empleando para ello tanto líneas telefónicas conmutadas como Internet.

En el escenario típico de PPTP, el cliente establecerá una conexión *dial-up* con el servidor de acceso a red (NAS) del proveedor del servicio, empleando para ello el protocolo PPP. Una vez conectado, el cliente establecerá una segunda conexión con el servidor PPTP el cual estará situado en la red privada. Dicho servidor será utilizado como intermediario de la conexión, recibiendo los datos del cliente externo y transmitiéndolos al correspondiente destino en la red privada. PPTP está documentado en el RFC 2637. [57]

PPTP es una extensión de PPP, el cual es utilizado tradicionalmente para las conexiones dial-up. PPTP fue diseñado principalmente para las VPN de acceso remoto, sin embargo también puede trabajar en las VPN de sitio a sitio. PPTP opera en la capa 2 del modelo OSI. [22]

PPTP encapsula los paquetes PPP en datagramas IP. Una vez que los datagramas llegan al servidor PPTP, son desensamblados con el fin de obtener el paquete PPP y descifrados de acuerdo al protocolo de red transmitido. Por el momento, PPTP únicamente soporta los protocolos de red IP, IPX, y NetBEUI. PPTP especifica además una serie de mensajes de control con el fin de establecer, mantener y destruir el túnel PPTP. Estos mensajes son transmitidos en paquetes de control en el interior de segmentos TCP. De este modo, los paquetes

de control almacenan la cabecera IP, la cabecera TCP y el mensaje de control PPTP.

En el caso de Microsoft, la autenticación utilizada para el acceso a los RAS soporta los protocolos CHAP, MS-CHAP, PAP, y debido a los problemas de seguridad, en versiones posteriores también se usa EAP. En cuanto a la encriptación de datos, PPTP utiliza el proceso de encriptación de secreto compartido en el cual sólo los extremos de la conexión comparten la clave. Dicha clave es generada empleando el protocolo MPPE a partir de la contraseña del usuario. [57]

PPTP permanece como una opción popular para implementar VPN gracias a Microsoft. El cliente PPTP se distribuye gratuitamente en todas las versiones de estación de trabajo Windows, mientras que el servidor PPTP se instala junto con los sistemas operativos de servidor Windows. PPTP puede ser también implementado en sistemas Linux así como en Macintosh. También diversos modelos de *firewalls* soportan PPTP, tales como servidores ISA, PIX de Cisco y SonicWall. [22] [59]

Una desventaja que tiene PPTP es que no posee un único estándar para la encriptación y la autenticación, ya que PPTP se ocupa únicamente de crear un túnel. Además, PPTP es el protocolo VPN menos seguro. L2TP e IPSec ofrecen mejores alternativas para garantizar la seguridad en una VPN. [22]

3.1.2 Estructura de PPTP

3.1.2.1 Concentrador de Acceso PPTP (PAC)

El Concentrador de Acceso PPTP (PAC, *PPTP Access Concentrator*) es un dispositivo conectado a las líneas PSTN o ISDN capaz de realizar operaciones PPP y de manejar el protocolo PPTP. Lo único que necesita el PAC es

implementar TCP/IP para transportar el tráfico hacia uno o más PNS. También puede entunelar protocolos que no son IP. Es también conocido como FEP o Procesador Final Frontal.

3.1.2.2 Servidor de Red PPTP (PNS)

El Servidor de Red PPTP (PNS, *PPTP Network Server*) es un dispositivo que opera como un servidor de túnel. Puesto que PPTP se basa completamente en TCP/IP y es independiente de la interfase de hardware, el PNS puede utilizar cualquier combinación de hardware incluyendo dispositivos LAN y WAN.

3.1.2.3 Conexión de control

Antes de que PPP pueda ser entunelado entre un PAC y un PNS, se debe establecer una conexión de control entre ambos dispositivos. La conexión de control es una sesión TCP estándar sobre la cual pasa el control de la llamada PPTP y la administración de la información. El control de la sesión está asociado lógicamente pero separado de las sesiones que son entuneladas a través de un túnel PPTP. Para cada pareja PAC-PNS existe tanto un túnel como una conexión de control. La conexión de control es responsable de establecer, administrar y liberar las sesiones transportadas a través del túnel.

Mensajes de control. PPTP define un conjunto de mensajes enviados como datos TCP en la conexión de control entre un PAC y un PNS. La sesión TCP para establecer la conexión de control es establecida al iniciar una conexión TCP en el puerto 1723. El conexión de control puede ser establecido tanto por el PNS como por el PAC. Cada mensaje inicia con una cabecera de ocho octetos fija. Dicha cabecera contiene la longitud total del mensaje, el indicador del tipo de mensaje PPTP y una constante conocida como *Magic Cookie*. [39]

La *Magic Cookie* es siempre enviada como la constante 0x1A2B3C4D. Su propósito es permitirle al receptor asegurarse de que está sincronizado adecuadamente con el flujo de datos TCP.

Los mensajes utilizados para mantener el control de las conexiones PPTP se muestran en la tabla 3.1.

Código	Nombre	Descripción
1	Start-Control-Connection-Request	Inicia el establecimiento de la sesión PPTP
2	Start-Control-Connection-Reply	Es la respuesta al mensaje 1. Contiene un código resultante que indica el éxito o el fracaso del establecimiento de la sesión así como el número de la versión del protocolo
3	Stop-Control-Connection-Request	Es una petición para cerrar el conexión de control
4	Stop-Control-Connection-Reply	Es la respuesta al mensaje 3. Contiene el código resultante que indica el éxito o fracaso del cierre de la conexión
5	Echo-Request	Enviado periódicamente tanto por el cliente como por el servidor para mantener activa la conexión
6	Echo-Reply	Es la respuesta al mensaje 5 para indicar que la conexión sigue activa
7	Outgoing-Call-Request	Es una petición enviada por el cliente para crear un túnel
8	Outgoing-Call-Reply	Es la respuesta al mensaje 7, la cual contiene un identificador único para ese túnel
9	Incoming-Call-Request	Es una petición del cliente para recibir una llamada entrante por parte del servidor
10	Incoming-Call-Reply	Es la respuesta al mensaje 9. Esta indica si la llamada entrante debería ser contestada
11	Incoming-Call-Connected	Es la respuesta al mensaje 10. Provee parámetros de llamada adicionales al servidor
12	Call-Clear-Request	Es una petición para desconectar o una llamada entrante o saliente, enviada del servidor al cliente
13	Call-Disconnect-Notify	Es una respuesta al mensaje 12 para indicar que se realizará la desconexión y las razones para hacerlo
14	WAN-Error-Notify	Notifica que un error ha ocurrido en la conexión WAN, esto es, en la interfase que soporta PPP
15	Set-Link-Info	Notifica cambios en las opciones PPP

Tabla 3.1 *Mensajes de control de conexión en PPTP* [22]

Códigos de error. Los códigos de error determinan si ocurrió un error en la conexión PPTP. En la tabla 3.2 se muestra cuáles pueden ser estos errores.

Código	Nombre	Descripción
0	None	No hay error
1	Not-connected	Todavía no existe un 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 valores de algún campo está fuera de rango o un campo reservado no está en ceros
4	No-Resource	Recursos insuficientes para manejar este comando
5	Bad-Call-ID	El identificador de llamada es incorrecto
6	PAC-Error	Un error específico ocurrió en el PAC

Tabla 3.2 *Códigos de error en PPTP*

3.1.2.4 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. [39]

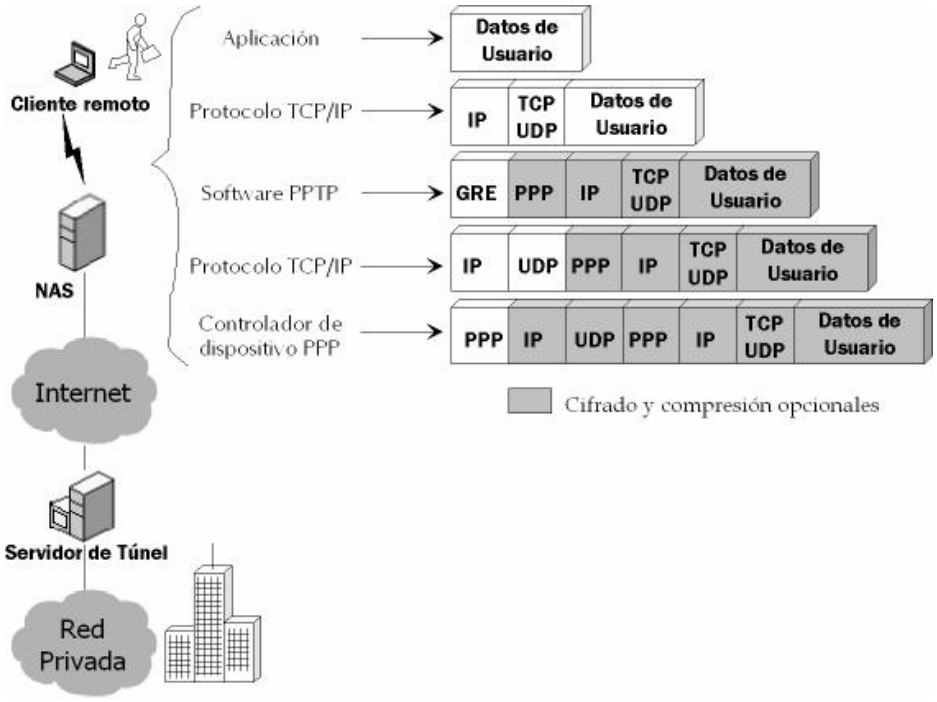

Figura 3.1 *Construcción de un paquete PPTP*

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. [8]

Encapsulación Genérica para Ruteo (GRE, *Generic Routing Encapsulation).* Es un protocolo para encapsular cualquier protocolo de la capa de red dentro de cualquier otro protocolo de la capa de red. El GRE es utilizado normalmente utilizado también para servicios VPN. GRE no posee mecanismos de seguridad y debe ser combinado por ejemplo con IPSec para que los datos viajen seguros. [41] [19]

La cabecera GRE utilizada en PPTP, la cual aparece en la figura 3.2, contiene una pequeña mejora que la hace diferente del protocolo GRE original. Esta diferencia consiste en incluir un número de reconocimiento el cual es utilizado para determinar si un paquete o grupo de paquetes GRE en particular ha alcanzado el otro extremo del túnel. Sin embargo, no se utiliza en la retransmisión de paquetes, sino que se utiliza para determinar la frecuencia con que deben ser transmitidos los paquetes a través del túnel para una determinada sesión.

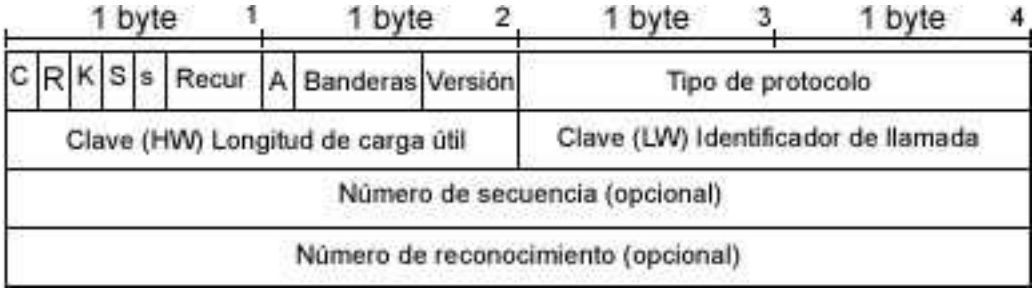

Figura 3.2 *Cabecera GRE mejorada*

La cabecera GRE es descrita a continuación:

- C indica chequeo de suma presente. Se establece en 0.
- R indica ruteo presente. Se establece en 0.
- K indica clave presente. Se establece en 1.
- S indica número de secuencia presente. Se establece en 1 si un paquete de datos está presente, de lo contrario se establece en 0.
- s indica ruta de fuente estricta. Se establece en 0.
- Recur indica control de la recursión. Se establece en 0.
- A indica número de secuencia de reconocimiento presente. Se establece en 1 si el paquete contiene número de reconocimiento para ser usado en el reconocimiento de tramas previamente transmitidas.
- Banderas siempre están en 0.
- Versión siempre está en 1.
- Tipo de protocolo se establece en 880B hexadecimal.
- Clave (HW) indica tamaño de la carga útil.

- Clave (LW) contiene el indicador de llamada para la sesión a la cual pertenece el paquete.
- Número de secuencia contiene el número de secuencia de la carga útil. Presente si S está en 1.
- Número de reconocimiento contiene el número del paquete GRE con el número más grande recibido durante la sesión. Presente si A está en 1. [39]

3.1.3 Seguridad en PPTP

PPTP por sí solo no proporciona ningún mecanismo de seguridad. Si los datos que atraviesan el túnel no son cifrados, cualquier usuario no autorizado puede apropiarse de la información. PPTP requiere de protocolos adicionales para poder autenticar usuarios y encriptar la información.

3.1.3.1 Autenticación y control de acceso

Un servidor PPTP actúa como una puerta de enlace a una VPN, es decir, se encarga de controlar todo el acceso a una VPN. La autenticación de los clientes remotos PPTP se realiza utilizando los métodos de autenticación de PPP. Como ya se vio anteriormente, los protocolos de autenticación que usa PPP son CHAP, MS-CHAP y PAP. En los sistemas Windows los clientes PPTP deben proporcionar un nombre de usuario y una clave para poder ser autenticados.

En cuanto a las cuentas de los usuarios, éstas son almacenadas en un directorio del servidor Windows y son administradas a través del administrador de usuarios para dominios, lo cual proporciona una administración centralizada. Sólo las cuentas que tienen permiso de acceso a la VPN a través de un dominio confiable son permitidas. Se requiere de una administración muy cuidadosa de las cuentas para reducir lo más posible los riesgos en la seguridad.

Después de la autenticación, todo el acceso a una LAN privada debe seguir un modelo de seguridad estricto. Todo acceso a los recursos de la red debe de tener los permisos apropiados. [8]

Debido a problemas de seguridad que ha tenido PPTP, se ha incluido el uso de EAP para la autenticación. EAP mejora notablemente la seguridad de las VPN basadas en PPTP. Una ventaja de PPTP es que no requiere del uso de una PKI, sin embargo, EAP requiere de certificados digitales para la autenticación mutua y así elevar la seguridad al máximo. [59]

3.1.3.2 Cifrado de datos

Para el cifrado de los datos, PPTP utiliza un modelo de cifrado simétrico, es decir, se utiliza una clave secreta compartida por ambas partes que se van a comunicar. La clave secreta es la contraseña de usuario. PPTP utiliza los esquemas de compresión y cifrado de PPP. El Protocolo de Control de Compresión (CCP, *Compression Control Protocol*) es utilizado por PPP para negociar la encriptación. PPTP hace uso del protocolo MPPE para poder cifrar la información. [8]

Cifrado Punto a Punto de Microsoft (MPPE, *Microsoft Point-to-Point Encryption).* Es un protocolo que cifra los datos de las conexiones PPP de acceso telefónico o de las conexiones VPN basadas en PPTP. Los esquemas de cifrado MPPE compatibles son: de alto nivel (clave de 128 bits) y estándar (clave de 40 bits). MPPE proporciona seguridad a los datos entre la conexión PPTP y el servidor de túnel. Para crear la clave se utiliza el estándar de cifrado RSA RC4. Esta clave es utilizada para encriptar todos los datos que atraviesan Internet, manteniendo la conexión privada y segura.

La versión de 40 bits se puede utilizar en todo el mundo; está integrada en todos los equipos que ejecutan Windows. El nivel de cifrado de 128 bits sólo está

disponible en EE.UU. y Canadá. Es posible habilitar la versión de 128 bits si instala una versión de software específica en el cliente y en el servidor. [51]

En un principio MPPE cambiaba la clave de encriptación cada 256 paquetes o cuando se perdía un paquete. Si el paquete perdido era detectado por el receptor, éste enviaba una solicitud autenticada al emisor para cambiar la clave a fin de resincronizar. Este comportamiento permitía que un intruso emprendiera un ataque de negación de servicio a través de la modificación del contabilizador en un paquete MPPE, o rechazando una petición de resincronización. Para manejar este problema, en PPTP de manera predeterminada las claves MPPE ahora se cambian de manera predeterminada en cada paquete. Este cambio evita el ataque a la resincronización de claves. [32]

3.1.3.3 Filtrado de paquetes PPTP

El filtrado de paquetes PPTP es una característica muy importante. El administrador de red puede decidir que sólo los usuarios PPTP tengan permiso de conectarse a la red corporativa a través de Internet. Todos los paquetes que no son PPTP son filtrados lo que evita el riesgo de que alguien ataque la VPN a través del servidor PPTP.
Cuando el filtro de paquetes PPTP es activado, el servidor PPTP de la VPN acepta y enruta sólo los paquetes de usuarios autenticados. Esto evita que todos los demás paquetes que no son PPTP puedan ingresar a la VPN. Esto asegura que sólo los datos cifrados autorizados entran y salen de la LAN privada.

3.1.3.4 Utilizar PPTP con *firewalls* y *routers*

El tráfico PPTP utiliza el puerto TCP 1723, y el protocolo IP utiliza el ID 47, de acuerdo a la IANA. PPTP puede ser utilizado en la mayoría de los *firewalls* y *routers* al activar el tráfico destinado al puerto 1723 para que sea enrutado a través del *firewall* o *router*.

Los *firewalls* protegen la seguridad de una red empresarial a regular de forma estricta los datos que llegan a la VPN a través de Internet. Una organización puede desplegar un servidor Windows PPTP detrás del *firewall*. El servidor PPTP acepta los paquetes PPTP que llegan del exterior a través del *firewall* y extraer la trama PPP del datagrama IP, descifrar el paquete y enviarlo a la computadora destino dentro de la VPN. [8]

3.2 Protocolo de Túnel de Capa 2 (L2TP)

3.2.1 Reenvío de Capa 2 (L2F)

El protocolo de Reenvío de Capa Dos (L2F, *Layer 2 Forwarding*) tiene como objetivo proporcionar un mecanismo de *tunneling* para el transporte de tramas a nivel de enlace de datos del modelo OSI (HDLC, PPP, SLIP, etc). L2F es un protocolo de encapsulamiento creado por Cisco Systems.

Entre las principales ventajas que ofrece el protocolo L2F cabe destacar el soporte multiprotocolo, la multiplexación de múltiples sesiones remotas (minimizando el número de túneles abiertos en un momento dado), y la gestión dinámica de los túneles, en la cual los recursos de los servidores de acceso a la red se minimizan al iniciar los túneles únicamente cuando existe tráfico de usuario.

Además, por cada túnel L2F establecido, el proceso de seguridad genera una clave aleatoria como medida de prevención ante posibles ataques basados en *spoofing*. A su vez, en el interior de los túneles, cada una de las sesiones multiplexadas mantendrá un número de secuencia para evitar problemas debidos a la duplicidad de paquetes. L2F sólo puede funcionar en túneles obligatorios. [57]

Este protocolo no fue muy popular y se comenzó entonces a trabajar en un nuevo protocolo que combinara las mejores características de L2F con PPTP. El resultado fue la creación de L2TP.

3.2.2 Definición de L2TP

El Protocolo de Túnel de Capa 2 (L2TP, *Layer 2 Tunneling Protocol*) es un protocolo estándar diseñado para transmitir datos y conectar de forma segura redes a través de Internet. Aceptado ya por la mayoría de firmas y vendedores de productos de conectividad, se prevé que en un futuro inmediato constituya una de

las funciones más revolucionarias, importantes, y usadas, por todo tipo de redes de datos mundiales en la creación de VPN.

L2TP es un protocolo estándar aprobado por el IETF (*Internet Engineering Task Force*), en oposición al protocolo propietario de Microsoft PPTP. L2TP se encuentra documentado en el RFC 2661. Es soportado prácticamente por la totalidad de firmas del mercado de la comunicación de datos, incluyendo Microsoft y Cisco. L2TP es una extensión del Protocolo Túnel Punto a Punto usado por los ISP para permitir la operación de VPN sobre Internet. L2TP emerge de la fusión de las mejores características de los protocolos PPTP de Microsoft y L2F de Cisco. L2TP encapsula las tramas PPP que van a enviarse a través de redes IP, X.25, *Frame Relay*, o ATM.

Cuando está configurado para utilizar IP como su transporte, L2TP se puede utilizar como protocolo de túnel VPN en Internet. L2TP utiliza UDP para mantener el túnel y para enviar tramas PPP encapsuladas en L2TP como datos del túnel. Las tramas PPP encapsuladas se pueden cifrar o comprimir. Cuando los túneles L2TP aparecen como paquetes IP, pueden hacer uso de IPSec, en una configuración denominada L2TP/IPSec, lo cual proporciona gran seguridad cuando se transportan datos en redes públicas IP.

L2TP se diseñó específicamente para conexiones de acceso remoto, así como para conexiones sitio a sitio. Mediante la utilización del protocolo PPP, L2TP gana compatibilidad multiprotocolo para protocolos como IPX y *AppleTalk*.

L2TP también proporciona una amplia gama de opciones de autenticación de usuario, incluidos CHAP, MS-CHAP, MS-CHAPv2 y EAP que admite mecanismos de autenticación de tarjetas *token* y tarjetas inteligentes. L2TP requiere preferentemente del uso de certificados digitales para la autenticación. L2TP es soportado por diferentes sistemas operativos así como *routers* y *firewalls*. [43]

3.2.3 Estructura de L2TP

3.2.3.1 Concentrador de Acceso L2TP (LAC)

Es un nodo que actúa en un extremo del túnel L2TP y trabajo junto con el LNS. El envío de paquetes entre el LAC y el LNS requiere de la creación de un túnel utilizando el protocolo L2TP. La conexión del LAC al sistema remoto puede ser local o a través de un enlace PPP. [40]

El LAC es un dispositivo físico que se añade a los elementos de interconexión de la red conmutada; como lo es la red telefónica convencional RDSI, o se coloca con un sistema de terminación PPP capaz de gestionar el protocolo L2TP. Un LAC sólo necesita implementar el medio sobre el cual opera el L2TP para admitir el tráfico de una o más LNS. El LAC puede entunelar cualquier protocolo que incluya el PPP además, es el iniciador de las llamadas entrantes y el receptor de las llamadas salientes. Un servidor de Acceso a la Red (NAS) es un LAC.

3.2.3.2 Servidor de Red L2TP (LNS)

Un LNS opera sobre cualquier plataforma con capacidad de terminación PPP. El LNS gestiona el lado del servidor del protocolo L2TP. Ya que L2TP se apoya sobre el medio al que llegan los túneles L2TP, LNS sólo puede tener una única interfaz LAN o WAN, aunque es capaz de terminar las llamadas entrantes en cualquiera de la amplia gama de las interfaces PPP LAC (asíncronos, RDSI, PPP sobre ATM, PPP sobre *Frame Relay*) [43]

3.2.3.3 Topología L2TP

El objetivo de L2TP es entunelar tramas PPP entre el sistema remoto o cliente LAC y el LNS ubicado en una LAN privada. La topología típica de L2TP se muestra en la figura 3.3.

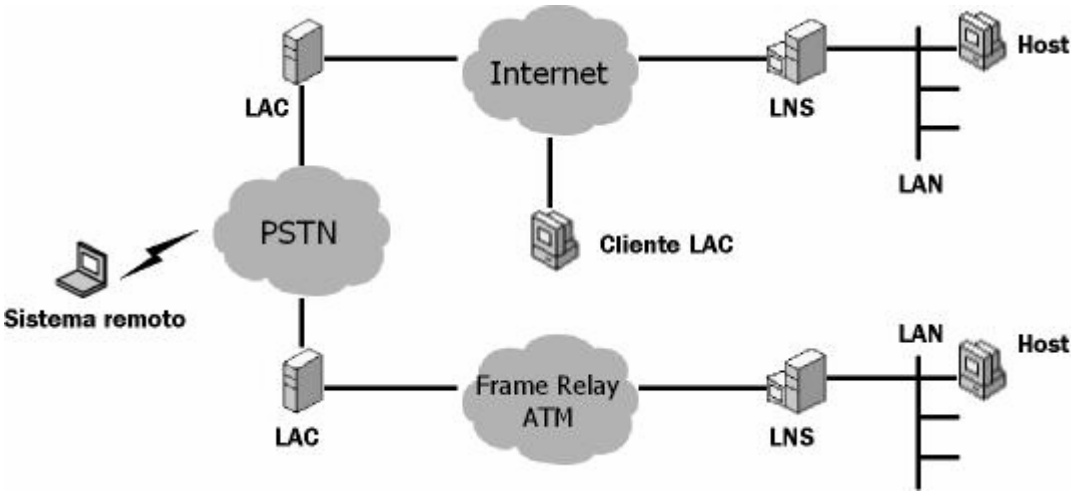

Figura 3.3 *Topología de L2TP* [40]

El sistema remoto inicia una conexión PPP a través de la nube PSTN hacia el LAC. Entonces, el LAC entunela la conexión PPP a través de Internet, *Frame Relay* o ATM hacia un LNS donde podrá tener acceso a una LAN privada. La autenticación, autorización y contabilidad son provistas por la LAN privada como si el usuario estuviera conectado a un NAS directamente.

Un cliente LAC (el cual es una computadora que ejecuta L2TP de forma nativa) participa en el *tunneling* hacia la red privada sin necesidad de usar un LAC separado. En este caso, el *host* que contiene el software L2TP cliente ya posee una conexión a Internet. Una conexión virtual PPP es creada entonces y el cliente LAC crea un túnel con el LNS o servidor L2TP. La autenticación, autorización y contabilidad son provistas por la LAN privada.

3.2.3.4 Mensajes de control y de datos

L2TP utiliza dos tipos de mensajes, mensajes de control y mensajes de datos. Los mensajes de control son utilizados para establecer, mantener y limpiar los túneles y las llamadas. Los mensajes de datos son utilizados para encapsular las tramas PPP que son transportadas a través del túnel. Los mensajes de control utilizan un canal de control confiable dentro de L2TP para garantizar el envío de la

información. Los mensajes de datos, por el contrario, no son retransmitidos cuando ocurren pérdidas en los paquetes.

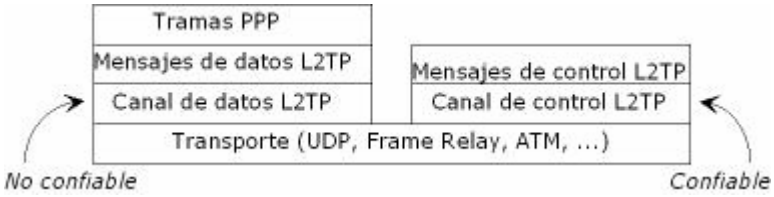

Figura 3.4 *Estructura de mensajes L2TP*

En la figura 3.4 se puede observar la relación entre las tramas PPP y los mensajes de control sobre el control L2TP y los canales de datos. Las tramas PPP son transportadas sobre un canal de datos no confiable encapsulado primeramente por una cabecera L2TP y después por un medio de transporte como puede ser UDP, ATM o *Frame Relay*.

Los mensajes de control son enviados sobre un canal de control L2TP confiable el cual transmite los paquetes en el mismo medio de transporte que utilizan los mensajes de datos. Tanto los mensajes de datos como los de control comparten el mismo formato de la cabecera.

L2TP utiliza varios mensajes de control, los cuales se muestran en la tabla 3.3.

Código	Nombre	Descripción
0	(Reservado)	
1	Start-Control-Connection-Request (SCCRQ)	Inicia el establecimiento de la sesión L2TP y el proceso de autenticación del túnel
2	Start-Control-Connection-Reply (SCCRP)	Es la respuesta al mensaje 1. Indica el éxito o el fracaso del establecimiento de la sesión así como la respuesta a la autenticación
3	Start-Control-Connection-Connected (SCCCN)	Es la respuesta al mensaje 2
4	Stop-Control-Connection-Notification (StopCCN)	Notifica el fin del túnel
5	(Reservado)	
6	Hello	Enviado periódicamente tanto por el cliente como por el servidor para mantener activa la conexión
7	Outgoing-Call-Request (OCRQ)	Es una petición enviada por el cliente para crear un túnel
8	Outgoing-Call-Reply (OCRP)	Es la respuesta al mensaje 7, la cual contiene un identificador único para ese túnel
9	Outgoing-Call-Connected (OCCN)	Es la respuesta al mensaje 8. Provee parámetros de llamada adicionales al servidor
10	Incoming-Call-Request (ICRQ)	Es una petición del cliente para recibir una llamada entrante por parte del servidor
11	Incoming-Call-Reply (ICRP)	Es la respuesta al mensaje 10. Esta indica si la llamada entrante debería ser contestada
12	Incoming-Call-Connected (ICCN)	Es la respuesta al mensaje 11. Provee parámetros de llamada adicionales al servidor
13	(Reservado)	
14	Call-Disconnect-Notify (CDN)	Notifica el fin de una sesión L2TP
15	WAN-Error-Notify (WEN)	Notifica que un error ha ocurrido en la conexión WAN, esto es, en la interfase que soporta PPP
16	Set-Link-Info (SLI)	Notifica cambios en las opciones PPP

Tabla 3.3 *Mensajes de control en L2TP* [40]

Formato de la cabecera L2TP. Los paquetes L2TP tanto de control como de datos comparten un mismo formato de la cabecera, el cual se muestra en la figura 3.5.

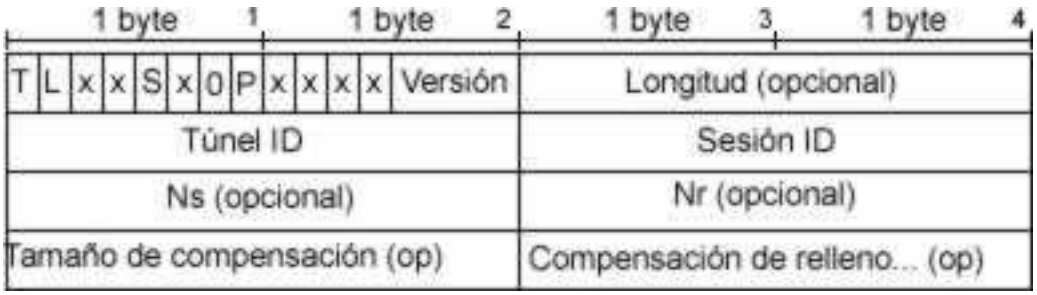

Figura 3.5 *Formato de la cabecera L2TP*

- El bit T (tipo) indica el tipo de mensaje. Se establece en 0 si es de datos o 1 si es de control.
- Cuando esta en 1 el campo Longitud (L) existe. En un mensaje de control L siempre esta en 1.
- Los bits x están reservados para extensiones futuras. Permanecen en 0.
- Si el bit S (secuencia) está en 1 los campos Ns y Nr existen. En un mensaje de control S siempre es 1.
- Si el bit O (compensación) está en 1, el campo Tamaño de compensación existe. En un mensaje de control O siempre es 0.
- Si el bit P (prioridad) está en 1, este mensaje tiene prioridad durante la transmisión.
- El campo Versión indica la versión de la cabecera del mensaje L2TP.
- El campo Longitud indica la longitud del mensaje en octetos
- El túnel ID indica el identificador para la conexión de control. Los túneles L2TP son identificados con este campo.
- La Sesión ID indica el identificador para una sesión dentro de un túnel.
- Ns indica el número de secuencia para el mensaje. Inicia en 0 y cada mensaje enviado incrementa el número de secuencia.
- Nr indica el número de secuencia esperado en el siguiente mensaje.
- La compensación de relleno especifica el número de octetos después de la cabecera antes del inicio de los datos. [40]

3.2.3.5 Túneles en L2TP

L2TP puede ser utilizado como protocolo de túnel en una red IP como Internet. Para el mantenimiento del túnel, L2TP sobre redes IP utiliza UDP y una serie de mensajes L2TP. Al igual que los datos entunelados, L2TP también utiliza UDP para enviar tramas PPP encapsuladas. La carga útil de las tramas PPP encapsuladas puede ser comprimida al igual que cifradas. L2TP usa el puerto UDP 1701. El ensamblado de un paquete L2TP al momento de su transmisión se muestra en la figura 3.6. [8]

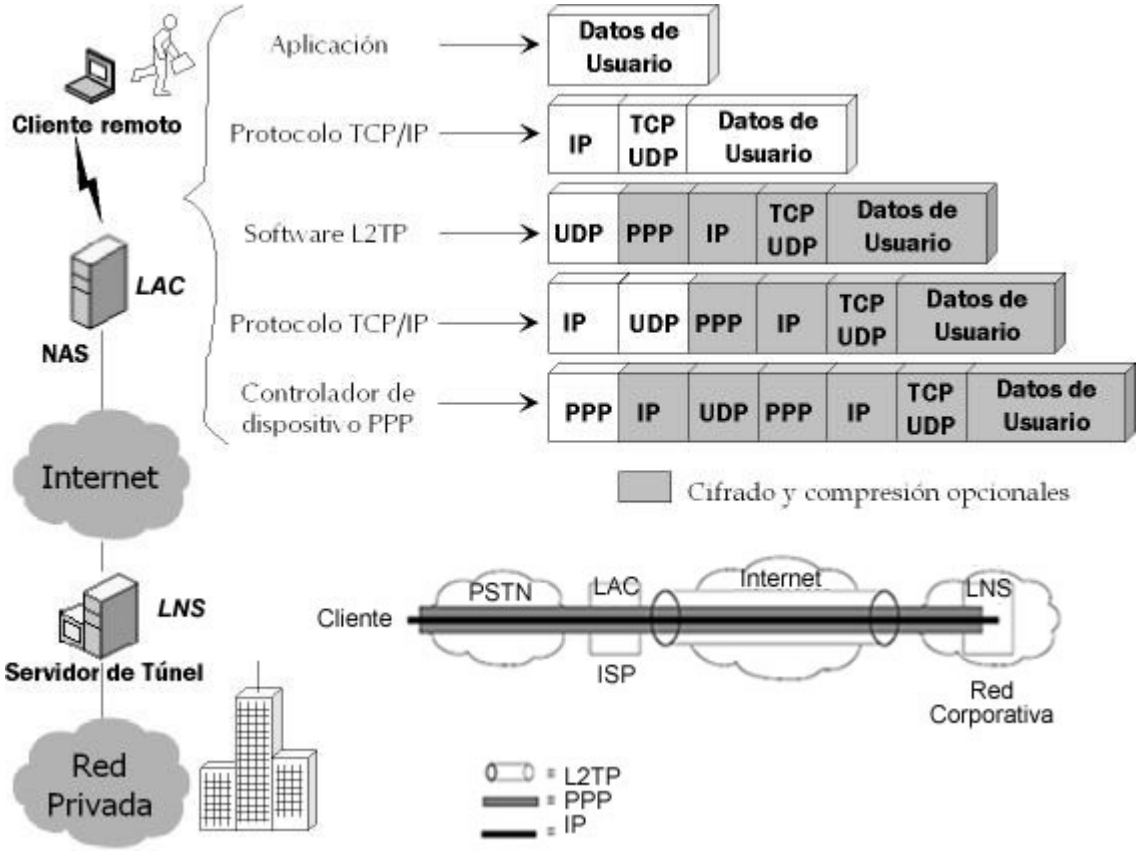

Figura 3.6 *Construcción de un paquete L2TP*

3.2.4 Funcionamiento de L2TP

El túnel y su correspondiente conexión de control deben ser establecidas antes de que se inicien las llamadas entrantes o salientes. Una sesión L2TP debe ser establecida antes de que L2TP comience a entunelar tramas PPP. Sesiones múltiples pueden existir a través de un único túnel y múltiples túneles pueden existir entre el mismo LAC y LNS.

La operación del protocolo L2TP se lleva a cabo de la siguiente manera y se muestra en la figura 3.7.

1. Se establece la conexión de control inicial entre el LAC y el LNS intercambiando los mensajes SCCRQ, SCCRP y SCCCN.
2. Se lleva a cabo la autenticación del túnel utilizando CHAP para ello.
3. Después de que se establece la conexión de control, se crean sesiones individuales. Cada sesión corresponde a un único flujo de tramas PPP entre el LAC y el LNS. Se intercambian los mensajes ICRQ, ICRP, ICCN para llamadas entrantes y OCRQ, OCRP Y OCCN para llamadas salientes.
4. Una vez que se establece el túnel, las tramas PPP del sistema remoto son recibidas por el LAC, encapsuladas en L2TP y enviadas por el túnel apropiado. El LNS recibe el paquete y desencapsula la trama PPP.
5. Se utilizan números de secuencia con el fin de identificar los mensajes para mantener un transporte confiable de éstos.
6. Se emplea el mensaje Hello para mantener activa la conexión.
7. Para finalizar la sesión, o el LAC o el LNS envían un mensaje CDN.
8. Para finalizar la conexión de control, o el LAC o el LNS envían un mensaje StopCCN.

Se usa un mensaje ZLB ACK para indicar que ya no hay más mensajes que transmitir entre el par LAC-LNS.

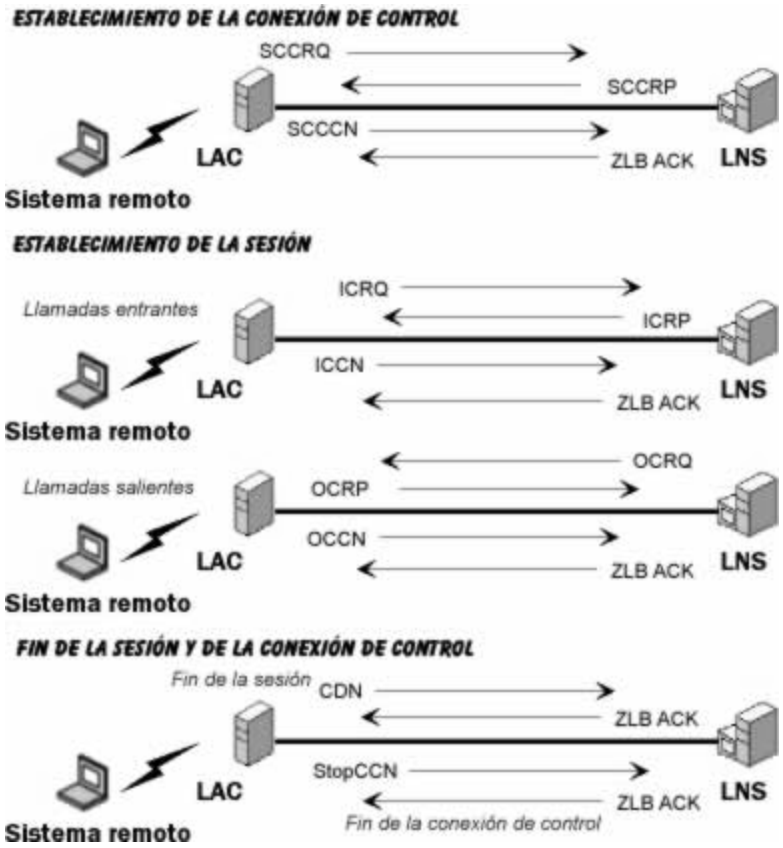

Figura 3.7 *Funcionamiento de L2TP*

Para establecer una conexión entre un usuario remoto, un dispositivo LAC ubicado en el punto de presencia (POP) del ISP, y el LNS en la LAN destino usando un túnel L2TP se siguen los siguientes pasos descritos en la figura 3.8 y explicados posteriormente.

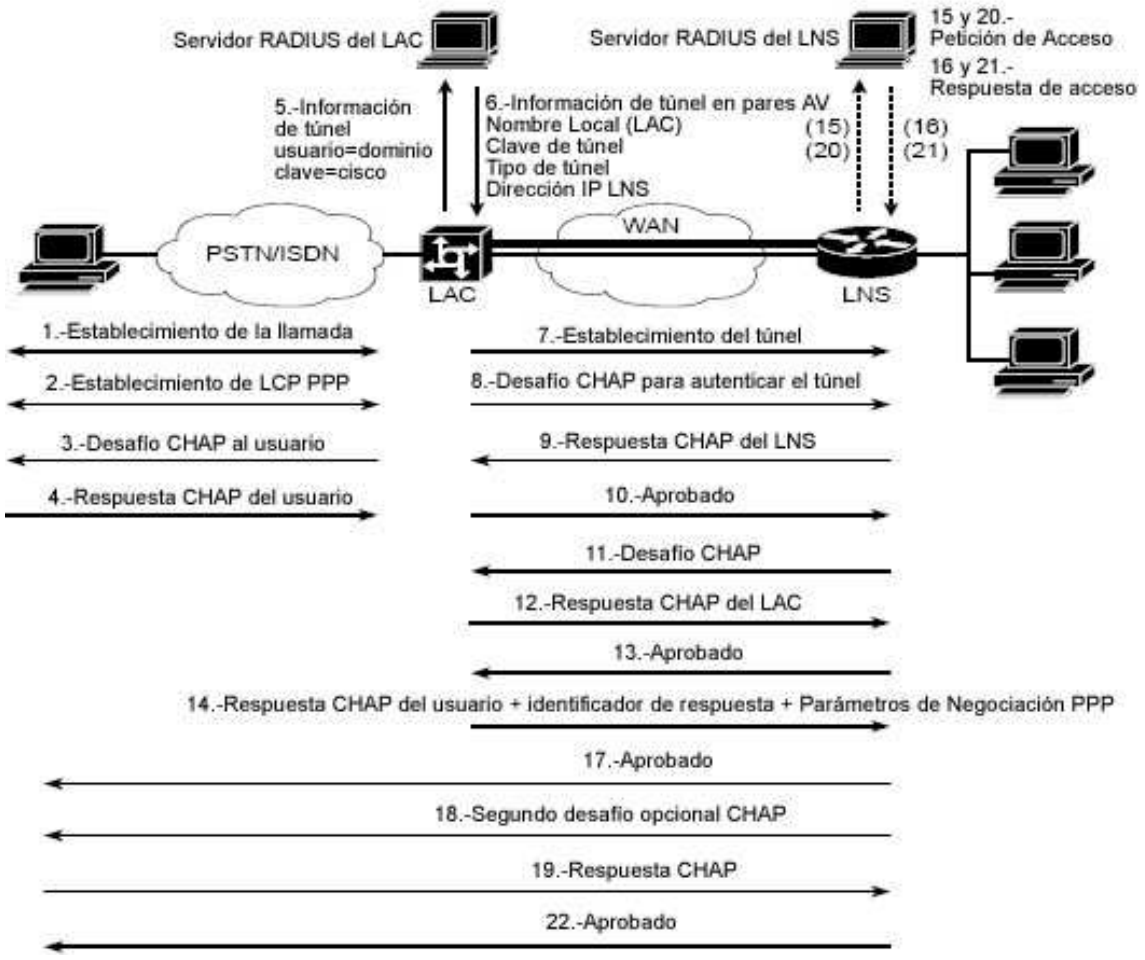

Figura 3.8 *Establecimiento de una conexión L2TP*

1. El usuario remoto inicia una conexión PPP con el ISP, utilizando la red telefónica analógica o ISDN.
2. El LAC de la red del ISP acepta la conexión en el POP y se establece el vínculo PPP.
3. Después de que el usuario final y el LNS negocian LCP, el LAC autentica parcialmente al usuario final con PAP o CHAP. El nombre de usuario o nombre de dominio es utilizado para determinar si el usuario es cliente de la VPN.
4. Los extremos del túnel (LAC y LNS), se autentican mutuamente antes de que comience cualquier sesión dentro del túnel.
5. Una vez que el túnel existe, se crea una sesión L2TP para el usuario final.

6. El LAC propagará las opciones LCP negociadas y la información CHAP/PAP al LNS y establecerá la conexión.

3.2.5 Seguridad en L2TP

3.2.5.1 Seguridad en los extremos del túnel

Los extremos del túnel pueden opcionalmente ejecutar un procedimiento de autenticación durante el establecimiento del túnel. Esta autenticación tiene los mismos atributos de seguridad como CHAP y tiene protección razonable contra los ataques de repetición durante el proceso de establecimiento del túnel. Sin embargo, este mecanismo no está designado para proveer autenticación más allá del establecimiento del túnel. Para que exista la autenticación, tanto el LAC como el LNS comparten una misma clave.

3.2.5.2 Seguridad a nivel paquete

Para asegurar L2TP se requiere que el transporte proporcione servicios de encriptación, seguridad y autenticación para todo el tráfico L2TP. Este transporte seguro opera sobre el paquete L2TP completo y funciona independientemente de PPP y del protocolo que este siendo transportando por PPP. L2TP sólo se preocupa de la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los extremos del túnel (LAC y LNS).

3.2.5.3 L2TP/IPSec

Cuando L2TP opera sobre redes IP, el mejor método de proporcionar seguridad es utilizando IPSec en combinación con L2TP. IPSec provee seguridad a nivel paquete utilizando ya sea ESP, AH o ambos. Toda los datos L2TP de un túnel en particular aparecen como paquetes de datos UDP/IP para el sistema IPSec. L2TP

se utiliza para enviar los datos por un túnel a través de una red compartida o pública como Internet, y ESP de IPSec para cifrar los datos.

Además de garantizar seguridad en el transporte de paquetes IP, IPSec define un modo de operación que permite entunelar paquetes IP. La autenticación y cifrado a nivel paquete proporcionados por IPSec modo túnel y el proporcionado por L2TP/IPSec otorgan un nivel equivalente de seguridad tal como lo requiere una VPN.

IPSec también define características de control de acceso que son requeridas para una implementación de seguridad completa. Estas características permiten el filtrado de paquetes basado en las características de la capa de red y de transporte tales como dirección IP, puertos, etc. En el modelo de *tunneling* L2TP, un filtrado análogo es ejecutado lógicamente a nivel PPP o en la capa de red sobre L2TP. [40]

Crear VPN de acceso remoto con L2TP/IPSec. Un requisito habitual es proteger las comunicaciones entre los clientes de acceso remoto y la red empresarial a través de Internet. Puede ser el caso de un consultor de ventas que pasa la mayor parte del tiempo de viaje o un empleado que trabaja desde casa.

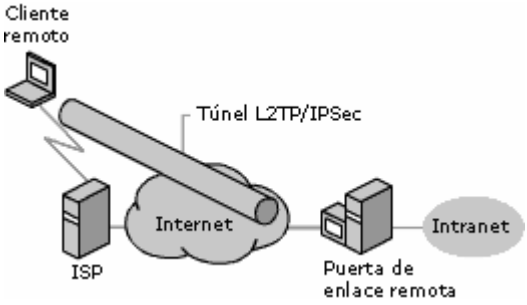

Figura 3.9 *VPN de acceso remoto con L2TP/IPSec*

En la figura 3.9, la puerta de enlace remota es un servidor que proporciona alta seguridad para la intranet de la empresa. El cliente remoto representa un usuario itinerante que precisa obtener acceso frecuente a los recursos y la información de la red. En el ejemplo se utiliza un ISP para ilustrar la ruta de comunicación cuando el cliente utiliza un ISP para el acceso a Internet. L2TP se combina con IPSec para

proporcionar un modo sencillo y eficaz de construir el túnel y proteger la información a través de Internet.

Crear VPN sitio a sitio con L2TP/IPSec. Una gran empresa a menudo dispondrá de varios sitios que precisan comunicarse, por ejemplo una oficina corporativa en Nueva York y una oficina de ventas en Washington. En este caso, L2TP se combina con IPSec para proporcionar la conexión VPN y proteger la información entre los distintos sitios.

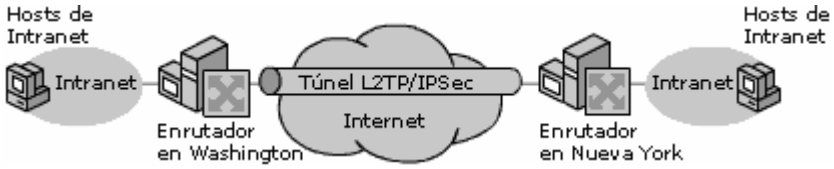

Figura 3.10 *VPN de sitio a sitio con L2TP/IPSec*

En la figura 3.10, los *routers* VPN se encargan de la seguridad exterior. Es posible que los *routers* utilicen una línea alquilada, acceso telefónico u otro tipo de conexión a Internet. La SA de IPSec y el túnel L2TP se establecen entre los *routers*, y permiten la comunicación segura a través de Internet. [48]

3.3 Seguridad IP (IPSec)

3.3.1 Definición de IPSec

La Seguridad del Protocolo de Internet (IPSec, *Internet Protocol Security*) es un marco de estándares abiertos para lograr comunicaciones privadas seguras a través de redes IP mediante el uso de servicios de seguridad criptográfica. IPSec es la tendencia a largo plazo para las redes seguras. Proporciona una sólida protección contra ataques a redes privadas e Internet mediante la seguridad de extremo a extremo. Los únicos equipos que deben conocer que existe protección con IPSec son el remitente y el receptor de la comunicación. IPSec tiene dos objetivos:

- Proteger el contenido de los paquetes IP.
- Defender contra los ataques de red mediante el filtrado de paquetes y la exigencia de comunicaciones de confianza.

Ambos objetivos se alcanzan gracias al uso de servicios de protección criptográfica, protocolos de seguridad y administración dinámica de claves. Estos fundamentos proporcionan al mismo tiempo la capacidad y la flexibilidad para proteger las comunicaciones entre equipos de redes privadas, dominios, sitios, sitios remotos, extranets y clientes de acceso telefónico. Incluso pueden utilizarse para bloquear la recepción o la transmisión de determinados tipos de tráfico.

IPSec se basa en un modelo de seguridad completo, y establece la confianza y la seguridad desde una dirección IP de origen hasta una dirección IP de destino. La dirección IP en sí no se considera necesariamente una identidad, sino que el sistema que hay tras la dirección IP tiene una identidad que se valida a través de un proceso de autenticación. Los únicos equipos que deben conocer que el tráfico está protegido son los equipos remitente y receptor.

Cada equipo trata la seguridad en su extremo respectivo y supone que el medio a través del cual tiene lugar la comunicación no es seguro. Los equipos que se limitan a enrutar datos desde el origen hasta el destino no necesitan ser compatibles con IPSec, salvo en el caso de que se filtren paquetes de tipo servidor de seguridad o se traduzcan direcciones de red entre los dos equipos. Este modelo permite implementar correctamente IPSec en los siguientes casos:

- Red de área local (LAN): cliente-servidor y entre homólogos
- Red de área extensa (WAN): entre *routers* y entre puertas de enlace
- Acceso remoto: clientes de acceso telefónico y acceso a Internet desde redes privadas

IPSec se basa en los estándares desarrollados por el grupo de trabajo de IPSec del IETF. IPSec se encuentra documentado en diversos RFC de los cuales el principal es el RFC 2401. [48]

IPSec utiliza dos protocolos que proporcionan seguridad en el tráfico. Estos protocolos son:

- Cabecera de autenticación (AH, *Authentication Header*)
- Carga de Seguridad de Encapsulamiento (ESP, *Encapsulating Security Protocol*)

AH proporciona integridad en la conexión, autenticación de los datos de origen y un servicio opcional contra paquetes repetidos. ESP provee confidencialidad de los datos utilizando técnicas de encriptación. Opcionalmente puede proporcionar también autenticación, integridad y protección contra paquetes repetidos. Ambos protocolos son vehículos para el control de acceso, basado en la distribución de claves criptográficas y la administración de los flujos de tráfico relativos a estos protocolos de seguridad.

Cada protocolo soporta dos modos de uso: modo transporte y modo túnel. En el modo transporte los AH y ESP proveen protección a los protocolos de capas

superiores. En el modo túnel AH y ESP son aplicados para entunelar paquetes IP. [38]

También se utiliza un conjunto protocolos necesarios para la gestión de llaves criptográficas. La Asociación de Seguridad (SA), utilizada para llevar a cabo la autenticación, representa una conexión unidireccional para la cual se definen todos los servicios de seguridad que deben ser aplicados al tráfico de red. Las SA pueden ser creadas tanto automáticamente como manualmente, empleando para ello el protocolo ISAKMP/Oakley. [57]

3.3.2 Protocolos de IPSec

3.3.2.1 Cabecera de Autenticación (AH)

La cabecera de autenticación (AH, *Authentication Header*) puede detectar paquetes alterados y puede autenticar la identidad del emisor basándose en el usuario final o en la dirección IP fuente. Las partes que se comunican en IPSec usando AH pueden utilizar diferentes algoritmos ya sea MD5 o SHA-1 con el fin de crear una firma *hash* utilizando un componente secreto de la SA, la carga útil del paquete y varias partes de la cabecera del paquete.

Contenido del paquete AH. La cabecera AH contiene esencialmente cinco campos los cuales se muestran a continuación en la figura 3.11.

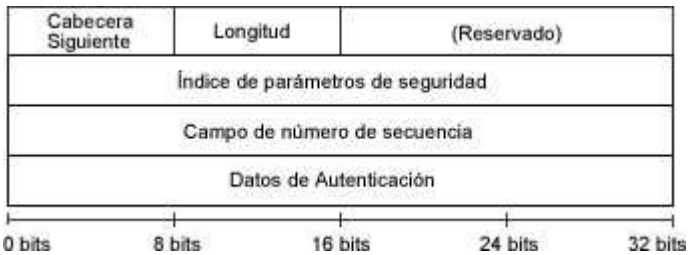

Figura 3.11 *Contenido del paquete AH*

- La cabecera siguiente describe la cabecera de la capa 4 (TCP, UDP, ICMP) para un datagrama IPv4 (8 bits)
- La longitud de la firma *hash* (8 bits)
- El Índice de Parámetro de Seguridad (SPI) (32 bits)
- El campo de número de secuencia antirepetición, el cual evita los ataques de repetición (32 bits)
- La firma *hash* propiamente dicha (32 bits) [9]

AH en modo transporte. En el modo transporte (Ver figura 3.12), los servicios AH protegen la cabecera IP externa junto con la carga útil de datos. Los servicios AH protegen todos los campos en la cabecera que no cambia durante el transporte. AH se coloca después de la cabecera IP y antes de la cabecera ESP si está presente, y antes de los protocolos de capas superiores.

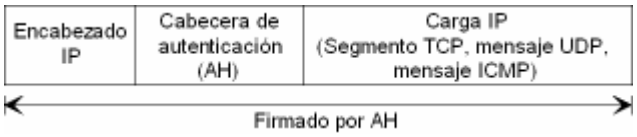

Figura 3.12 *AH en modo transporte*

AH en modo túnel. En el modo túnel (Ver figura 3.13), la cabecera original entera es autenticada, se construye una cabecera IP nueva y la nueva cabecera IP es protegida de la misma manera que en el modo transporte. [45]

Figura 3.13 *AH en modo túnel*

3.3.2.2 Carga de Seguridad de Encapsulación (ESP)

La Carga de Seguridad de Encapsulamiento (ESP, *Encapsulating Security Protocol*) puede proporcionar servicios de confidencialidad, autenticidad e integridad. El modo túnel ESP también ofrece confidencialidad en el flujo del

tráfico. Las primeras versiones de ESP se enfocaron principalmente en la confidencialidad; sin embargo, el estándar final también incluye una gran funcionalidad como la que proporciona AH. Los estándares ESP soportan principalmente dos métodos de cifrado DES y 3DES.

Contenido del paquete ESP. Al igual que AH, la cabecera ESP contiene lo siguiente, como se muestra en la figura 3.14.

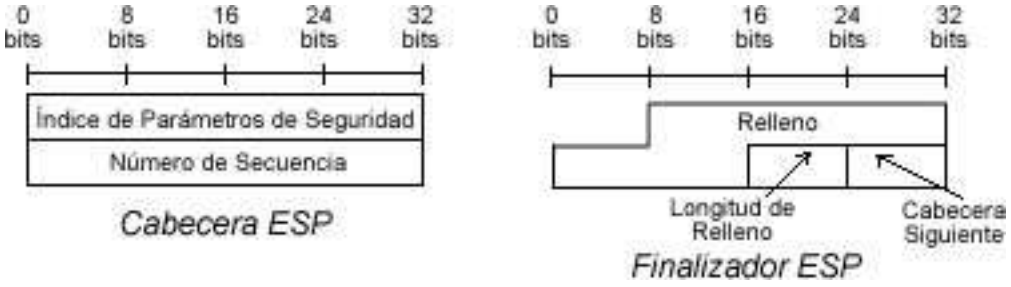

Figura 3.14 *Contenido del paquete ESP*

- Índice de Parámetro de Seguridad (SPI) (32 bits)
- El campo de número de secuencia antirepetición (32 bits)
- Longitud de relleno (8 bits)
- Cabecera siguiente (8 bits)
- Relleno (0-255 bits)

A diferencia de AH, ESP también incluye el campo cabecera siguiente como una parte del finalizador del paquete. La carga del paquete debe incluir relleno para que pueda operar el algoritmo de cifrado. El finalizador también debe contener un monto variable de datos de autenticación. [9]

ESP en modo transporte. En el modo transporte (Ver figura 3.15), la carga IP es cifrada y las cabeceras originales se dejan intactas. La cabecera ESP es insertada después de la cabecera IP y antes de la cabecera del protocolo de capa superior. Los protocolos de capa superior son cifrados y autenticados utilizando la cabecera ESP. ESP no autentica la cabecera IP. También hay que notar que la información de capas superiores no está disponible debido a que pertenece a la carga cifrada.

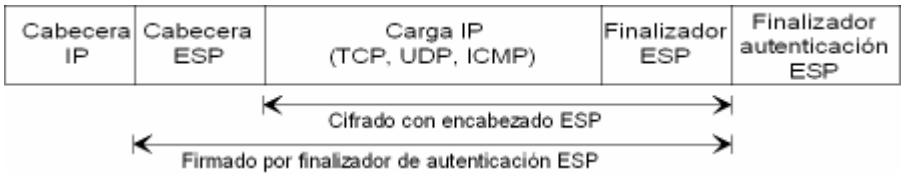

Figura 3.15 *ESP en modo transporte*

ESP en modo túnel. En el modo túnel (Ver figura 3.16), la cabecera IP original se encuentra bien protegida debido a que el datagrama original IP completo se encuentra cifrado. Con el mecanismo de autenticación ESP, el datagrama IP original y la cabecera ESP son incluidas. Se construye una nueva cabecera IP, sin embargo, ésta no es incluida en la autenticación. [45]

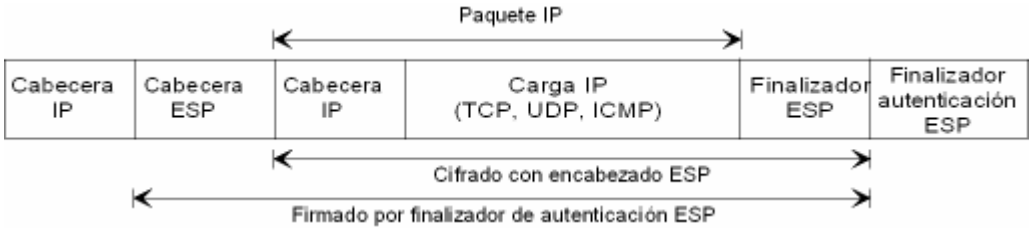

Figura 3.16 *ESP en modo túnel*

3.3.3 Asociaciones de Seguridad (SA)

El concepto de Asociación de Seguridad (SA, *Security Association*) es fundamental en la arquitectura IPSec. Una SA es una conexión que permite servicios de seguridad para el tráfico transportado por ésta, dicho en otra forma, una SA es un acuerdo entre ambas partes acerca de cómo cifrar y descifrar los datos que se van a transmitir. Los servicios de seguridad son proporcionados a una SA utilizando AH o ESP pero no ambos. Si ambos protocolos son aplicados a influjo de datos determinado, entonces dos o más SA son creadas para dar protección a dicho flujo. Para asegurar una típica comunicación bidireccional entre dos *hosts*, o entre dos *gateways* de seguridad, dos SA (una en cada dirección) son requeridas.

Una SA es identificada de forma única por medio de valores diferentes tales como un Índice de Parámetro de Seguridad (SPI, *Security Parameter Index*), una

dirección IP destino y un identificador del protocolo de seguridad (AH o ESP). Los estándares definen un riguroso mecanismo para asegurar que cada SA es única. Los dispositivos IPSec almacenan estas SA en una Base de Datos SA (SAD, *SA Database*). Un ejemplo de estos valores se muestra en la figura 3.17. [38]

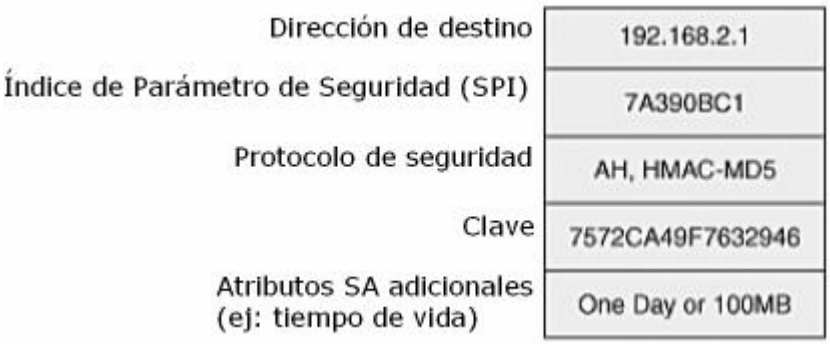

Figura 3.17 *Asociación de Seguridad (SA)* [45]

3.3.4 Administración de claves en IPSec

3.3.4.1 Los protocolos ISAKMP/Oakley e IKE

Puesto que IPSec es una arquitectura abierta, los protocolos de seguridad (AH y ESP) están diseñados para ser independientes con respecto a la administración de claves cifradas de forma automática. Sin embargo, las implementaciones de IPSec que cumplan con los estándares deben soportar tanto el uso de claves previamente compartidas como el mecanismo de administración de claves automatizado conocido como Intercambio de claves de Internet (IKE, *Internet Key Exchange*).

IKE es un diseño específico dentro de un sistema mayor conocido como Protocolo de Administración de Claves y Asociación de Seguridad de Internet (ISAKMP, *Internet Security Association and Key Management Protocol*). ISAKMP es un sistema de intercambio de claves y autenticación que es independiente de cualquier tecnología de claves específica. IKE trabaja con otro protocolo llamado Oakley, para el intercambio de claves seguro dentro del modelo ISAKMP. [9]

ISAKMP/Oakley proporciona un mecanismo que permite a servidores VPN separados compartir información de claves de encriptación y hace que IPSec sea práctico en el entorno actual. [16]

3.3.4.2 Protocolo Oakley

Oakley es un protocolo que utiliza un intercambio de claves *Diffie-Hellman* para establecer una clave compartida de forma segura entre las dos partes que se comunican. Oakley trabaja dentro del marco ISAKMP para establecer las SA de IPSec. El estándar de determinación de clave Oakley establece una SA de ISAKMP inicial, pero permite un mecanismo más ligero para permitir SA subsecuentes.

3.3.4.3 Intercambio de Claves de Internet (IKE)

El protocolo de Intercambio de claves de Internet (IKE) pertenece al conjunto ISAKMP/Oakley. Es un protocolo de administración de claves seguro diseñado para establecer las SA de IPSec y para permitir una rápida reasignación de claves para las SA existentes. IKE opera en dos fases, las cuales se describen a continuación. [9]

Fase 1 de IKE. El objetivo básico de la fase 1 de IKE es autenticar ambas partes de IPSec. Durante esta fase se llevan a cabo las siguientes funciones:

- Identificar y proteger las identidades de ambas partes de IPSec
- Negociar una póliza SA de ISAKMP entre ambas partes para proteger el intercambio de IKE
- Ejecutar un intercambio *Diffie-Hellman* autenticado con el resultado final de tener claves secretas compartidas.
- Establecer un túnel seguro para negociar los parámetros de la fase 2 de IKE

Fase 2 de IKE. El propósito de la fase 2 de IKE es negociar las SA de IPSec para establecer el túnel IPSec. La fase 2 de IKE lleva a cabo las siguientes funciones como también se ve en la figura 3.18.

- Negociar los parámetros SA de IPSec protegidos por una SA de ISAKMP existente.
- Establece SA de IPSec
- Periódicamente renegocia las SA de IPSec para garantizar la seguridad
- Ejecuta opcionalmente un intercambio *Diffie-Hellman* adicional

Figura 3.18 *Funcionamiento de IKE*

3.3.5 Funcionamiento de IPSec

IPSec es una tecnología que envuelve muchos componentes tecnológicos y métodos de encriptación. Así pues, la operación de IPSec se puede descomponer en cinco pasos principales que se explican a continuación y que aparecen en la figura 3.19.

1. En este primer paso se determina el tráfico inicial IPSec. Determinar este tráfico inicial es parte de la formulación de una póliza de seguridad para usar en una VPN. Esta póliza es implementada en ambas partes que se comunican.
2. El segundo paso consiste en ejecutar la Fase 1 de IKE, donde se autentican ambos extremos.

3. El tercer paso consiste en ejecutar la Fase 2 de IKE, donde se establecen las SA para crear el túnel.
4. El cuarto paso es donde se lleva acabo la transferencia de datos por el túnel IPSec. Los paquetes son cifrados y descifrados de acuerdo con el método especificado en la SA de Ipsec.
5. El último paso consiste en la terminación del túnel IPSec, donde las SA expiran y se deben negociar nuevas SA para continuar transmitiendo datos. Entonces se regresa a la Fase 2 o a la Fase 1. Esto resulta en nuevas SA y nuevas claves. [45]

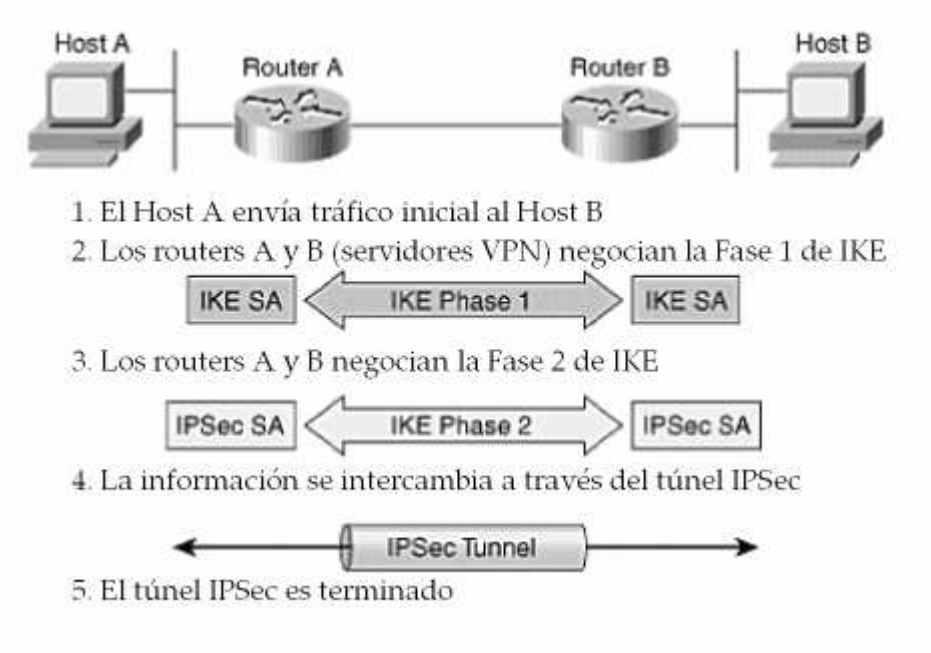

Figura 3.19 *Funcionamiento de IPSec*

4

Configuración de una VPN

Este capítulo está dedicado a explicar de forma general los pasos a seguir para poder implementar una VPN. Existen varias formas de hacerlo, ya que se puede elegir entre un router, un firewall, un sistema operativo de red o contratar un proveedor de servicios. En este caso, se presentará la forma de configurar una VPN en el sistema operativo Windows Server 2003 y en el firewall PIX de Cisco.

4.1 Configuración de una VPN en un sistema operativo

4.1.1 Configuración de una VPN en Windows Server 2003[7]

Windows Server 2003 es un sistema operativo de red de Microsoft Corporation específicamente diseñado para funcionar como servidor. El objetivo de Microsoft con este sistema operativo es crear un sistema tan bueno como UNIX. Aunque las familias de servidores Windows siempre se han comparado de manera favorable con UNIX en cuanto a facilidad de uso y administración, UNIX siempre es más confiable y ofrece mejor desempeño en hardware. [5]

Windows Server 2003 se encuentra en el mercado en cuatro ediciones diferentes, cada una con su precio y características específicos. Las cuatro ediciones son las siguientes:

- Standard Edition
- Enterprise Edition
- DataCenter Edition
- Web Edition

Windows Server 2003 ofrece la posibilidad de crear un servidor VPN. En Windows Server 2003 Web Edition y Windows Server 2003 Standard Edition se pueden crear hasta 1000 puertos PPTP y hasta 1000 puertos L2TP. Sin embargo, Windows Server 2003, Web Edition sólo puede aceptar una conexión VPN cada vez. Windows Server 2003 puede aceptar hasta 1000 conexiones VPN simultáneas. Si se conectan 1000 clientes VPN, se denegarán los intentos de conexión posteriores hasta que el número de conexiones sea inferior a 1000.

[7] La configuración de una VPN es única para cada caso. Aquí sólo se mencionan las normas generales a seguir

4.1.1.1 Configurar una VPN de acceso remoto

Se deberá tener en cuenta los siguientes aspectos de diseño antes de implementar conexiones VPN de acceso remoto:

- **Elegir entre conexiones L2TP/IPSec o basadas en PPTP.** PPTP acepta clientes VPN como Windows 95, 98, 2000, Me y XP mientras que L2TP sólo acepta clientes con Windows 2000 o XP.
- **Instalar certificados.** Para obtener mayor seguridad en conexiones L2TP/IPSec se prefiere instalar certificados. Los certificados deben instalarse tanto en el servidor como en el cliente VPN. PPTP no requiere de certificados a menos que se use EAP.
- **Configurar filtros de paquetes del servidor de seguridad.** Esto se hace con el fin de permitir el tráfico entre los clientes VPN de Internet y el servidor VPN.
- **Crear una directiva de acceso remoto para las conexiones VPN de acceso remoto.** Mediante las directivas de acceso remoto, se puede crear una directiva que requiera que las conexiones VPN de acceso remoto utilicen un método de autenticación y refuerzo de cifrado específicos.
- **Usar un servidor RADIUS.** Si se dispone de varios servidores VPN que ejecutan Windows Server 2003, se debe configurar las directivas de acceso remoto y el registro para cada servidor VPN. Si se desea aprovechar las directivas de acceso remoto y el registro centralizado, se puede configurar los servidores VPN como clientes de un RADIUS.
- **Usar *Connection Manager.*** En una gran implantación VPN de acceso remoto, es posible utilizar *Connection Manager* y el Kit de administración de *Connection Manager* para proporcionar un marcador personalizado con conexiones VPN configuradas previamente a todos los clientes de acceso remoto de una organización.
- **Impedir el enrutamiento de tráfico a través de los clientes de acceso remoto.** Esto se hace con el fin de impedir que el servidor VPN envíe

tráfico a través de la conexión VPN para equipos que no sean clientes VPN de acceso remoto autenticados.

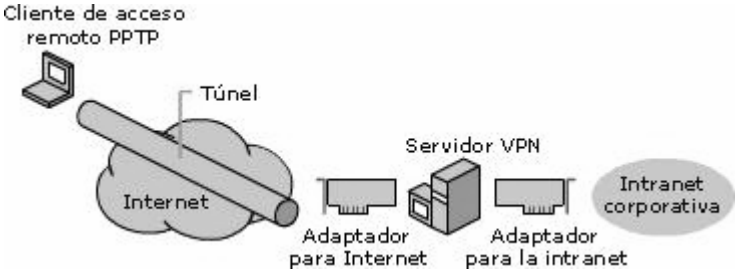

Figura 4.1 *VPN de acceso remoto con Windows Server 2003*

La figura 4.1 muestra una VPN de acceso remoto con Windows Server 2003. Se puede utilizar el acceso remoto con Windows Server 2003 para proporcionar acceso a una intranet corporativa a los clientes de acceso remoto que establecen conexiones PPTP o L2TP/IPSec a través de Internet. Si se desea que el servidor de acceso remoto admita varias conexiones PPTP o L2TP/IPSec, hay que realizar los pasos siguientes:

1. **Configurar la conexión a Internet.** en donde la conexión a Internet desde un equipo que ejecuta un sistema operativo Windows Server 2003 es una conexión dedicada, es decir, un adaptador para WAN instalado en el equipo. Normalmente, el adaptador para WAN es un adaptador T1, T1 fraccional o *Frame Relay*. Se debe contratar los servicios de una compañía telefónica local para que instale el cableado físico apropiado en sus instalaciones. Se tiene que comprobar que el adaptador para WAN es compatible con los productos de la familia Windows Server 2003. Se debe configurar en el adaptador para WAN la dirección IP y la máscara de subred asignadas por InterNIC o por un ISP, además de la puerta de enlace predeterminada del *router* del ISP. Para permitir que los clientes VPN se conecten al servidor VPN mediante el nombre en lugar de la dirección IP, se puede solicitar al ISP el registro del servidor VPN en el sistema DNS.
2. **Configurar la conexión a la intranet.** La conexión a la intranet desde un equipo que ejecuta un sistema operativo Windows Server 2003 se establece a través de un adaptador para LAN instalado en el equipo. Se

tiene que comprobar que el adaptador para LAN es compatible con los productos de la familia Windows Server 2003. Se deben configurar en el adaptador para LAN la dirección IP y la máscara de subred asignadas por el administrador de la red, así como los servidores de nombres DNS y WINS correspondientes de la intranet corporativa.

3. **Configurar el servidor de acceso remoto como *router*[8] de una intranet corporativa.** Para que el servidor de acceso remoto reenvíe el tráfico correctamente en la intranet corporativa, debe configurarse como un *router* con rutas estáticas o protocolos de enrutamiento, de manera que se pueda tener acceso a todas las ubicaciones de la intranet desde el servidor de acceso remoto.
4. **Configurar el servidor VPN.** Para configurar el servidor VPN, se ejecuta el Asistente para la instalación del servidor de enrutamiento y acceso remoto. El asistente permite configurar un servidor de seguridad básico en la interfaz pública, el método que utiliza el servidor VPN para asignar direcciones a los clientes de acceso remoto (mediante direcciones que el servidor VPN obtiene de un servidor DHCP o mediante direcciones de un intervalo de direcciones especificado que se configure en el servidor VPN), así como el reenvío de mensajes de autorización y autenticación a un servidor RADIUS, es decir, la configuración del servidor VPN como cliente RADIUS.
5. **Instalar certificados.** Para crear conexiones VPN de acceso remoto L2TP/IPSec utilizando la autenticación mediante certificados de equipo para IPSec, se debe instalar certificados de equipo en el cliente VPN y en el servidor VPN.
6. **Configurar los filtros de paquetes del servidor de seguridad.** Si se utiliza un servidor de seguridad, se debe configurar filtros de paquetes PPTP o L2TP/IPSec en el servidor de seguridad para permitir el tráfico

[8] Microsoft denomina *router* o enrutador a la computadora que ejecuta Windows Server 2003 y que proporciona servicios VPN

PPTP o L2TP/IPSec entre los clientes VPN basados en Internet y el servidor VPN.

7. **Configurar las directivas de acceso remoto.** En el caso del modelo administrativo de acceso por usuario, deberá establecer el permiso de acceso remoto en *Permitir acceso* en las cuentas de usuario correspondientes a aquellos usuarios que vayan a establecer conexiones VPN. En el caso del modelo de acceso por directiva, se realizan los cambios adecuados en el permiso de acceso remoto de las cuentas de usuario.

4.1.1.2 Configurar una VPN de sitio a sitio

Se deberá tener en cuenta los siguientes aspectos de diseño antes de implementar conexiones VPN de sitio a sitio:

- **Conexiones L2TP/IPSec o basadas en PPTP.** Se debe decidir si utilizar L2TP/IPSec o PPTP.
- **Instalar certificados.** Para obtener mayor seguridad en conexiones L2TP/IPSec de sitio a sitio se deben instalar certificados en ambos *routers*.
- **Conexiones a petición o persistentes.** Las conexiones de marcado a petición que son a petición requieren que el *router* de respuesta esté conectado permanentemente con Internet. El *router* de llamada establece una conexión con Internet mediante un vínculo de acceso telefónico como una línea de teléfono analógica o RDSI. Se debe configurar una única interfaz de marcado a petición en el *router* de respuesta. Se debe configurar dos interfaces de marcado a petición en el *router* de llamada: una para la conexión con un ISP local y otra para la conexión VPN de *router* a *router*. Las conexiones VPN de *router* a *router* de marcado a petición también requieren una ruta de *host* adicional en la tabla de enrutamiento IP del *router* de llamada. Las conexiones persistentes requieren que ambos *routers* estén conectados con Internet mediante conexiones WAN permanentes. Sólo necesita configurar una única interfaz de marcado a petición en cada *router*. Las conexiones

permanentes se pueden iniciarse y mantener en un estado de conexión de 24 horas al día.

- **Restringir el inicio de conexiones a petición.** Para impedir que el *router* de llamada establezca conexiones innecesarias, se puede restringir las conexiones VPN de *router* a *router* a petición del *router* de llamada de dos maneras. La primera es usar filtros de marcado a petición para configurar tanto los tipos de tráfico IP para que no se establezca una conexión de marcado a petición como los tipos de tráfico IP para que sí se establezca. La segunda es utilizar las horas de acceso telefónico de salida para configurar las horas a las que se permite o no que un *router* de llamada establezca una conexión VPN de *router* a *router*.
- **Conexiones iniciadas en uno o dos sentidos.** Se debe decidir si uno o ambos *routers* iniciarán las conexiones VPN de *router* a *router*. Si las conexiones se inician en un único sentido, un *router* es el servidor VPN y el otro es el cliente VPN. El servidor VPN acepta la conexión y el cliente VPN la inicia. Se recomiendan las conexiones que se inician en un único sentido para las topologías de concentrador de conexión permanente, donde el *router* de la sucursal es el único que inicia la conexión. Con conexiones que se inician en ambos sentidos, cualquier *router* puede ser el servidor VPN o el cliente VPN, según quién esté iniciando la conexión. Los dos *routers* se deben configurar para iniciar y aceptar una conexión VPN. Puede utilizar conexiones que se inicien en ambos sentidos cuando la conexión VPN de *router* a *router* no se encuentre activa 24 horas al día y el tráfico de cualquiera de los *routers* se utilice para crear la conexión a petición.
- **Número de puertos PPTP o L2TP necesarios.** Se pueden crear hasta 1000 puertos PPTP y hasta 1000 puertos L2TP.
- **Configurar filtros de paquetes del servidor de seguridad.** Si se tiene un servidor de seguridad, se debe configurar en él filtros de paquetes para permitir el tráfico entre el *router* VPN y los *routers* de Internet.
- **Enrutamiento.** Los dos *routers* de una conexión VPN de sitio a sitio deben tener las rutas adecuadas en sus tablas de enrutamiento para reenviar tráfico

a través de la conexión. Las rutas pueden ser estáticas o dinámicas. Se puede agregar rutas estáticas a la tabla de enrutamiento manualmente o mediante una actualización autoestática. Se pueden agregar rutas dinámicas a la tabla de enrutamiento; para ello, es necesario agregar la interfaz de marcado a petición de la conexión VPN a un protocolo de enrutamiento. Sin embargo, únicamente se recomienda habilitar un protocolo de enrutamiento en la interfaz de marcado a petición de la conexión VPN cuando la interfaz de marcado a petición esté conectada permanentemente.

- **Salto único en la conexión VPN.** Con el fin de diseñar una infraestructura enrutada, se puede considerar la conexión VPN de *router* a *router* como un único salto, independientemente de cuántos *routers* se atraviesen cuando se envían datos encapsulados a través de Internet.
- **Crear una directiva de acceso remoto para las conexiones VPN de *router* a *router*.** Mediante las directivas de acceso remoto, puede crear una directiva que requiera que las conexiones VPN de *router* a *router* utilicen un método de autenticación y niveles de cifrado específicos.

La figura 4.2 muestra una VPN de sitio a sitio que utiliza Windows Server 2003 como servidor VPN.

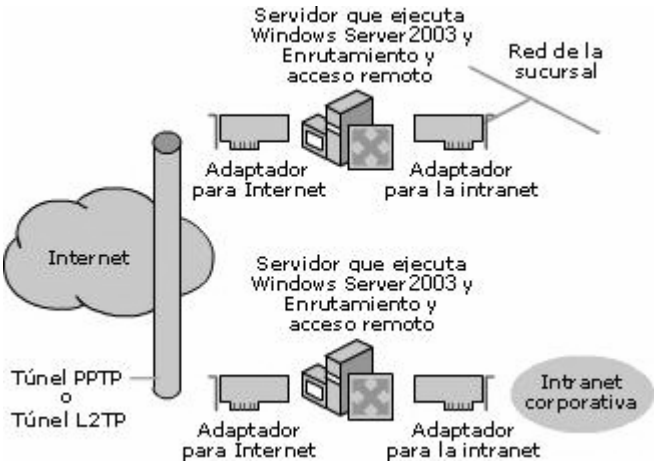

Figura 4.2 *VPN de sitio a sitio con Windows Server 2003*

Para crear una conexión VPN de *router* a *router* basada en PPTP o L2TP para enviar datos privados a través de Internet, se deben seguir los siguientes pasos:

1. Configurar el *router* que ejecuta un sistema operativo Windows Server 2003 en la oficina corporativa para que reciba conexiones PPTP o L2TP desde el *router* de una sucursal.
2. Configurar el *router* que ejecuta un sistema operativo Windows Server 2003 en la sucursal para que inicie una conexión PPTP o L2TP con el *router* de la oficina corporativa.
3. Iniciar la conexión PPTP o L2TP desde el *router* de la sucursal.

Si se desea que el *router* que ejecuta un sistema operativo Windows Server 2003 en la oficina corporativa admita varias conexiones PPTP o L2TP con sucursales, se deben realizar los pasos siguientes:

1. **Configurar la conexión a Internet.** Esta conexión se configura de la misma forma que en la VPN de acceso remoto.
2. **Configurar la conexión a la intranet.** Esta conexión se configura de la misma forma que en la VPN de acceso remoto. Además, puesto que el *router* de la oficina corporativa enrutará el tráfico entre la oficina corporativa y la sucursal, se debe configurar el mismo con rutas estáticas o con protocolos de enrutamiento, de manera que sea posible el acceso a todos los destinos de la red corporativa desde el *router* de la oficina corporativa.
3. **Instalar un certificado de equipo.** Aunque es posible utilizar certificados de equipo o una clave previamente compartida con el fin de proporcionar autenticación para las asociaciones de seguridad IPSec en una conexión L2TP/IPSec, el método recomendado son los certificados de equipo. Por ello, se debe instalar un certificado en el *router* de la oficina corporativa.
4. **Configurar el router de la oficina corporativa.** Se debe habilitar el *router* de la oficina corporativa; para ello, hay que instalar el Servicio de enrutamiento y acceso remoto.
5. **Configurar las interfaces de marcado a petición.** Para cada *router* de sucursal, se puede crear una interfaz de marcado a petición con el Asistente para interfaz de marcado a petición, donde se configura el nombre de la interfaz que representa la conexión a la sucursal, el tipo de

conexión (es una conexión VPN), el tipo de VPN (ya sea PPTP o L2TP), los protocolos y seguridad para agregar una cuenta de usuario para que un *router* remoto se conecte, las rutas estáticas para que se reenvíe el tráfico a la sucursal mediante la interfaz de marcado a petición apropiada y las credenciales de llamada saliente donde se asigna el dominio y la contraseña de la cuenta que se utilizará para autenticar el *router* de la sucursal.

6. **Configurar los filtros de paquetes del servidor de seguridad.** Si se utiliza un servidor de seguridad en la oficina corporativa, se deben configurar filtros de paquetes PPTP o L2TP/IPSec en el servidor de seguridad para permitir el tráfico PPTP o L2TP/IPSec entre los *routers* de las sucursales y el *router* de la oficina corporativa.
7. **Configurar las directivas de acceso remoto.** Al utilizar el Asistente para interfaz de marcado a petición, las propiedades de marcado de las cuentas de usuario que utilizan los *routers* de las sucursales ya están configuradas para permitir el acceso remoto. La configuración predeterminada admite todos los niveles de cifrado y permite que no haya cifrado.

Si se desea que el *router* que ejecuta un sistema operativo Windows Server 2003 en la sucursal inicie una conexión PPTP o L2TP con el *router* de la oficina corporativa, se deben realizar los pasos siguientes:

1. **Configurar la conexión a Internet.** Esta conexión se configura de la misma forma que en la VPN de acceso remoto.
2. **Configurar la conexión a la red de la sucursal.** Esta conexión se configura de la misma forma que en la conexión a la intranet de la VPN de acceso remoto.
3. **Instalar un certificado de equipo.** Puesto que el *router* de la sucursal utiliza certificados de equipo para autenticar la asociación de seguridad IPSec para la conexión L2TP/IPSec, se debe instalar un certificado de

equipo en el *router* de la sucursal para que se pueda establecer correctamente una conexión L2TP/IPSec.

4. **Configurar una interfaz de marcado a petición.** Para crear una interfaz de marcado a petición, se utiliza el *Asistente para interfaz de marcado a petición* donde se configura el nombre de la interfaz que representa a la oficina corporativa, el tipo de conexión, el tipo de VPN, la dirección IP o el nombre de *host* asignado a la interfaz con Internet del *router* de la oficina corporativa y el nombre de dominio y la contraseña de la cuenta de usuario correspondiente al *router* de la sucursal.
5. **Configurar las rutas estáticas.** Es necesario agregar rutas estáticas para que se reenvíe el tráfico a la oficina corporativa mediante la interfaz de marcado a petición apropiada. Para cada ruta de la oficina corporativa, hay que configurar la interfaz, el destino, la máscara de red y la métrica. Para la interfaz, se selecciona la interfaz de marcado a petición que corresponda a la oficina corporativa.
6. **Configurar los filtros de paquetes del servidor de seguridad.** Se configura de la misma manera que en el caso de la oficina corporativa.

Para probar la conexión del *router* de la sucursal con el *router* de la oficina corporativa, en *Enrutamiento y acceso remoto*, se hace clic con el botón secundario del ratón en la interfaz de marcado a petición que conecte con la oficina corporativa y, a continuación, se hace clic en *Conectar*.

4.1.1.3 Implementar certificados para la autenticación

Certificados para conexiones L2TP/IPSec. Windows Server 2003 admite dos métodos de autenticación para las conexiones VPN basadas en L2TP/IPSec: certificados de equipo y claves previamente compartidas.

Para crear una conexión L2TP/IPSec con el método de autenticación de certificados de equipo, se debe instalar un certificado en el almacén de certificados

del equipo local en el cliente VPN y en el servidor VPN. Para instalar un certificado de equipo, se debe haber una entidad emisora de certificados. Una vez configurada la entidad emisora de certificados, se podrá instalar certificados de tres formas distintas:

- Mediante la configuración de la inscripción automática de certificados de equipo en los equipos de un dominio de Windows Server 2003.
- Mediante el complemento Certificados para obtener un certificado de equipo.
- Mediante el explorador para conectarse a las páginas de inscripción en Web de la entidad emisora de certificados (CA) con el fin de instalar un certificado en el equipo local o almacenarlo en un disquete para su instalación en otro equipo, por ejemplo en el equipo doméstico de un usuario.

En función de las directivas de certificados establecidas en su organización, sólo se debe realizar una de las asignaciones anteriores. Los equipos que no son miembros de un dominio no pueden obtener certificados mediante la inscripción automática.

Para configurar una entidad emisora de certificados e instalar el certificado de equipo, se deben realizar los pasos siguientes:

1. Si no se tiene ya una CA raíz de empresa si es necesario, hay que promover el equipo que funcionará como CA a controlador de dominio (DC) e instalar el componente *Servicios de Certificate Server* como una entidad emisora de certificados raíz de empresa en un equipo que ejecute Windows Server 2003.
2. Para inscribir automáticamente certificados de equipo, configurar el dominio de Windows Server 2003. Para crear un certificado de equipo para el servidor VPN que es miembro del dominio en el que se ha configurado la inscripción automática (así como otros equipos miembros del dominio), hay que reiniciar el equipo o escribir `gpupdate/target:computer` en el símbolo del sistema de Windows Server 2003.

3. Para inscribir manualmente certificados de equipo, se debe utilizar el complemento Certificados para instalar el certificado raíz de la CA.

Tarjetas inteligentes y conexiones de acceso remoto. El uso de tarjetas inteligentes para la autenticación de usuarios es la forma de autenticación más segura en Windows Server 2003. Para las conexiones VPN de acceso remoto, se debe utilizar EAP con el tipo EAP Tarjeta inteligente u otro certificado, también conocido como EAP-TLS. Para utilizar tarjetas inteligentes en la autenticación VPN de acceso remoto, se deben realizar las acciones siguientes:

1. Configurar el servidor VPN para que proporcione servicios VPN de acceso remoto.
2. Instalar un certificado de equipo en el servidor VPN.
3. Habilitar el proceso de inicio de sesión con tarjetas inteligentes en el dominio.
4. Habilitar EAP y configurar el tipo EAP Tarjeta inteligente u otro certificado en el servidor VPN.
5. Habilitar la autenticación de tarjetas inteligentes en la conexión VPN del equipo cliente de acceso remoto.

Se tiene que instalar un lector de tarjetas inteligentes en el equipo cliente de acceso remoto. Una vez instalado el lector de tarjetas inteligentes en el equipo que ejecuta Windows XP, se le preguntará si desea utilizar la tarjeta inteligente para realizar la autenticación cuando se creen conexiones VPN o de acceso telefónico. En las conexiones VPN o de acceso telefónico existentes, se puede habilitar la autenticación de tarjetas inteligentes en las propiedades de la conexión VPN o de acceso telefónico.

Autenticación basada en certificados para las VPN de sitio a sitio. El uso de certificados para la autenticación de *routers* de llamada es la forma más segura de autenticación en la familia Windows Server 2003. Para la autenticación basada en certificados de las conexiones de marcado a petición, se debe utilizar EAP con el

tipo EAP Tarjeta inteligente u otro certificado (EAP-TLS). EAP-TLS requiere el uso de certificados de usuario para el *router* de llamada y certificados de equipo para el *router* de respuesta. [52]

4.1.2 Configuración de un cliente VPN en Windows XP

Para configurar un cliente VPN en el sistema operativo Windows XP es necesario seguir los siguientes pasos:

1. Abrir la carpeta de *Conexiones de red* y en el menú Archivo seleccionar *Nueva conexión*. En el asistente para conexión nueva seleccionar *Conectarse a la red de mi lugar de trabajo*, y pulsar siguiente.
2. Seleccionar *Conexión de red privada virtual*, y pulsar siguiente.

En la figura 4.3 se ilustran los pasos 1 y 2.

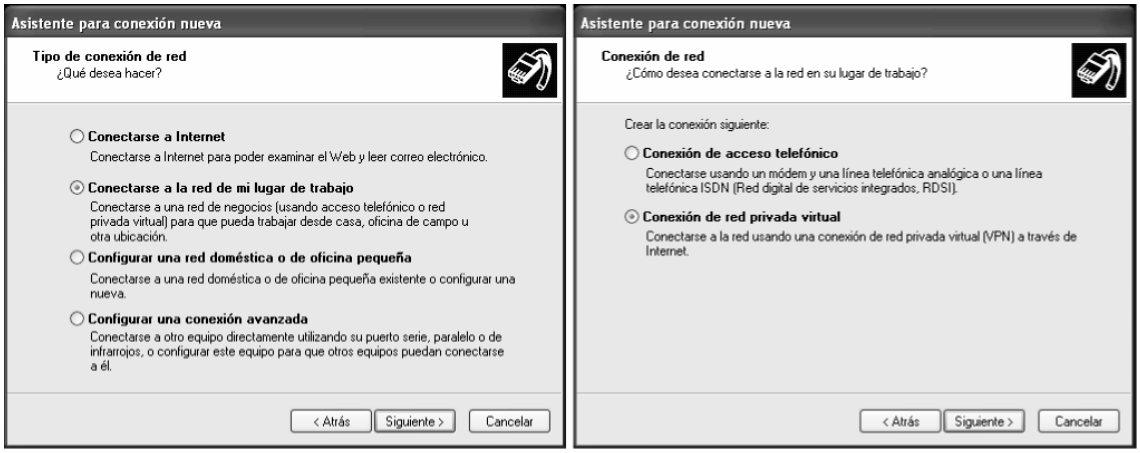

Figura 4.3 *Fichas Tipo de conexión de red y conexión de red del Asistente*

3. En la siguiente ventana, marcar la opción *no usar conexión inicial* a menos que se quiera que con la VPN se utilice otra de las conexiones a Internet, si se indica que al activar esta conexión se active antes otra conexión, por ejemplo una conexión telefónica, se conectará primero a Internet y luego se establecerá la VPN. Si se dispone de cable o ADSL no es necesario activar ninguna de estas conexiones. Tampoco lo es si se está conectado a Internet cuando se activa la conexión VPN o no se quiere que ésta marque

ninguna conexión. En la siguiente ventana se indica el nombre de la conexión. Por último indicar la dirección IP del servidor VPN, esta es la dirección IP pública, es decir, la que tiene en Internet en el momento de establecer la conexión entre los clientes y el servidor. Esto se muestra en la figura 4.4.

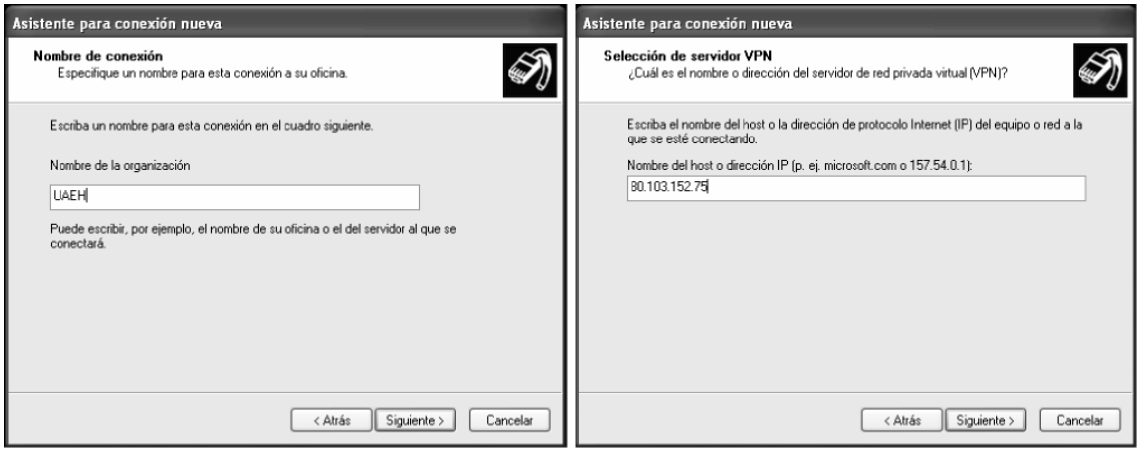

Figura 4.4 *Fichas Nombre de conexión y Servidor VPN del Asistente*

4. Al finalizar el asistente ya se tendrá la conexión lista para activarse. Ahora se indica el usuario y las contraseñas que se han activado en el servidor, tal como aparece en la figura 4.5. [34]

Figura 4.5 *Ventana de inicio para conectarse al servidor VPN*

5. Para configurar correctamente el cliente VPN, se debe seleccionar *Propiedades* de la conexión VPN. La ficha *Seguridad* permite configurar el método de validación de identidades y el botón de *Configuración* permite configurar los protocolos de seguridad (PAP, CHAP, EAP, SPAP, MS-CHAP y MS-CHAPv2) que se pueden utilizar para conectar con el servidor. También se puede configurar la utilización de un nombre de inicio y contraseña de Windows. El botón de *Configuración IPSec* permite establecer una clave previamente compartida. Estos parámetros deben ser configurados por el administrador del servidor; de lo contrario una mala configuración podría abrir brechas en la seguridad o ser incapaz de conectarse con el servidor VPN. Esto se muestra en la figura 4.6.

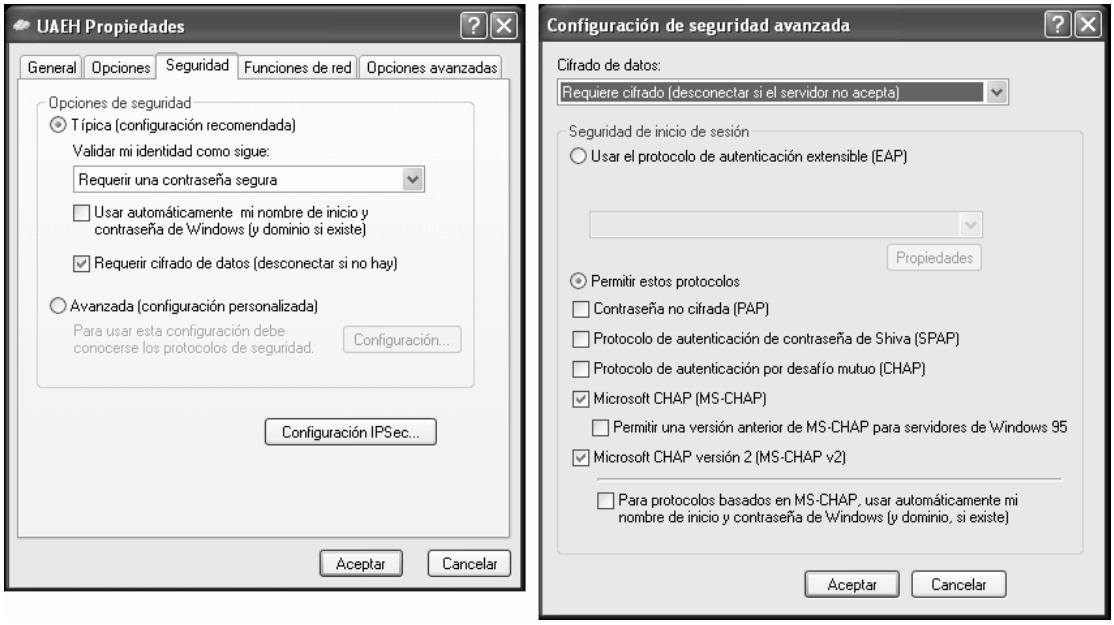

Figura 4.6 *Ficha Seguridad y Configuración Avanzada*

6. La ficha *Funciones de red* permite seleccionar el tipo de túnel que se va a utilizar, así como los componentes de red que va a utilizar la conexión, como se muestra en la figura 4.7.

Figura 4.7 *Ficha Funciones de Red* [16]

Con estos pasos se configura la conexión VPN de tal manera que ya está lista para funcionar. Si se trabaja con conexiones lentas (módem o similar), la VPN también irá lenta. Es recomendable disponer de conexiones de banda ancha (módem de cable, ADSL) para sacarle todo el rendimiento a este tipo de conexiones.

Para realizar las comunicaciones usando la VPN se deben usar las direcciones IP de la VPN. Es decir, además de la dirección IP de Internet que tiene el servidor y los clientes se han generado otras direcciones IP internas de la VPN, pues esas se deberán usar para comunicarse con los equipos de la VPN, éstas se obtendrán como las habituales, pero en el icono de la nueva conexión que aparece en la barra de notificación.

En conexiones lentas, el Explorador de Windows no será capaz de mostrar los otros equipos de la red, o le llevará mucho tiempo, en ese caso, se puede acceder a ellos escribiendo en la barra de direcciones del Explorardor de Windows `\\dirección_IP_del_equipo` o `\\nombre_maquina` de la computadora a la que se desea acceder. Por ejemplo, si la IP (en la VPN) de la otra máquina es 169.254.3.117 se escribirá `\\169.254.3.117` en la barra de direcciones del Explorador de Windows y de esta forma ya se tendrá acceso a los archivos e

impresoras de la computadora indicada. Para usar otros recursos, como servidores de base de datos, etc. simplemente se utilizará la dirección IP en la VPN de la computadora destino.

Además, si los equipos no tienen realizada la configuración de red adecuadamente, o tienen mal asignados los permisos puede ocurrir que no se pueda acceder a recursos. Esto no es un problema de la VPN sino de cómo se tienen establecidos los permisos en cada ordenador, al igual que pasa en una red local.

Por último, y como recomendación final, es aconsejable mantener el equipo actualizado e instalar las actualizaciones que va publicando Microsoft así como los programas que la organización requiera para garantizar la seguridad. Al tratarse de un servicio de red es muy vulnerable a ser atacado y si no está convenientemente actualizado es posible ser víctimas de ataques, o los datos quizás no viajen lo suficientemente seguros como se esperaba. [34]

4.2 Configuración de una VPN en un *firewall*

4.2.1 Configuración de IPSec en el *firewall* PIX de Cisco[9]

El *firewall* PIX es un dispositivo que puede funcionar también como un activador de servicios VPN, el cual cumple con los estándares y es fácil de configurar. Los PIX 515, 520 y 525 pueden tener una tarjeta aceleradora VPN opcional (VAC). Esta tarjeta ofrece un rendimiento de cifrado 3DES a 100 Mbps sin necesidad de software adicional y sin tener que modificar la configuración del PIX. En la figura 4.8 se muestra el *firewall* PIX. [1]

Figura 4.8 *El firewall PIX de Cisco* [62]

El *firewall* PIX crea VPN en varias topologías, las cuales se presentan en la siguiente lista y en la figura 4.9:

- **De PIX a *gateway* VPN seguro de PIX.** Dos o más *firewalls* PIX pueden habilitar una VPN, que protege el tráfico entre los dispositivos colocados detrás de los *firewalls* PIX. La topología de *gateways* VPN seguros impide que el usuario tenga que implementar dispositivos o software VPN dentro de la red, haciendo que el *gateway* seguro sea transparente para los usuarios.
- **De PIX a *gateway* VPN seguro de *router* Cisco IOS.** El *firewall* PIX y el *router* Cisco, que ejecutan software VPN de Cisco Secure, pueden interactuar para crear un *gateway* VPN seguro entre redes.
- **De cliente VPN de Cisco a PIX a través de acceso telefónico.** El *firewall* PIX puede convertirse en un punto final para el cliente VPN de Cisco a

[9] Nuevamente, se menciona que la configuración VPN es diferente para cada caso, describiéndose aquí sólo los pasos generales.

través de una red de acceso telefónico. Esta red puede estar formada por RDSI, PSTN o DSL.

- **De cliente VPN de Cisco a PIX a través de red.** El *firewall* PIX puede convertirse en un punto final VPN para el cliente VPN 3000 de Cisco Secure a través de una red IP.
- **De productos de otros fabricantes a PIX.** Los productos de otros fabricantes pueden conectarse con el *firewall* PIX si se adaptan a los estándares VPN abiertos.

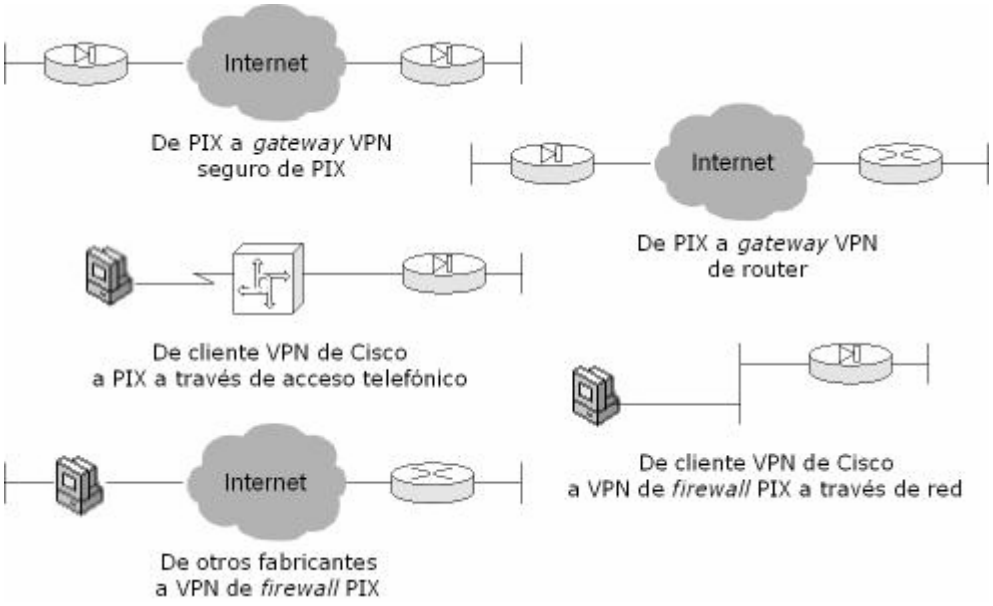

Figura 4.9 *Topologías VPN con el firewall PIX*

Cualquier *firewall* PIX que ejecute el sistema operativo 5.0 y posterior del PIX utiliza el conjunto de protocolos IPSec para activar las opciones VPN. El *firewall* PIX soporta los estándares IPSec tales como IKE, DES, 3DES, D-H, MD5, SHA-1, RSA, CA, SA.

Se puede configurar IPSec en el *firewall* PIX por medio de claves previamente compartidas para la autenticación. El uso de estas claves IKE para la autenticación de sesiones IPSec es relativamente fácil de configurar, aunque no escala bien cuando hay un gran número de iguales IPSec; en cuyo caso, habrá

que usar certificados digitales. Para configurar IPSec se deben llevar a cabo los siguientes pasos:

1. Preparar la VPN para IPSec
2. Configurar IKE para el uso de claves previamente compartidas
3. Configurar IPSec en el *firewall*
4. Comprobar y verificar la configuración de IPSec

4.2.1.1 Preparación de IPSec

La implementación satisfactoria de una VPN basada en IPSec requiere una planificación minuciosa antes de empezar a configurar los *firewalls* PIX individuales y otros dispositivos IPSec. Se debe empezar por definir detalladamente las normas de seguridad IPSec basándose en las normas de seguridad de la empresa en cuestión. Se debe identificar los *hosts* y las redes que se desea proteger, la elección de un método de autenticación, la determinación de los detalles acerca de los iguales IPSec, la identificación de las opciones IPSec necesarias y la garantía de que las listas de acceso existentes permiten el tráfico IPSec. Si hay un *router* frente al *firewall* PIX, éste deberá permitir los protocolos IP 50 y 51 y el puerto UDP 500.

Para planear adecuadamente una VPN con IPSec es conveniente seguir los siguientes pasos:

1. Determinación de las normas de la fase 1 de IKE entre iguales IPSec en base al número y la ubicación de los iguales.
2. Determinación de las normas de la fase 2 de IKE, incluyendo detalles del igual IPSec, como las direcciones IP y los conjuntos y modos de transformación IPSec.
3. Comprobación de la configuración activa del *firewall* utilizando los comandos necesarios.

4. Asegurarse de que la red funciona sin cifrado para eliminar problemas básicos utilizando el comando *ping* y ejecutando el tráfico de prueba antes de probar el cifrado.
5. Asegurarse de que las listas de acceso existentes en el *router* de perímetro y en el *firewall* PIX permiten el tráfico IPSec, o el tráfico deseado será filtrado.

4.2.1.2 Configuración de IKE o de una CA

Uso de claves previamente compartidas con IKE. El segundo paso para configurar IPSec en el *firewall* PIX consiste en configurar los parámetros del IKE. En los comandos de configuración del PIX, ISAKMP es sinónimo de IKE. La configuración del cifrado IPSec puede ser complicada, por lo que se deberá planificar previamente el cifrado con el fin de minimizar los errores en la configuración. Se deben definir las necesidades y la estrategia de seguridad general basándose en las normas de seguridad de la empresa. Los pasos necesarios para configurar IKE son los siguientes:

1. Activar o desactivar IKE utilizando el comando `isakmp enable`
2. Crear las normas IKE con los comandos `isakmp policy`
3. Configurar las claves previamente compartidas usando el comando `isakmp key` y sus comandos asociados. Al igual que ocurre con cualquier igual IPSec que use claves previamente compartidas, se deberá configurar la misma clave en cada par de iguales IPSec. Es conveniente configurar claves distintas para cada par de iguales IPSec; de lo contrario, la seguridad de la VPN se pondría en riesgo.
4. Verificar qué método va a utilizar IKE para verificar su igual de cifrado. Cuando dos iguales utilizan IKE para establecer SA de IPSec, cada igual enviará su identidad ISAKMP al igual remoto. Enviará su dirección IP o su nombre de *host* en función de cómo esté establecida la identidad ISAKMP de cada uno. Por defecto, la identidad ISAKMP de la unidad del *firewall* PIX está establecida a la dirección IP. Como regla general, se establece el

firewall PIX y las identidades de sus iguales de la misma forma para evitar un fallo en la negociación de IKE. Este fallo podría ser debido al *firewall* PIX o al igual que no está reconociendo su identidad. Para determinar el método que va a utilizar el PIX para verificar la identidad de un igual, se utiliza el comando `show isakmp identity`.

5. Verificar la configuración de IKE con el comando `show isakmp policy`.

Uso de una CA en el *firewall* PIX. El uso de claves previamente compartidas para la autenticación sólo funciona cuando hay pocos iguales IPSec. Es uso de una CA permite ampliar la autenticación a un gran número de iguales IPSec. Mientras que IKE requiere la Intervención manual para generar y distribuir las claves a un igual cada vez, el proceso de inscripción a un servidor CA puede automatizarse mucho, por lo que es conveniente cuando la empresa es muy grande. Cada igual IPSec se inscribe individualmente en el servidor CA y obtiene un certificado digital compatible con otros iguales que estén inscritos en el servidor. Para inscribirse a una CA se siguen los pasos siguientes:

1. El *firewall* PIX genera un par de claves RSA
2. El *firewall* PIX obtiene el certificado de la CA, el cual contiene la clave pública de la CA
3. El *firewall* PIX pide un certificado firmado de la CA que utilice las claves RSA públicas generadas y la clave/certificado públicos del servidor CA
4. El administrador de la CA verifica la petición y envía un certificado firmado.

4.2.1.3 Configuración de IPSec

El siguiente paso en la configuración de IPSec en el *firewall* PIX es configurar los parámetros IPSec recopilados en los pasos anteriores. Los pasos a seguir para configurar IPSec en el *firewall* PIX se enlistan a continuación:

1. Configurar las listas de acceso de cifrado con el comando `access-list`
2. Configuración de paquetes de conjuntos de transformación con el comando `crypto ipsec transform-set`

3. Este paso es opcional. Se puede configurar los tiempos de existencia globales de las SA de IPSec con el comando `crypto ipsec security-association lifetime`
4. Configurar los mapas de cifrado con el comando `crypto-map`
5. Aplicación de los mapas de cifrado a la interfaz de terminación/origen con el comando `crypto map map-name interface`

Configuración de las listas de acceso de cifrado. Estas listas definen qué tráfico IP va a ser protegido por IPSec. Estas listas realizan las siguientes funciones para IPSec:

- Seleccionar el tráfico saliente que IPSec va a proteger
- Procesar el tráfico entrante para filtrar y descartar el tráfico que tendría que ser protegido por IPSec
- Determinar si se van a aceptar peticiones para las SA IPSec con respecto a los flujos de datos solicitados a la hora de procesar negociaciones IKE.

La configuración de las listas de acceso deberán ser iguales en cada partes IPSec o de lo contrario no podrá crearse una SA. Para configurar la lista de acceso, se utiliza el comando `access-list`.

Configuración de paquetes de conjuntos de transformación. Este es el siguiente paso en la configuración de IPSec en el *firewall* y consiste en usar las normas de seguridad para definir un conjunto de transformación. Un conjunto de transformación es una combinación de transformaciones IPSec individuales que habilitan unas normas de seguridad para el tráfico. Los conjuntos de transformación combinan los siguientes factores IPSec:

- Un mecanismo para la autenticación de paquetes: la transformación AH
- Un mecanismo de cifrado y autenticación: la transformación ESP
- El modo IPSec, ya sea transporte o túnel.

El comando utilizado para realizar esto es `crypto ipsec tranform-set`.

La elección de transformaciones IPSec puede ser compleja, por lo que se sugiere tomar en cuenta lo siguiente:

- Si se desea confidencialidad de los datos, utilizar la transformación ESP
- Considerar la inclusión de una transformación ESP o AH para proporcionar servicios de autenticación al conjunto de transformación
- Para garantizar la autenticación de los datos de la cabecera IP externa, además de los datos, incluir una transformación AH
- Para garantizar la autenticación de los datos (ESP o AH), se puede optar entre los algoritmos de autenticación MD5 o SHA[10]
- El algoritmo SHA es más robusto que MD5, pero resulta más lento

Configuración de los tiempos de existencia globales de las SA IPSec. El tiempo de existencia determina el tiempo durante el que las SA IPSec mantienen su validez antes de ser negociadas nuevamente. Los tiempos de existencia sólo se aplican a las SA que estén establecidas a través del IKE. Las SA establecidas manualmente no expiran. Cuando una SA expira, se negocia una nueva sin interrumpir el flujo de datos.

Antes de que expire una clave, el IKE negocia otra basándose en el valor del tiempo de existencia de la SA IPSec para permitir que haya una transición suave de clave a clave sin necesidad de cortar las conexiones.

El comando utilizado para cambiar los valores de tiempo es `crypto ipsec security-association lifetime`.

Creación de los mapas de cifrado. Es necesario crear entradas de mapas de cifrado para que IPSec configure las SA para los flujos de tráfico que deban ser cifrados. Las entradas de mapa de cifrado creados para IPSec configuran

[10] El *firewall* PIX utiliza una versión de MD5 y SHA-1 mejorado con un algoritmo llamado HMAC, el cual proporciona un nivel de dispersión (*hash*) mayor

parámetros de la SA, ensamblando las distintas partes que se configuran para IPSec, entre las que se incluyen las siguientes:

- El tráfico que debe ser protegido por IPSec (lista de acceso de cifrado)
- La diversidad del tráfico que una serie de SA va a proteger
- Dónde debe ser enviado el tráfico protegido con IPSec; es decir, quién es el igual IPSec remoto
- La interfaz local que se va a usar para el tráfico IPSec
- Qué protocolo de seguridad IPSec debe ser aplicado a este tráfico (conjuntos de transformación)
- El hecho de que las SA se establezcan manualmente o con IKE
- El tiempo de existencia de las SA IPSec
- Otros parámetros extras que podrán ser útiles para definir una SA IPSec

Se utiliza el comando `crypto-map` para configurar los mapas de cifrado.

Es posible definir múltiples iguales remotos utilizando mapas de cifrado que permitan la redundancia de *gateways*. Si un igual falla, seguirá siendo una ruta protegida. Si el intento de comunicación con un igual es fallido, el IKE probará con el siguiente igual de la lista de mapas de cifrado.

Aplicación de los mapas de cifrado a las interfaces. Este último paso consiste en aplicar el conjunto de mapas de cifrado a una interfaz. Se aplica el mapa de cifrado a la interfaz del *firewall* PIX que esté conectada a Internet a través del comando `crypto map`.

Tan pronto como se aplique el mapa de cifrado, la base de datos de SA deberá inicializarse en la memoria del sistema. Las SA estarán disponibles para ser configuradas cuando se transmita o reciba el tráfico definido por la lista de acceso de cifrado.

4.2.1.4 Comprobación y verificación de IPSec

Una vez que se ha configurado el *firewall* PIX, se procede a comprobar que todo esté funcionando de forma correcta. Existen varios comandos que ayudan a realizar esto.

Comprobar y verificar IKE. Para comprobar IKE se usan los comandos de la tabla 4.1.

Comando	Descripción
show isakmp	Muestra las normas IKE configuradas
show isakmp policy	Muestra las normas predeterminadas y las que se hayan configurado en el IKE

Tabla 4.1 *Comandos para verificar IKE*

Comprobar y verificar IPSec. Con los comandos de la tabla 4.2 se comprueba la configuración de IPSec.

Comando	Descripción
show access-list	Muestra las listas de acceso configuradas
show crypto map	Muestra la configuración del mapa de cifrado
show crypto ipsec transform-set	Muestra los conjuntos de transformación definidos
show crypto ipsec security-association lifetime	Muestra el tiempo de existencia global de la SA IPSec activa

Tabla 4.2 *Comandos para verificar IPSec*

Controlar y administrar las comunicaciones IKE e IPSec. Para observar la configuración IKE e IPSec y controlar y administrar las comunicaciones entre los iguales IPSec se usan los comandos de la tabla 4.3. [1]

Comando	Descripción
show isakmp sa	Muestra el estado actual de las SA del IKE
show crypto ipsec sa	Muestra el estado actual de las SA de IPSec. Se puede ver si el tráfico está siendo cifrado
clear crypto isakmp sa	Borra las SA IKE
clear crypto ipsec sa	Borra las SA IPSec
debug crypto isakmp	Muestra las comunicaciones IKE entre los iguales
debug crypto ipsec	Muestra las comunicaciones IPSec entre los iguales

Tabla 4.3 *Comandos para administrar comunicaciones IPSec e IKE*

4.3 Implementación de una solución VPN

4.3.1 Ejemplo de costos de una VPN

A continuación se muestra un ejemplo de cómo una solución VPN puede disminuir de manera significativa los costos económicos en comparación con una solución tradicional de acceso remoto.[11] El cálculo está basado en la solución de Cisco menos cara que se pueda implementar basado en el número de usuarios remotos simultáneos que se necesite y si se requieren clientes VPN basados en software, hardware o soluciones de *router* para los teletrabajadores.

Los datos para este ejemplo se muestran en la siguiente tabla:

Variables	Datos
Número total de usuarios remotos que actualmente hacen llamadas usando un número 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 remotos 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:

Costo mensual con solución tradicional dial-up de acceso remoto			**Costo mensual de una VPN**	
Usuarios remotos de larga distancia o número 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 Semanas/Mes (constante)	X	240	Usuarios de banda ancha	5
			Costo del ISP	x 500
				$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				
Período de reembolso: 1 mes				

[11] Este ejemplo está basado en una aplicación web creada por Cisco llamada *Cisco VPN Savings Calculator* la cual calcula el ahorro aproximado que ocurre cuando se implementa una solución VPN que permita conectividad remota para los empleados de alguna organización en particular.

4.3.1.1 Gastos de inversión

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

4.3.1.2 Ahorros mensuales

Al implementar una VPN de acceso remoto, 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.

4.3.1.3 Variables

Para este ejemplo 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 aumentarán.

4.3.1.4 Administración de la VPN

La puesta en marcha y la administración de las soluciones 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, muchas 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.

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

	Administración de una VPN internamente	Administración de una VPN externamente
	Porcentaje de ahorro de una 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 interna de una VPN. En este caso se ha estimado que costará aproximadamente $300 por usuario la administración.

Costo de administración externa de una 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 costará $300/mes y el acceso a Internet de banda ancha costará $700/mes. [25]

Conclusiones

Debido a las ventajas económicas que ofrecen las Redes Privadas Virtuales se puede concluir que se trata de una excelente tecnología para el acceso remoto, puesto que el uso de una VPN constituye un sustituto indispensable a los métodos tradicionales caros de marcación telefónica de larga distancia. Además, constituye una buena solución alterna a los métodos de implementación de redes WAN tradicionales. Mientras mayor sea la VPN, el ahorro económico será mayor.

El auge de Internet ha hecho que muchas de las tecnologías de información giren alrededor de la red de redes, y con una VPN no es la excepción, ya que esta tecnología se está convirtiendo en una tecnología casi exclusiva para redes IP y dejando atrás sus orígenes en ATM y *Frame Relay*. Es por eso que se espera que el término VPN se aplique solamente a las redes IP, y por lo tanto, a Internet.

La cuestión de la seguridad en una VPN es muy importante. La gran mayoría de las organizaciones podrán ver satisfechas sus necesidades de seguridad con las tecnologías de seguridad existentes, pero siempre será necesario llevar un control estricto de la seguridad y mantener actualizada la VPN con los últimos avances en tecnología.

Una VPN podrá ser aplicada en todo tipo de entornos, desde las grandes empresas con sucursales en diversas partes del país o del mundo y varios trabajadores móviles hasta las pequeñas empresas que tengan una o dos sucursales en una sola ciudad; así como también las diversas dependencias del gobierno que necesiten intercambiar información entre ellas; e instituciones educativas como universidades y en general cualquiera que necesite acceder a sus archivos desde una ubicación remota de manera segura podrá obtener beneficios con esta tecnología.

Anexos

Anexo 1.- Proveedores de Servicios VPN [18]

Este es un listado de los algunos proveedores de servicios VPN en México:

- Enter Computadoras y Servicios SA de CV
  - www.entercs.com.mx
  - telemarketing@entercs.com.mx
- Sistemas Comerciales RAC
  - www.sisrac.com
  - informes@sisrac.com
- Conecta SA de CV/Ericsson
  - www.conectaericsson.com.mx
  - ventas@conectaericsson.com.mx
  - servicio@conectaericsson.com.mx
- DataPhone
  - www.dataphone.com.mx
  - 5355-4788
- SDSC/Alcatel
  - www.sdsc.com.mx
  - dirección@sdsc.com.mx
  - Ventas: 5273-2121
  - Servicio: 9172-4220
  - Interior de la República: 01-800-2217-214
- Synetcom
  - www.synetcom.com.mx
  - soluciones@synetcom.com.mx
  - ventas@synetcom.com.mx
- Avantel
  - www.avantel.com.mx

    - Clientes empresa: 01-800-021-0111
    - Ventas empresarial: 01-800-800-7963
- Telmex
    - www.telmex.com.mx
- Axtel
    - www.axtel.com.mx
    - Empresas: 1515-0000
    - Hogar y PYMES: 1515-1515
    - Puebla, Toluca, Querétaro y Veracruz: 515-0000 y 515-1515
- RedUno
    - www.reduno.com.mx
- MTM Telecom
    - www.mtm-telecom.com
    - 5716-9065
- TEMSA
    - www.temsa.net.mx
    - ventas@temsa.net.mx
    - 5999-9959
- Mexis
    - www.mexis.net
    - informes@mexis.net
    - (55)-5000-4499

Anexo 2.- Caso de Estudio *American National de México* [24]

American National Insurance Company se fundó en 1905 en la Cd. de Galveston, Texas. Esta empresa ha sido catalogada como una de las empresas líderes en seguros en el mundo. Fue en 1998 cuando esta compañía de antecedentes norteamericanos conformó un nuevo proyecto mediante un plan de negocios para desarrollar operaciones de servicio domiciliado en todo México.

En la actualidad tiene establecidas oficinas en las plazas más importantes del norte del país incluyendo a Monterrey, Saltillo, Ciudad Juárez, Torreón, Gómez Palacio, Matamoros, Nuevo Laredo, Reynosa y Piedras Negras, pretendiendo en el futuro próximo extenderse a más ciudades en México.

American National de México es la empresa pionera y líder del mercado de servicio a domicilio, que busca desarrollar y mantener capacitada a su fuerza de ventas mediante una estructura organizacional flexible y efectiva. Ese objetivo está fundamentado en gran parte gracias al uso de la tecnología, que tiene como propósito mejorar las comunicaciones entre el personal del corporativo para mejorar la atención hacia sus clientes.

La demanda de servicios comenzaba a ser más intensa y los costos de comunicación se incrementaban constantemente. “Nuestra operación estaba basada en tecnología de marcación (*dial-up*). Era algo rudimentario la manera en que nos estábamos comunicando entre oficinas de ventas y el corporativo, era muy lento. Los procesos se llevaban alrededor de media hora a 45 minutos, era difícil”, comenta Gilberto Hernández, Gerente de Telecomunicaciones de *American National de México*. “Teníamos serios problemas en cuanto a gasto telefónico y además la productividad de la gente en cuanto a sus procesos no era la deseada”.

Analizando las tecnologías disponibles en el mercado, *American National de México* vio la respuesta a sus demandas en las soluciones de Cisco Systems, las cuales inmediatamente se ajustaron a las necesidades de comunicación y ofrecieron las alternativas suficientes para desarrollar una infraestructura de comunicaciones en la compañía.

La solución de Cisco vino a concretarse de la mano del socio *Plannet*, que recayó en la integración de una VPN que conectó las oficinas de ventas y los usuarios remotos, dando forma y disminuyendo los costos inmediatamente en cuanto a conectividad al ser una tecnología adaptada a Internet.

Fue un proyecto que duró varios meses de planeación, el cual requirió de una validación por el mismo cliente y a través del Centro de Soluciones de Cisco, quienes fungieron como guías en el desarrollo de la solución y su implantación, que abarcó la oficina matriz y sus 15 oficinas de ventas.

Establecida la infraestructura de comunicaciones basada en una VPN proveída por Cisco, *American National de México* sufrió varios y considerables cambios que retribuyeron en cuantiosos beneficios, algunos inmediatos y otros que se esperan a largo plazo.

En primera instancia el gasto telefónico fue de los primeros impactos positivos al implementar la solución. El costo por servicio telefónico disminuyó en un rango de 60% en el que se contempla un 85% por larga distancia, y un 50% por servicio medido.

El siguiente punto fue el incremento en productividad, traducida en reducción de tiempos para la transmisión de datos, que bajaron prácticamente un 90% debido a la nueva conectividad. El personal que percibió con muchísimo agrado la solución fue el administrativo. Para las personas que trabajan en esta área fue algo totalmente increíble, pues llevaban más de tres años acostumbrados a trabajar con dial-up, no tenían idea de lo que se podía lograr con esta nueva tecnología.

La tecnología VPN de Cisco ha contribuido de esta forma a los proyectos de expansión de *American National de México*, la cual busca extender sus servicios a otras ciudades de la República.

Anexo 3.- Especificaciones del Firewall PIX [26]

Características y ventajas de la serie Cisco Secure PIX *Firewall*, Software V.4.4

Características	**Ventajas**
Algoritmo de seguridad adaptable	Proporciona una seguridad completa para todas las sesiones TCP/IP en la protección de recursos privados y sensibles
Proxy Cut-through	Ofrece el mayor rendimiento de la industria en autenticación. Costes de propiedad más bajos en la reutilización de las actuales bases de datos de autenticación
Sistema en tiempo real seguro incorporado	Proporciona una mayor seguridad que otros sistemas operativos abiertos basados en estándares, como estaciones de trabajo UNIX o NT
Una variedad de tarjetas de interfaz de red	Ofrece una mayor seguridad a los servidores Web u otros servidores accesibles al público, enlaces múltiples extranet con distintos colaboradores, servidores de filtración URL y protección de acceso, entre otras funciones
Evita los ataques de denegación de servicio	Protege el firewall y los servidores y clientes que se hallan detrás de aquél, de hackers dañinos o perjudiciales; da seguridad a todas las transacciones y servicios contra posibles ataques de denegación de servicio
Admite hasta 256.000 conexiones simultáneas	Maximiza el rendimiento de los servidores proxy, lo que se traduce en la instalación de un menor número de firewalls
Soporta IETF IPSec	Permite la interoperatividad VPN, capacidad de ampliación y la reducción de los costes administrativos
Da soporte a una amplia gama de aplicaciones	Reduce el impacto de un firewall sobre los usuarios de una red
Asistente de configuración y PIX Firewall Manager	Ahorra tiempo y dinero reduciendo los periodos de inactividad de la red y los costes de instalación
Informes de gestión; contabilidad de URL	Ahorra tiempo al permitir una rápida visualización de la actividad del Firewall, incluyendo los datos de contabilidad
Filtración URL	Proporciona la posibilidad de controlar qué tipo de sitios Web visitan los usuarios, y mantiene un registro de la auditoría con fines contables; tiene un impacto mínimo sobre el rendimiento del PIX Firewall
Filtro de aplicaciones Java	Permite que el firewall pueda detener las aplicaciones Java potencialmente peligrosas, tomando como base el cliente o una dirección IP
Mail Guard	Elimina la necesidad de un retransmisor externo de correo en el perímetro de la red y los ataques de denegación de servicio sobre los retransmisores externos de correo
Soporte de aplicaciones multimedia	Reduce el tiempo y coste de administración necesarios para dar soporte a estos protocolos No requiere ninguna configuración especial en el cliente

Recuperación de fallos/mecanismo de espera en actividad	Ofrece una alta disponibilidad para aumentar al máximo la fiabilidad de la red
Conversión de direcciones de la red	Ahorra el alto coste de la renumeración IP Amplía el espacio de direcciones de la red
Sin conversión	Permite la identificación segura del cliente al usar direcciones IP existentes
Certificados/auditorías	Ofrece complementos de otros fabricantes en la validación de seguridad---Certificado ICSA, auditoria de seguridad de SRI, pendiente de la certificación NSA Common Criteria

Especificaciones y plataformas hardware	**PIX Firewall 515-R**	**PIX Firewall 515-UR**	**PIX Firewall 520**	**PIX Firewall 520-DC**
Estructura de hardware	Bastidor desmontable de 19 pulgadas (incluye el hardware de montaje)	Bastidor desmontable de 19 pulgadas (incluye el hardware de montaje)	Bastidor desmontable de 19 pulgadas (incluye el hardware de montaje)	Bastidor desmontable de 19 pulgadas (incluye el hardware de montaje)
Memoria de acceso aleatorio	32 MB	64 MB	128 MB	128 MB
Memoria Flash	16 MB	16 MB	16 MB	16 MB
Puerto de consola	RJ-45	RJ-45	DB-9 EIA/TIA-232	DB-9 EIA/TIA-232
Dispositivo de inicio/actualización	Sólo TFTP	Sólo TFTP	Unidad de disco flexible de 3,5 pulgadas	Unidad de disco flexible de 3,5 pulgadas
Puerto de recuperación de fallos	DB-25 EIA/TIA-232	DB-25 EIA/TIA-232	DB-25 EIA/TIA-232	DB-25 EIA/TIA-232
Dimensiones físicas				
Altura	1.72"	1.72"	5,21 pulgadas	5,21 pulgadas
Anchura	16,82 pulgadas	16,82 pulgadas	16,82 pulgadas	16,82 pulgadas
Profundidad	11,8 pulgadas	11,8 pulgadas	17,5 pulgadas	17,5 pulgadas
Peso	11 libras	11 libras	21 libras	21 libras
Requisitos de alimentación				
Autoconmutación	100-240 VCA	100-240 VCA	100-240 VCA	-48 VCC
Frecuencia	50-60 Hz	50-60 Hz	50-60 Hz	---
Corriente	1,5-0,75 amperios	1,5-0,75 amperios	4-2 amperios	4 amperios

Entorno de actividad				
Temperatura de actividad	de -5º0 a +45ºC (de -25ºF a 113ºF)	de -5º0 a +45ºC (de -25ºF a 113ºF)	de -5º0 a +45ºC (de -25ºF a 113ºF)	de -5º0 a +45ºC (de -25ºF a 113ºF)
Temperatura de inactividad	de -25ºC a +70ºC	de -25ºC a +70ºC	de -25ºC a +70ºC	de -25ºC a +70ºC
Humedad de actividad:	95% de humedad relativa (RH)	95% de humedad relativa (RH)	95% de humedad relativa (RH)	95% de humedad relativa (RH)
Altitud de actividad:	3.000 m (9.843 pies), 25º C (77º F)	3.000 m (9.843 pies), 25º C (77º F)	3.000 m (9.843 pies), 25º C (77º F)	3.000 m (9.843 pies), 25º C (77º F)
Altitud de inactividad	4.570m. (15.000 pies), 25º C (77º F)	4.570m. (15.000 pies), 25º C (77º F)	4.570m. (15.000 pies), 25º C (77º F)	4.570m. (15.000 pies), 25º C (77º F)
Choque de actividad	1,88 m/seg (74 pulgadas/seg.) 1/2 entrada de seno	1,88 m/seg (74 pulgadas/seg.) 1/2 entrada de seno	1,88 m/seg (74 pulgadas/seg.) 1/2 entrada de seno	1,88 m/seg (74 pulgadas/seg.) 1/2 entrada de seno
Choque de inactividad	60G 11 ms. 1/2 entrada de seno	60G 11 ms. 1/2 entrada de seno	60G 11 ms. 1/2 entrada de seno	60G 11 ms. 1/2 entrada de seno
Vibración de actividad	0,41 Grms2 (5-500 Hz) entrada aleatoria	0,41 Grms2 (5-500 Hz) entrada aleatoria	0,41 Grms2 (5-500 Hz) entrada aleatoria	0,41 Grms2 (5-500 Hz) entrada aleatoria
Vibración de inactividad	0,41 Grms2 (5-500 Hz) entrada aleatoria	0,41 Grms2 (5-500 Hz) entrada aleatoria	0,41 Grms2 (5-500 Hz) entrada aleatoria	0,41 Grms2 (5-500 Hz) entrada aleatoria
Disipación de calor (en el peor de los casos y con la máxima alimentación)	160,37 BTU/hr	160,37 BTU/hr	863,27 BTU/hr	863,27 BTU/hr
EMI	CE,VCCI clase II, FCC, BCIQ, Austel	CE,VCCI clase II, FCC, BCIQ, Austel	CE,VCCI clase II, FCC, BCIQ, Austel	CE,VCCI clase II, FCC, BCIQ, Austel
Agencias de seguridad	UL, C-UL, TUV, IEC 950	UL, C-UL, TUV, IEC 950	UL, C-UL, TUV, IEC 950	UL, C-UL, TUV, IEC 950
Estándar UL-1950	3ª edición	3ª edición	3ª edición	3ª edición
TUV EN 60950	2ª edición, Am.1-4	2ª edición, Am.1-4	2ª edición, Am.1-4	2ª edición, Am.1-4
Estándar IEC-950/VDE-0805 EN-60-950	Sí	Sí	Sí	Sí
Bellcore	No	No	No	NEBS Nivel 3 probado en Bellcore GR-63 y GR-1089

Glosario

- **Acceso remoto.** Conectarse a una red desde una ubicación distante.
- **Autenticación.** Es que un dato demuestre que viene del origen pretendido o que un usuario demuestre que es quien dice ser. Un sistema de autenticación es aquel donde un usuario se identifica ante un servidor remoto. Algunos sistemas de autenticación son *Kerberos* o PKI.
- **Cifrado.** Es un conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Existen muchas algoritmos de cifrado tales como DES, 3DES, RSA, SHA-1, MD5, etc.
- **Dial-up.** Forma de conectarse a una red donde se debe hacer una llamada para poder conectarse. La conexión finaliza en el momento de colgar.
- **Extranet.** Una extranet es una intranet orientada a las personas u organizaciones que son externas a su empresa, pero necesitan acceder a alguna información, así se les permite el acceso a este contenido adicional, siempre bajo un sistema de autenticación y control de acceso.
- **Firewall.** 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.
- **IETF.** Es una organización dedicada a desarrollar y proponer estándares para el funcionamiento de Internet. Dichos estándares están publicados en documentos llamados Solicitud de Comentarios (RFC).
- **Intranet.** Una intranet es una Internet orientada a una organización en particular. Una intranet reside dentro de un *firewall* y éste impide el acceso a los usuarios no autorizados.
- **IPSec.** Es un marco de estándares abiertos para lograr comunicaciones privadas seguras a través de redes IP mediante el uso de servicios de seguridad criptográfica.
- **ISP.** Es una organización que proporciona servicios de Internet a empresas y particulares.

- **MPLS.** Es un método de reenvío de paquetes basado en etiquetas. Estas pueden corresponder a los destinos IP en las redes, como en el reenvío IP tradicional, pero también puede representar otros parámetros, como fuentes de direcciones, calidad de servicio (QoS) y otros protocolos. MPLS implementa intercambio de etiquetas entre diferentes módulos entre las redes.
- **OSI.** Es un modelo creado por ISO que define los métodos y protocolos necesarios para lograr la comunicación entre los equipos en una red. Este modelo define el funcionamiento de las redes en siete capas.
- **PPP.** Es un protocolo que proporciona conexiones fiables de *router* a *router* y de *host* a red. PPP es el protocolo WAN más utilizado y conocido y funciona en la capa 2 del modelo OSI.
- **Protocolo.** Es un conjunto de reglas que definen cómo interactúan las entidades de comunicación. Para que una computadora se pueda comunicar con otra se requieren de varios protocolos los cuales van a definir las reglas de la comunicación.
- **Red privada.** Es aquella red exclusiva de una sola compañía u organización en particular. La información no se comparte con otras compañías u organizaciones.
- **Red pública.** Es una red a través de la cual circula información de muchas compañías y organizaciones. Una red pública siempre será menos segura que una red privada, pero resultan ser más económicas.
- **Router.** Es un equipo que direcciona los paquetes de datos de una red a otra. Este dispositivo puede determinar cuál es la ruta más corta de un paquete hacia su destino, además de que también pueden optimizar el ancho de banda de la red y ajustarse de manera dinámica a problemas de patrones de tráfico cambiantes dentro de la red.
- **Sistema operativo de red.** Es un sistema operativo especialmente diseñado para la configuración y administración de redes. Un sistema operativo de red se instala en aquellas computadoras que van a operar como servidores.

- **TCP/IP.** Es un conjunto de protocolos que permiten la comunicación a través de varias redes diferentes y el cual constituye la base del funcionamiento de Internet.
- **Teletrabajador.** Empleado de una empresa que trabaja desde una oficina remota, lo cual generalmente es su hogar. Desde su computadora tiene acceso a ciertos recursos de la red corporativa.
- **Tunneling.** El *tunneling* es un método utilizado para encapsular paquetes (conocidos como datos de usuario) dentro de otros paquetes los cuales son enviados utilizando la tecnología de la red por la que viaja. Algunos protocolos que usan esta tecnología son PPTP y L2TP.
- **VPN.** Es una red privada que utiliza la infraestructura de una red pública para poder transmitir información.
- **WAN.** Es aquella red que está formada por la interconexión de varias LAN. Una WAN abarca una gran área geográfica de varios kilómetros. Algunas tecnologías WAN son ATM, *Frame Relay*, T1, DSL, etc.

Siglario

- **3DES**. Triple DES
- **AAA**. *Authentication, Authorization, Accounting* (Autenticación, Autorización y Contabilidad)
- **ADSL**. *Asymmetric DSL* (DSL Asimétrico)
- **AH**. *Authentication Header* (Cabecera de autenticación)
- **ARP**. *Address Resolution Protocol* (Protocolo de Resolución de Direcciones)
- **ATM**. *Asynchronous Transfer Mode* (Modo de Transferencia Asíncrono)
- **BRI**. *Basic Rate Interface* (Interfaz de Servicio Básico)
- **CA**. *Certification Authority* (Autoridad de Certificación)
- **CAN**. *Campus Area Network* (Red de Área de Campus)
- **CCP**. *Compression Control Protocol* (Protocolo de Control de Compresión)
- **CHAP**. *Challenge Authentication Protocol* (Protocolo de Autenticación por Desafío)
- **CPE**. *Client Point Equipment* (Equipo Terminal del Cliente)
- **CRL**. *Certificate Revocation List* (Lista de Revocación de Certificados)
- **CSI**. *Computer Security Institute* (Instituto para la Seguridad en las Computadoras)
- **DC**. *Domain Controller* (Controlador de Dominio)
- **DCE**. *Data Circuit-Terminating Equipment* (Equipo Terminador de Circuitos de Datos)
- **DES**. *Data Encryption Standard* (Estándar de Cifrado de Datos)
- **D-H**. Diffie-Hellman
- **DHCP**. *Dinamic Host Configuration Protocol* (Protocolo de Configuración Dinámica de Host)
- **DLCI**. *Data-Link Connection Identifiers* (Identificadores de Conexión de Enlace de Datos)
- **DNS**. *Domain Name System* (Sistema de Nombres de Dominio)

- **DoS**. *Deny of Service* (Ataque de Denegación de Servicio)
- **DSL**. *Digital Suscriber Line* (Línea de Abonado Digital)
- **DTE**. *Data Terminal Equipment* (Equipo Terminal de Datos)
- **EAP**. *Extensible Autenthication Protocol* (Protocolo de Autenticación Extensible)
- **ESP**. *Encapsulating Security Protocol* (Carga de Seguridad de Encapsulamiento)
- **FDDI**. *Fiber Distributed Data Interfase* (Interfaz de Datos de Fibra Distribuida)
- **FTP**. *File Transfer Protocol* (Protocolo de Transferencia de Archivos)
- **Gbps**. Gigabits por segundo
- **GRE**. *Generic Routing Encapsulation* (Encapsulación Genérica para Ruteo)
- **HDLC**. *High Data Link Control* (Control de Enlace de Datos de Alto Nivel)
- **HDSL**. *High-bit-rate DSL* (DSL de Alta Velocidad)
- **HTTP**. *HyperText Transfer Protocol* (Protocolo de Transferencia de Hipertexto)
- **IANA**. *Internet Assigned Numbers Authority* (Autoridad de Asignación de Números de Internet)
- **ICMP**. *Internet Control Message Protocol* (Protocolo de Mensajes de Control en Internet)
- **IETF**. *Internet Engineering Task Force* (Grupo de Trabajo de Ingeniería de Internet)
- **IKE**. *Internet Key Exchange* (Intercambio de claves de Internet)
- **InterNIC**. *Internet Network Information Center* (Centro de Información de Redes de Internet)
- **IP**. *Internet Protocol* (Protocolo de Internet)
- **IPSec.** Internet Protocol Security (Seguridad del Protocolo de Internet)
- **IPX**. *Internetwork Packet Exchange* (Intercambio de Paquetes de Internet)

- **ISAKMP**. *Internet Security Association and Key Management Protocol* (Protocolo de Administración de Claves y Asociación de Seguridad de Internet)
- **ISDN**. *Integrated Services Digital Network* (Red Digital de Servicios Integrados)
- **ISO**. Organización Internacional de Estandarización
- **ISP**. *Internet Service Provider* (Proveedor de Servicios de Internet)
- **Kbps**. Kilobits por segundo
- **KDC**. *Key Distribution Center* (Centro de Distribución de Claves)
- **L2F**. *Layer 2 Forwarding* (Reenvío de Capa 2)
- **L2TP**. *Layer 2 Tunneling Protocol* (Protocolo de Túnel de Capa 2)
- **LAC.** *L2TP Access Concentrator* (Concentrador de Acceso L2TP)
- **LAN**. *Local Area Network* (Red de Área Local)
- **LCP**. *Link Control Protocol* (Protocolo de Control de Enlace)
- **LLC**. *Logical Link Control* (Control de Enlace Lógico)
- **LNS.** *L2TP Network Sever* (Servidor de Red L2TP)
- **MAC**. *Media Access Control* (Control de Acceso al Medio)
- **MAN**. *Metropolitan Area Network* (Red de Área Metropolitana)
- **Mbps**. Megabits por segundo
- **MD5**. *Message Digest version 5* (Resumen del Mensaje versión 5)
- **MIT**. *Massachussets Institute of Technology* (Instituto Tecnológico de Massachussets)
- **MPLS**. *Multiprotocol Label Switching* (Conmutación de Etiquetas Multiprotocolo)
- **MPPE**. *Microsoft Point to Point Encryption* (Cifrado Punto a Punto de Microsoft)
- **MS-CHAP**. *Microsoft Challenge Authentication Protocol* (Protocolo de Autenticación por Desafío de Microsoft)
- **NAS**. *Network Access Server* (Servidor de Acceso a Red)
- **NCP**. *Network Control Protocol* (Protocolo de Control de Red)

- **NFS**. *Network File System* (Sistema de Archivos de Red)
- **NIC**. *Network Interface Card* (Tarjeta de Interfaz de Red)
- **NOS**. *Network Operating System* (Sistema Operativo de Red)
- **OC**. *Optical Carrier* (Portadora Óptica)
- **OSI**. *Open Systems Interconnection* (Sistemas Abiertos de Interconexión)
- **PAC**. *PPTP Access Concentrator* (Concentrador de Acceso PPTP)
- **PAN**. *Personal Area Network* (Red de Área Personal)
- **PAP**. *Password Authentication Protocol* (Protocolo de autenticación de contraseña)
- **PBX**. *Private Branch Exchange* (Sistema telefónico empresarial)
- **PKI**. *Public Key Infraestructure* (Infraestructura de Claves Públicas)
- **PNS**. *PPTP Network Server* (Servidor de Red PPTP)
- **POP**. *Point of Presence* (Punto de Presencia)
- **POTS**. *Plain Old Telephone Service* (Servicio Telefónico Analógico Convencional)
- **PPP**. *Point to Point Protocol (*Protocolo Punto a Punto)
- **PPTP**. *Point to Point Tunneling Protocol* (Protocolo de Túnel Punto a Punto)
- **PRI**. *Primary Rate Interface* (Interfaz de Servicio Primario)
- **PSTN**. *Public Switched Telephone Network* (Red Pública Telefónica Conmutada)
- **PVC**. *Permanent Virtual Circuits* (Circuitos Virtuales Permanentes)
- **QoS**. *Quality of Service* (Calidad de Servicio)
- **RA**. *Registration Authority* (Autoridad de Registro)
- **RADIUS**. *Remote Authentication Dial-In User Service* (Servicio de Usuario de Marcación para Autenticación Remota)
- **RADSL**. *Rate Adaptable DSL* (DSL de Velocidad Adaptable)
- **RARP**. *Reverse Address Resolution Protocol* (Protocolo de Resolución Inversa de Direcciones)
- **RAS**. *Remote Access Server* (Servidor de Acceso Remoto)
- **RDSI**. Red Digital de Servicios Integrados

- **RFC**. *Request for Comments* (Solicitud de Comentarios)
- **RSA**. Rivest Shamir Adleman
- **SA**. *Security Association* (Asociación de Seguridad)
- **SAD**. *Security Association Database* (Base de Datos de la SA)
- **SDSL**. *Single-line DSL* (DSL Simétrico o de Línea Única)
- **SHA-1**. *Security Hash Algorithm version 1* (Algoritmo de Dispersión Segura versión 1)
- **SLA**. *Service Level Agreements* (Acuerdos a Nivel del Servicio)
- **SLIP**. *Serial IP* (IP Serial)
- **SMDS**. *Switched Multimegabit Data Service* (Servicio de Datos Multimegabit Conmutado)
- **SMTP**. *Simple Network Management Protocol* (Protocolo Simple de Administración de Redes)
- **SNMP**. *Simple Network Management Protocol* (Protocolo Simple de Administración de Redes)
- **SONET**. *Synchronous Optical Network* (Red Óptica Síncrona)
- **SPAP**. *Shiva Password Authentication Protocol* (Protocolo de autenticación de contraseña de Shiva)
- **SPI**. *Security Parameter Index* (Índice de Parámetro de Seguridad)
- **STM**. *Synchronous Time Division* (División del Tiempo Síncrona)
- **STP**. *Shielded Twisted Pair* (Par Trenzado Blindado)
- **STS**. Señal de Transporte Síncrono
- **SVC**. *Switched Virtual Circuits* (Circuitos Virtuales Conmutados)
- **TCP**. *Transmission Control Protocol* (Protocolo de Control de Transmisión)
- **TDM**. *Time Division Multiplexing* (Multiplexación por División del Tiempo)
- **TFTP**. *Trivial File Transfer Protocol* (Protocolo Trivial de Transferencia de Archivos)
- **TLS**. *Transport Layer Security* (Seguridad en la Capa de Transporte)
- **UDP**. *User Datagram Protocol* (Protocolo de Datagrama de Usuario)
- **UIT-T**. Sector de Normalización de las Telecomunicaciones

- **UTP**. *Unshield Twisted Pair* (Par Trenzado sin blindaje)
- **VAC**. *VPN Acelerator Card* (Tarjeta Aceleradora VPN)
- **VC**. *Virtual Circuits* (Circuitos Virtuales)
- **VDSL**. *Very-high-data-rate DSL* (DSL de muy Alta Velocidad)
- **VPN**. *Virtual Private Network* (Red Privada Virtual)
- **WAN**. *Wide Area Network* (Red de Área Amplia)
- **WDM**. *Wavelength Division Multiplexing* (Multiplexación por División de Longitud de Onda)

Referencias bibliográficas

1. Chapman, David W; Fox, Andy. *Firewalls PIX de Cisco Secure*. Pearson Education. España, 2002
2. Cisco Systems. *Guía del Primer Año CCNA 1 y 2 3° Edición*. Pearson Education. España, 2004
3. Cisco Systems. *Guía del Segundo Año 2° Edición*. Pearson Education. España, 2002
4. Devorak, John C; Nick Anis. *Telecomunicaciones para PC*. Mc Graw-Hill. México, 1992.
5. Hallberg, Bruce A. *Fundamentos de redes*. Mc Graw-Hill. México, 2003.
6. Herrera Pérez, Enrique. *Tecnología y Redes de Transmisión de Datos*. Limusa. México, 2003.
7. Housley, Russ; Polk, Tim. *Planning for PKI*. Wiley. Estados Unidos, 2001
8. Kasacavage, Víctor. *Complete Book of Remote Access Connectivity and Security*. Auerbach. Estados Unidos, 2003
9. Kauffman, Elizabeth; Newman, Andrew. *Implementing IPSec*. Wiley. Estados Unidos, 1999
10. Keshav, S. *An Engineering Approach to Computer Networking*. AT&T Addison-Wesley. Estados Unidos, 1997
11. León-García, Alberto; Widjaja, Indra. *Redes de Comunicación*. Mc Graw-Hill. España, 2002.
12. Oppliger, Rolf. *Sistemas de autenticación para seguridad en redes*. Alfaomega. Colombia, 1998.
13. Parra Reynada, Leopoldo. *Reparación y ensamblado de computadoras*. Computación aplicada. México, 2004. pp 320
14. Pepelnjack, Ivan; Guichard, Jim. *Arquitecturas MPLS y VPN*. Pearson Education. España, 2003
15. Rábago, José Félix. *Introducción a las redes locales 2° Edición*. Anaya Multimedia. España, 2002.

16. Schmidt, Jeff. *Seguridad en Microsoft Windows 2000*. Prentice Hall. España, 2001
17. Schneier, Bruce. *Applied Cryptography*. Wiley. Estados Unidos, 1996
18. Sección Amarilla 2004-2005
19. Shneyderman, Alex. *Mobile VPN*. Wiley. Estados Unidos, 2003
20. Stallings, William. *Comunicaciones y redes de computadoras*. Prentice-Hall. México, 2004.
21. Tannembaun, Andrew. *Redes de Computadoras 4° Edición* . Prentice Hall. México, 2003.

Referencias electrónicas

22. About. *Introduction to VPN (Introduction to PPTP)*: compnetworking.about.com/od/vpn/l/aa030103a.htm
23. ADTRAN, Inc. *Understanding Virtual Private Networking*: www.adtran.com
24. Cisco Systems. *Casos de Estudio (American National de México)* :www.cisco.com/global/MX/sne/pc/tecnologia/seguridad/american.shtml
25. Cisco Systems. *Cisco VPN Savings Calculator* http://www.cisco.com/warp/public/779/largeent/learn/technologies/vpn/vpn_calc/vpnstart.html
26. Cisco Systems. *Hoja de datos Serie Cisco Secure PIX Firewall* www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/_sp_pie_ds.pdf
27. Cisco Systems. *Internetworking Technology Handbook (ATM):* www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm
28. Cisco Systems. *Internetworking Technology Handbook (Frame Relay):* www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm
29. Cisco Systems. *Internetworking Technology Handbook (QoS):* www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm
30. Cisco Systems. *Internetworking Technology Handbook (X.25):* www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/x25.htm

31. Cisco Systems. *Managed IPSec CPE VPN Solution for Service Providers*: www.cisco.com/en/US/netsol/ns562/networking_solutions_solution_category.html
32. Comunidad Académica de Microsoft Corporation. *Seguridad de Red Privada Virtual de Microsoft*: www.microsoft.com/colombia/comunidadacademica/comunidad/documentos/tips/tips3.asp
33. Desarrollo Web. *Firewall*: www.desarrolloweb.com/articulos/513.php?manual=15
34. Dobarro, Alejandro; Lagos, Manuel. *Como crear una VPN en Windows XP*. El Rincón del Programador. www.elrincondelprogramador.com/default.asp?pag=articulos/listados.asp
35. Eicon Networks, ISDN Zone. *A five minute Guide to ISDN*: www.isdnzone.com/5minguide.htm
36. Enciclopedia Wikipedia: es.wikipedia.org
37. Hernández, José. *Seguridad en conexiones VPN*. Noticias Google. 2005:news.google.com.mx/news?hl=es&ned=es_mx&q=VPN
38. IETF. *RFC 2401: Security Architecture for the Internet Protocol*. 1998.www.ietf.org/rfc/rfc2401.txt
39. IETF. *RFC 2637: Point to Point Tunneling Protocol*. 1999. www.ietf.org/rfc/rfc2637.txt
40. IETF. *RFC 2661: Layer 2 Tunneling Protocol*. 1999. www.ietf.org/rfc/rfc2661.txt
41. IETF. *RFC 2784: Generic Routing Encapsulation*. 2000. www.ietf.org/rfc/rfc2784.txt
42. Instituto Superior Politécnico José Antonio Echeverría. *Revista Telem@tica*. Año III, No. 22: www.cujae.edu.cu/revistas/telematica
43. Instituto Superior Politécnico José Antonio Echeverría. *Revista Telem@tica*. Año II, No. 18. www.cujae.edu.cu/revistas/telematica
44. Internet Security Software. *VPN Software (ViPNet)*: www.vipnet.com.mx/
45. Mason, Andrew. *Cisco Secure Virtual Private Networks*. Cisco Press.

www.ciscopress.com/articles/article.asp?p=24833&seqNum=1

46. Mercado, Claudia. *VPN: transporte de datos privados sobre infraestructura IP pública*. InfoWorld México. 2004: infoworld.ediworld.com.mx/iw_news_read.asp?iwid=3752&back=2&HistoryParam=V
47. Microsoft Corporation Windows NT Server. *Red Privada Virtual, una descripción general*: www.softdownload.com.ar
48. Microsoft Corporation. *Centro de Ayuda y Soporte Técnico de Windows XP Profesional*
49. Microsoft Corporation. *Enciclopedia Encarta 2005*
50. Microsoft Corporation. *Windows 2000 Profesional (PPP)*: www.microsoft.com/windows2000/es/professional/help/default.asp?url=/windows2000/es/professional/help/i_ppp_ras.htm
51. Microsoft Corporation. *Windows Server 2000*: www.microsoft.com/windows2000/server/default.asp
52. Microsoft Corporation. *Windows Server 2003 Tech Center*: www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/1cc1d791-f9d5-42e8-b687-35033efd4c84.mspx
53. PC-News. *VPN o Redes Privadas Virtuales*: www.pc-news.com
54. Phifer, Lisa A. *VPNs: Virtually anything?* Corecom, Inc.: www.corecom.com/html/vpn.html
55. Redacción Virtual de Cisco Systems. *Digital Suscriber Line (DSL)*: www.ciscoredaccionvirtual.com/redaccion/perfilestecnologicos/conectividad.asp?Id=23%20
56. RSA Security. *Crypto FAQ* : www.rsasecurity.com/rsalabs/node.asp?id=2253
57. San José, Sergio Gonzalo. *Herramientas para circuitos y redes virtuales*. SGI (Soluciones Globales Internet): www.sgi.es/prensa/articulos_interes/sic-ssgs-oct98.pdf
58. Securitydocs. *Understanding EAP-MD5 Authentication with RADIUS*:www.securitydocs.com/library/2470

59. Shinder, Deb. *Comparing VPN options*. WindowSecurity. 2005:www.windowsecurity.com/articles/VPN-Options.html
60. Taylor, Laura; Hecht, Bradley. *VPNs Are Hot, but What Are They? Market overview*. Intranet Journal: www.intranetjournal.com/text/articles/199911/ft_11_16_99a.html
61. Tektronix. *SONET Telecommunications Standard*. www.tektronix.com/Measurement/cgi-bin/framed.pl?Document=/Mesurement/App_Notes/SONET/&Frameset=optical
62. Tyson, Jeff. *How does VPN Work?* Alliance Datacom, L.P.: www.alliancedatacom.com/why-use-vpn.asp
63. Universidad Iberoamericana. *Redes Privadas Virtuales*: www.iec.uia.mx/proy/titulacion/proy14/vpnprin.htm
64. VPN Consortium (VPNC). *Terms Used In VPNs*: www.vpnc.org/
65. Wachtel, Bob. *All you wanted to know about T1 but were afraid to ask*. Datacomm for business, Inc. www.dcbnet.com/notes/9611t1.html
66. Webcom. *Extranet*: www.webcom.com.mx