UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE VPN SOBRE TECNOLOGÍAS MICROSOFT PPTP Y LINUX/FREESWAN

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

MIGUEL ANGEL HILARIO YACSAVILCA

PROMOCIÓN
2001 - II

LIMA – PERÚ
2006

IMPLEMENTACIÓN DE VPN SOBRE TECNOLOGÍAS MICROSOFT PPTP Y LINUX/FREESWAN

DEDICATORIA

A Dios por acompañarme en las buenas y malas demostrándome su presencia en mi vida,

A mis padres por darme la vida, el apoyo incondicional, su gran amor y el ejemplo de valorar los estudios como medio de progreso.

A mis hermanos Alicia y Humberto por el apoyo moral y económico durante estos años.

SUMARIO

Una red privada virtual(VPN) es un grupo de dos o más sistemas de ordenadores, que permiten extender las redes privadas, de forma practica, segura y eficiente. Además de significar un ahorro considerable en el costo de su implementación, frente a otras tecnologías existentes.

Las tecnologías: Microsoft/PPTP y Linux/FREESWAN son algunas alternativas de implementación de VPN, las que se muestran enfáticamente en el presente informe.

El protocolo PPTP permite utilizar enlaces de Internet económicos para crear conexiones seguras entre ordenadores e IPSEC(Linux/Freeswan) principalmente por corregir problemas que el IP presenta y por otra parte proporcionar beneficios económicos su uso.

Las tecnologías VPN de entunelamiento PPTP e IPsec presentan mejores características de seguridad, rendimiento, facilidad y económicas.

INDICE

PRÓLOGO

El objetivo de este informe es mostrar las ventajas de estas tecnologías, proporcionando la información necesaria, utilizando conceptos teóricos y prácticos en su implementación y configuración.

Los siguientes capítulos componen este informe:

- **Capitulo I** - Descripción de las Redes Privadas Virtuales(VPN), objetivo, ventajas y desventajas sobre el uso de esta tecnología. Situaciones en las que se usan y sus componentes básicos.

- **Capitulo ll** .- Análisis sobre las Tecnologías de redes WAN utilizadas antes de la aparición de las VPN .

- **Capitulo lll** .- Descripción detallada sobre las ventajas y soluciones que proporciona la implementación de las Redes Privadas Virtuales(VPN) . Conceptos de seguridad en las cuales se basan las tecnologías existentes, sobre las que se implementa las VPNs. Equipamiento para la implementación.

- **Capitulo lV** .- Alternativas de soluciones, las que comprenden tecnologías existentes más usadas para crear túneles y enlaces. Abarca temas como PPTP e IPSec.

- **Capitulo V** .- Implementaciones VPN sobre las plataformas: Microsoft Windows y Linux.

El método utilizado en el presente informe es demostrativo, se realizó una implementación con ciertas limitaciones de hardware, a diferencia de software debido a que PPTP es una herramienta dentro del sistema operativo Microsoft e IPSEC(Linux/Freeswan) el que se puede descargar de forma libre y usar sin problemas de licencias.

CAPITULO I
REDES PRIVADAS VIRTUALES (VPN)

1.1. Introducción

Una RED se puede extender sobre una área geográfica amplia, dependiendo del tamaño de la organización propietaria de la red, puede extenderse a lo largo de todo un país o continente; contiene una colección de ordenadores dedicados a ejecutar aplicaciones o programas de usuario.

Las redes se han convertido en un factor critico para cualquier organización, por que transmiten información vital en gran proporción, por tal motivo dichas redes deben cumplir con requerimientos de seguridad, fiabilidad, escalabilidad y efectividad en cuanto a costos, sobre todo aquellas que cuentan con oficinas remotas.

Los elevados costos que representaban alquilar enlaces privados o dedicados y/o llamadas de larga distancia, hicieron que las organizaciones usaran la red pública como medio de transmisión, esta demanda llevo a la invención de las VPNs (redes privadas virtuales), que son redes superpuestas sobre redes públicas pero con muchas propiedades de las privadas.

Debido a que la información se distribuye a través de la red publica, la seguridad de las redes se convierte en un tema de mucha importancia, por tal motivo se requiere aplicaciones de seguridad como firewall y las VPNs.

1.2. Definición de VPN

Una Red Privada Virtual (Virtual Private Network) es una forma de compartir y transmitir información entre un círculo de usuarios que están situados en diferentes localizaciones geográficas. Normalmente usa la red publica o Internet como medio de transporte, para establecer enlaces seguros, extendiendo las comunicaciones a oficinas remotas. Su seguridad permite la transmisión de información confidencial entre la oficina central y las sucursales de una organización, también pueden ser socios, proveedores, distribuidores, empleados y clientes. La transmisión de datos se realiza partiendo de la creación de

túneles virtuales, asegurando la confidencialidad e integridad de los datos transmitidos.

1.3. Descripción de las VPNs

Una Red Privada Virtual (VPN) básicamente se compone de dos máquinas (una a cada "extremo" de la conexión) y una ruta o **túnel** que se crea dinámicamente en una red publica o privada. Para asegurar la privacidad de esta conexión, los datos transmitidos entre ambos ordenadores son previamente encriptados y posteriormente enrutados o encaminados sobre una conexión establecida(también remota, LAN o WAN).

Las VPN constituyen una estupenda combinación entre seguridad y garantía que ofrecen las costosas redes privadas. Esta combinación hace de las redes privadas virtuales o VPNs una infraestructura confiable y de bajo costo que satisface las necesidades de comunicación de cualquier organización.

Los requisitos indispensables para establecer interconectividad son: Políticas de seguridad, requerimientos de aplicaciones en tiempo real, compartir datos, aplicaciones y recursos, además de servidor de acceso y autenticación.

1.3.1. Objetivo de las VPN

El objetivo de las VPN es presentar una gran solución para las organizaciones y empresas en cuanto a seguridad, confidencialidad e integridad de los datos, es un tema importante en las organizaciones, por la reducción de costos en comunicación y transferencia de datos.

1.3.2. Ventajas y desventajas de implementación

Las siguientes son las ventajas:

- Integridad, confidencialidad y seguridad de los datos.
- Reducción de costos.
- Utilización de herramientas de diagnóstico remoto.
- Control de acceso basado en políticas de la organización.
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Facilidad y seguridad para que los usuarios remotos se conecten a las redes corporativas.

Podemos considerar como desventaja de las VPN, que primero se deben establecer correctamente las políticas de seguridad y de acceso, por que si esto no esta bien definido pueden existir consecuencias como por ejemplo las siguientes; acceso sin restricciones a información por parte de usuarios no pertenecientes a la organización, perdida de datos al ser transmitidos a través del enlace.

1.3.3. Escenarios de implementación de las VPNs

De acuerdo al tipo de red remota que requiera interconectar la organización, además del tipo de usuarios, sean o no de la organización, se presentan tres alternativas(En la Fig.1.1 es mostrada los escenarios VPNs):

- **Intranet VPN (LAN-to-LAN VPN):** En esta situación, múltiples redes remotas de una misma organización son conectadas entre si usando una red publica, convirtiéndolas en una sola LAN corporativa lógica, con todas las ventajas de la misma.

- **Acceso remoto VPN:** En este caso, un host remoto crea un túnel para conectarse a la intranet corporativa. El dispositivo remoto puede ser un computador personal con un software cliente para crear una VPN usando una conexión conmutada o una conexión de banda ancha permanente.

- **Extranet VPN:** En esta situación ciertos recursos de la red corporativa serán accesados por redes de otras compañías, tales como clientes o proveedores. En este escenario es fundamental el control de acceso.

1.3.4. Componentes básicos

Los elementos que intervienen en la composición de una VPN son los siguientes:

- **Servidor VPN** .- Encargado de administrar los enlaces lógicos "túneles", pudiendo utilizar alternativas de tecnología, ya sea que el servidor propio sea un hardware VPN o un software que comúnmente trae los productos Microsoft o software libre para establecer túneles.

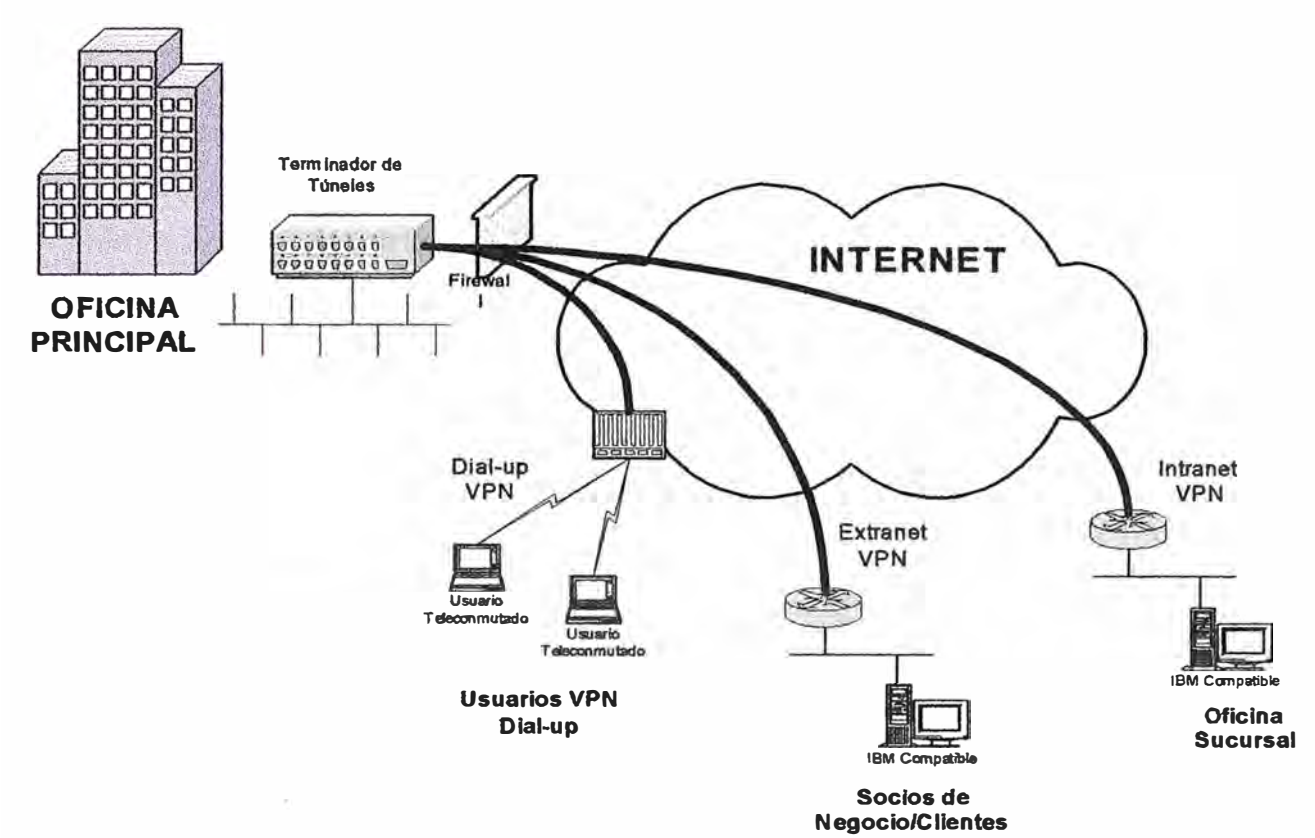

Fig.1.1Escenarios de Implementación

- **Túnel o conducto**.- Enlace lógico establecido para la transmisión de la data en forma segura y eficiente utilizando la red publica o internet como medio de transmisión.

- **Conexión VPN** .- Procedimiento en el cual se establece el túnel.

- **Red de transito**.- Medio por el cual se establecen los enlaces lógicos o túneles, y se transmite la información.

- **Clientes VPN**.- Software cliente necesario para implementar una VPN.

La implementación de la VPN debe proporcionar:

1.- Administración de usuarios, capaz de verificar la identidad de usuarios y restringir los accesos a aquellos usuarios que no estén autorizados

2.- Administración de direcciones, debe establecer direcciones de los clientes en la red privada.

3.- Codificación de datos, los datos se van a transmitir a través de la red pública debiendo ser previamente encriptados para evitar ser leídos por clientes no autorizados de la red.

4.- Administración de claves, la VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

5.- Soporte de protocolos múltiples, la VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquete de Internet(IPX) entre otros.

1.4. Resumen

El objetivo del las VPN es presentar soluciones y ventajas, a organizaciones y empresas, para interconectar redes de la misma forma que lo hace las costosas redes privadas, presentando distintos escenarios de implementación; Intranet VPN, acceso remoto VPN y extranet VPN.

CAPITULO II
NECESIDADES DE LAS TECNOLOGIAS DE REDES WAN PREVIAS A LA APARICION DE LAS VPN

Las organizaciones a través de sus redes de computadores, siempre han buscado transferir sus datos a grandes distancias, buscando la mayor confidencialidad, para satisfacer esta necesidad aparecieron los llamados "enlaces privados", además de ofrecer confidencialidad proporcionaban seguridad a los datos transmitidos. La principal desventaja que se tenia al efectuar el uso de estos enlaces, era el elevado costo que significaban a las organizaciones su uso e implementación, en los siguientes puntos se presenta alternativas de enlaces privados.

2.1. Enlaces privados

Los enlaces privados son vías de transmisión que van de extremo a extremo brindando seguridad a los datos que transmiten. Están generalmente sobre redes de transmisión en algunos casos sobre redes de conmutación.
Previamente a la aparición de las VPNs ya existían los enlaces conmutados y los enlaces dedicados.

2.1.1. Enlaces conmutados

Se dividen en enlaces conmutados analógicos que transmiten y reciben de 48kbps hasta 56kbps y enlaces conmutados digitales o enlaces RDSI o ISDN que transmiten y reciben de 64kbps hasta 128kbps (RDSI-Red Digital de Servicios Integrados).

a) Enlaces conmutados análogos

La primera tecnología de transmisión de datos, usada para construir redes privadas entre lugares remotos, aprovechó la tradicional red de telefonía publica conmutada para

transferencia de datos(al inicio solo era para voz), debido al gran desarrollo que se ha tenido en los últimos años y a la creciente demanda de transferencia de datos.

La ITU ha definido un canal de voz en la banda de 300hz a 3.4Khz, por cuestiones prácticas, y para evitar efectos de interferencia se maneja el canal desde los 0Hz hasta los 4Khz, dejando unos pocos Hz como bandas de guarda.

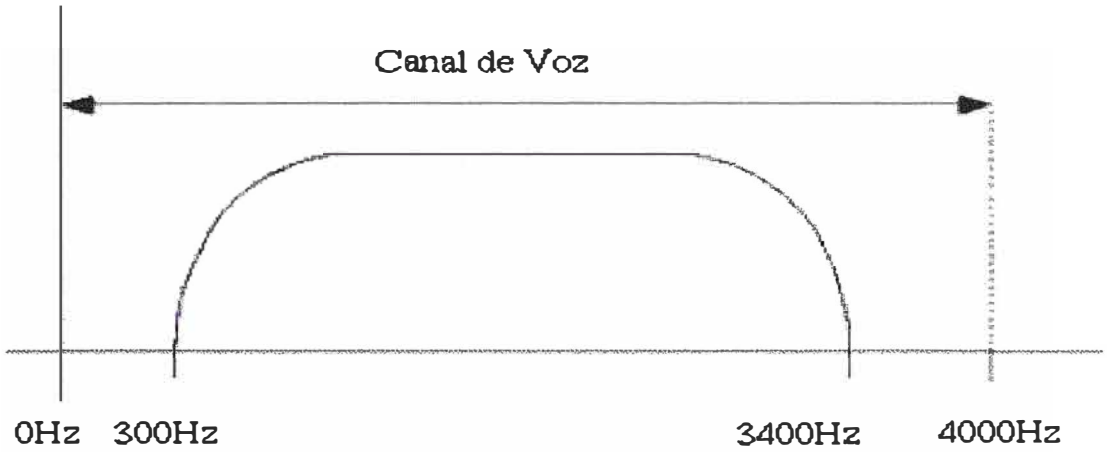

Fig.2.1 Rango de Frec. del canal de voz

Por tal motivo todos los equipos fueron diseñados para transmitir señales en este rango. Las investigaciones hechas en el campo de las comunicaciones han demostrado que transportar cualquier señal, incluso la voz, en formato digital tiene inmensas ventajas comparado con la transmisión análoga.

La teoría de Nyquist dice que para recuperar una señal análoga partiendo de ella misma pero digitalizada se tiene que muestrear al doble de la frecuencia máxima, es decir que para la voz humana la frecuencia de muestreo es 8khz.

$$fnyquist > 2fmax \qquad \text{Ecuación 2.1}$$

Considerando que usan conversores A/D - D/A de 8bits se necesita un canal de transporte de 64kbit/s de donde proviene la tasa básica de transmisión de voz, y que hoy ha sido prácticamente un limitante para las comunicaciones de datos sobre redes telefónicas, pensadas :inicialmente para voz.

En un enlace conmutado intervienen varios equipos desde el usuario inicial hasta el equipo destino. Dentro de los componentes de un enlace típico de datos sobre la red telefónica

publica, existe la necesidad de conversión A/D y D/A. Por tal motivo de todo este proceso electrónico es que limita a 56Kbits una comunicación análoga, que incluso puede llegar a 33Kbit/s cuando aparece una nueva conversión A/D y D/A al otro lado de la comunicación.

EL iniciador de una llamada y la central telefónica es análoga, y se lleva a cabo usando el mismo par de cobre de la línea telefónica, para esto se usa un modem análogo.

Mientras que en el lado remoto es digital, y para esto se usan enlaces RDSI PRI o BRI. Por lo general los equipos que intervienen en este lado son servidores de acceso remoto (RemoteAccess Server – RAS). Cuando este enlace es también análogo, se puede notar que en el proceso total de la conexión intervienen cuatro conversiones, dos A/D y dos D/A, esto hace que la tasa de transmisión y de recepción máximas sean apenas de 33Kbit/s.(Fig.2.2).

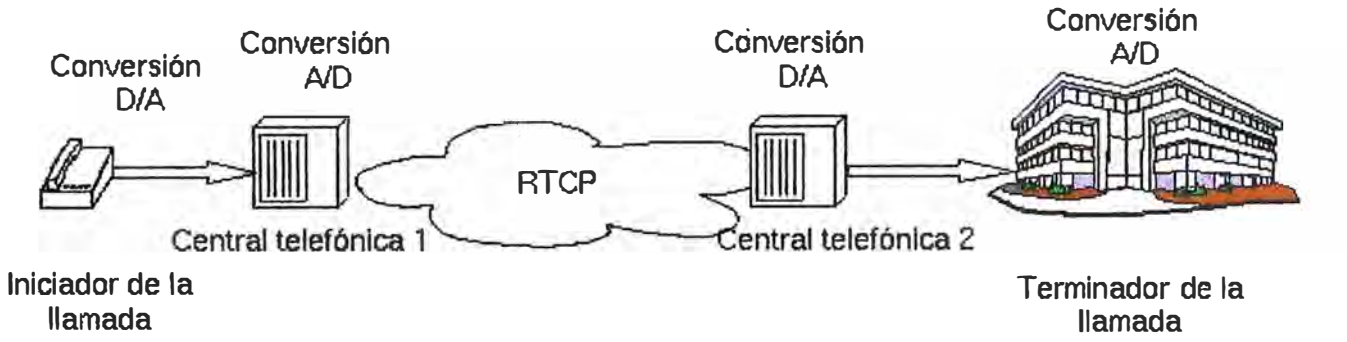

Fig.2.2 Procesos de conversión A/D Y D/A

b) Enlaces conmutados digitales – RDSI

Permite la transmisión de voz y data en forma digital, la transmisión se realiza a una velocidad de 64kbit/s a través de canales B (B del Bearer, RDSI la voz y data se transmiten a través de canales B). Los canales D(Canal para transmitir únicamente datos) se usan para señalización donde su transmisión va de 16kbit/s o 64kbit/s dependiendo del tipo servicio.

Tipos básicos de servicios RDSI:

- BRI(Basic Rate Interface).- Consiste en dos canales B de 64 Kbps y un canal D de 16 kbps para un total de 144 kbps orientada a usuarios residenciales.
- PRI (Primary Rate Interface).-Consiste en 30 canales B y 2 canales D, todos de 64 kbps para un total de 2048 kbps, orientada usuarios que requieran mayor ancho de banda.

A diferencia de las conexiones conmutadas análogas en una conexión RDSI la trayectoria es totalmente digital, desde la central hasta el abonado, no hay conversiones A/D o viceversa, lo cual facilita la obtención de velocidades de 64 kbps o 128 kbps, lo que se logra convirtiendo los dos canales B en un canal lógico de 128 kbps.

2.1.2. Enlaces dedicados

Son conexiones permanentes punto-punto o punto - multipunto, utilizando Infraestructura de transporte (Capa 1, enlaces clear chanel) o infraestructura transporte y conmutación (Capa1 y 2, enlaces Frame relay o ATM).

a) Clear channel

Permite comunicar los diferentes sitios de una empresa para formar Redes de Area Amplia (WANs) y para la interconexión de los diferentes puntos de un cliente. Estos circuitos están diseñados para transmitir señales de cualquier naturaleza a través de un mismo enlace dedicado, para crear redes privadas de Voz, Datos y Video.

El ancho de banda de "punto a punto" es de uso exclusivo para el cliente que lo contrato y puede transmitir cualquier tipo de información, además de que es un servicio de ancho de banda permanente y sin ningún proceso de conmutación de enlaces o de paquetes de datos, es decir se establece una conexión sin interferir con el protocolo de comunicación que desee utilizar el cliente.

Los enlaces Clear Channel ofrecen un tráfico efectivo casi del 100% ya que no usan ningún tipo de encapsulación de nivel 2, es decir no hay presentes cabeceras de ningún tipo.

Para el mercado corporativo comúnmente van desde los 64 kbps hasta los 2048 kbps, en pasos de nx64. Para el mercado de proveedores de servicio van desde E1hasta tasas de transmisión superiores.

Por lo general, las compañías (o clientes en general) deben tener un puerto disponible en el circuito terminal de datos que cumpla con especificaciones técnicas del equipo de

comunicaciones entregado por el proveedor. La mayoría de los equipos que se usan para recibir los enlaces Clear Channel por parte del cliente son enrutadores o switches de nivel 3. Y son estos, los que se encargan de manejar los niveles 2 y 3.
Los enlaces Clear Channel usan una topología robusta y estática a la vez lo que significa que para poder aumentar o disminuir la tasa de enlace es necesario cambiar de equipos o manipularlos localmente. Lo que para el cliente se transforma en indisponibilidades del servicio no deseables.
Remontando a la historia, la tecnología clear channel fue la primera tecnología WAN que se adopto usando infraestructura de voz PCM de los distintos operadores de telefonía locales, nacionales e internacionales. Como la tecnología no había sido pensada para transmitir datos fue superada rápidamente por otras tecnologías Frame Relay y ATM, actualmente muchas empresas usan aún clear channel.

b) Frame relay

Es una tecnología de conmutación rápida de tramas, basada en estándares internacionales, que puede utilizarse como un protocolo de transporte y como protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicación.
Frame relay surgió para satisfacer requisitos de comunicaciones de alta velocidad con otros ordenadores conectados a su misma red LAN, e incluso a redes LAN geográficamente dispersas, la demanda ahora es mayor en cuanto ahorro en costos de comunicaciones mediante integración de trafico de voz y datos, además de su transporte por una única red que responde a las siguientes necesidades:

- Alta velocidad y bajo retardo
- Soporte eficiente para tráficos a ráfagas
- Flexibilidad
- Eficiencia
- Buena relación coste-prestaciones
- Transporte integrado de distintos protocolos de voz y datos
- Conectividad "todos con todos"
- Simplicidad en la gestión
- Interfaces estándares

Frame Relay es una evolución de las redes X.25, como se observa en la Tabla N° 2.1 gran parte de las funciones de X.25 se eliminan en Frame relay, el direccionamiento pasa de la capa 3 en X.25 a la capa 2 en Frame Relay, el resto de funciones del nivel 3 de X.25 no se incorporan en Frame relay.

X.25		*Frame Relay*
Establecimiento de circuito Control de circuito Control de flujo de circuito Direccionamiento	Red	
Control de enlace Creación de tramas Control de errores Control de flujo de enlaces Fiabilidad	Enlace	Direccionamiento Creación de tramas Control de errores Gestión de interfaces
Conexión Física	Físico	Conexión Física

Tabla N° 2.1 Comparación X.25 y Frame Relay

La estandarización de esta tecnología se logro en el año 1990 cuando Cisco, Digital Equipment, Nortel Networks y StrataCom conformaron un forum y desarrollaron un conjunto de normas llamadas LMI(Local Management Interface) que fueron agregados a una propuesta inicial presentada a la CCITT(Comité Consultivo Internacional de Telefonía y Telegrafía), que junto con la organización americana ANSI publicaron un standar, que fue apoyado por la ITU-T.

Esto permitió que prácticamente todos los fabricantes de equipos de comunicaciones de datos desarrollaran dispositivos que soportaran Frame Relay.

1) Dispositivos Frame Relay

Los equipos que usa Frame Relay estan divididos en dos categorías:

- Equipos terminales de Datos (DTEs).- Generalmente considerados equipos

terminales de una red especifica y típicamente son enrutadores, computadores personales, terminales o bridges. Estos equipos se localizan en las premisas del cliente (mayormente son propiedad de los mismos).

- Equipos Terminales de Circuitos de Datos (DCEs).- Son propiedad del proveedor del servicio, el propósito es generar señales de reloj y conmutar los paquetes de la red. Por lo general, son los llamados conmutadores (packets switchs).

En la conexión entre los dispositivos DCE Y DTE intervienen dos componentes, uno de nivel físico y otro de nivel de enlace de datos. En el nivel físico se definen todas las características físicas, eléctricas y mecánicas entre los dos, y el nivel de enlace de datos define todas las especificaciones Frame Relay según sea el caso.

2) Circuitos Virtuales Frame Relay

La comunicación en frame relay se define entre un par de dispositivos y que cada una de las conexiones existentes en la red tiene un identificador asociado particular. Este servicio es implementado usando circuitos virtuales, que son conexiones lógicas creadas entre dos dispositivos DTE a través de la red conmutada de paquetes Frame Relay.
Un circuito lógico puede crearse a través de múltiples dispositivos intermediarios DCE dentro de la red Frame Relay.

Los circuitos virtuales Frame Relay se pueden dividir en dos categorías:

- **Circuitos Virtuales Conmutados (SVCs).-** Son conexiones temporales y que se usan en situaciones donde la transferencia de datos entre un par de dispositivos DTE es esporádica a través de la red Frame Relay.

- **Circuitos Virtuales Permanentes (PVCs).-** Son conexiones establecidas permanentemente que se usan donde la transferencia de datos es continua entre dos dispositivos DTE. Este tipo de conexiones no requieren hacer una llamada de configuración ni de terminación como en los SVCs.

Generalmente los PVCs siempre operan en uno de los siguientes estados:
- Data Transfer: Cuando los DTEs están intercambiando tráfico.
- Idle: Cuando no hay transferencia de datos, pero la conexión sigue activa.

3) Identificadores de conexión de enlace de datos (DLCI)

Los circuitos virtuales Frame Relay son identificados por los DLCIs, cuyos valores son asignados por el proveedor de servicio y tiene solo significado a nivel local, esto quiere decir que en una red Frame Relay pueden existir varios DLCIs con el mismo valor, pero no puede haber varios DTEs con un mismo DLCI conectados al mismo conmutado de paquetes (Packet Switch).

c) ATM (Modo de Transferencia Asíncrono)

Son redes orientadas a conexión, transmite múltiples servicios, tales como voz, video y datos mediante técnicas de conmutación de celdas pequeñas de tamaño fijo. Este estandar fue desarrollado por la Unión Internacional de Telelecomunicaciones (ITU-T).

1) Funcionamiento de las redes ATM y formato de celdas ATM

En el funcionamiento de ATM se combinan las ventajas de una red de conmutación de circuitos y de una red de conmutación de paquetes. Permitiendo transmisiones desde Mbps hasta Gbps.
La fig.2.3 muestra como una celda ATM esta conformada, contiene una celda 53 bytes, los 5 primeros para la cabecera y los restantes 48 bytes para la información del usuario, el tamaño pequeño de cada celda hace que las transmisiones de voz, video y data gocen de buena calidad, ya que estas celdas no tienen el problema en la transmisión de esperar grandes paquetes.

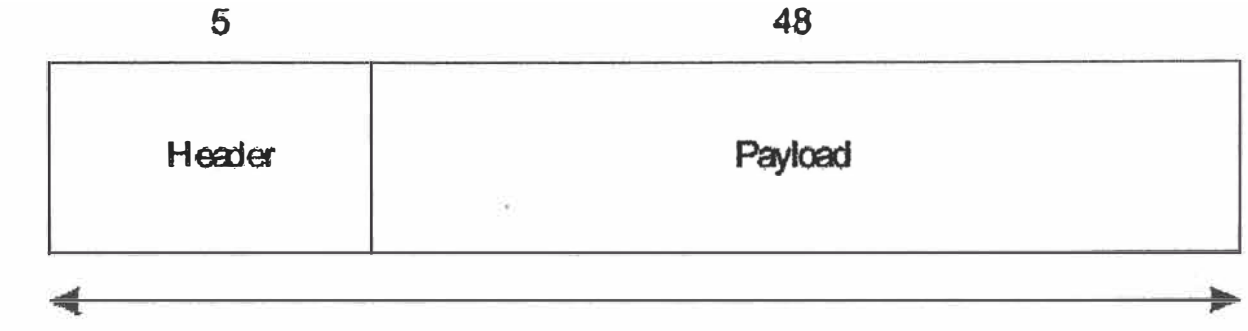

Fig.2.3 Formato de celda básico ATM

2) Equipos ATM

Los switches ATM y los terminadores ATM, son los equipos usados por esta tecnología:

- Switch ATM.- Recibe celdas de otro switch ATM, lee y actualiza las cabeceras de cada celda y luego las direcciona hasta llegar a su destino.
- Terminadores ATM.- Contienen un adaptador de interfaz de red ATM, se encuentran en los clientes.

En ATM se usa interfaces UNI(Interfaz de red de usuario) que interconecta un terminador y un switch ATM y la NNI(Interfaz de nodo de red) interconecta dos switches ATM.

3) Conexiones virtuales ATM

Debido a que ATM son redes orientadas a conexión, se configuran canales virtuales (VC) a través de la red para una adecuada transmisión de data.
Los tipos de conexiones que se tienen son: los caminos virtuales (VP:Virtual Path) identificados por VPIs (Virtual Path Identifiers), y los canales virtuales (VC:virtual channel), identificados con una combinación entre VPIs y VCIs(Virtual Channel Identifier).
Un camino virtual es la suma de varios canales virtuales.

4) Conmutación ATM

Una celda es recibida a través de un enlace por un switch ATM con un VCI o VPI, comprobando que puerto de salida tiene disponible para establecer el siguiente trafico, cambiando de VPI o VCI antes de enviar la celda la siguiente switch ATM.

2.2. Resumen

Previamente a la aparicion de las VPN, las organizaciones disponían de alternativas de realizar transmisión de información, pero siempre buscando la mayor confidencialidad.
Estas alternativas son los llamados enlaces privados compuestas por; enlaces conmutados análogos y digitales(RDSI) además de los enlaces dedicados(CLEAR CHANNEL, Frame relay, ATM). Los que presentan en común un alto costo por el uso e implementación, además de que algunos muestran ciertas limitaciones en cuanto a la transmisión y administración de información.

CAPITULO III
VENTAJAS DE IMPLEMENTACIÓN DE LAS REDES PRIVADAS VIRTUALES(VPN)

Las redes privadas virtuales son formas de compartir información y aplicaciones entre círculo de usuarios de una determinada organización, los cuales están en distintas localizaciones geográficas, gozando además de la apariencia y ventajas de los enlaces dedicados. El uso de técnicas de entunelamiento(tunneling) garantizan que los datos gocen de seguridad y confidencialidad al ser enrutados vía la red pública.

Las VPNs son multiprotocolo por que en el transporte pueden utilizar diferentes protocolos LAN(ip, ipx, apple talk, netbeui).

El éxito de las VPNs radica en realizar una adecuada elección de tecnología y escenario, acorde a la necesidad de la organización. Tecnología implica: técnicas de entunelamiento, autenticación, control de acceso y seguridad de los datos, mientras los escenarios donde se pueden implementar son Intranet VPN, Acceso remoto VPN y Extranet VPN(Vistos en Capitulo I).

3.1. Componentes tecnológicos críticos

Una buena solución VPN requiere de la buena combinación de componentes tecnológicos críticos:

3.1.1. Técnicas de entunelamiento

Consiste en encapsular los paquetes de datos que salen de una LAN o equipo de usuario remoto, esta encapsulación se realiza a nivel 2 y/o 3 de OSI, los componentes básicos de un túnel son:

- Un iniciador de túnel
- Uno ó varios dispositivos de entunelamiento

- Un conmutador de túneles (Opcional)
- Uno varios terminadores de túneles

3.1.2. Seguridad

Principalmente por el control de acceso, que garantiza la seguridad de las conexiones de la red, además de usar técnicas de cifrado, para garantizar la privacidad de datos y utilizar la autenticación para verificar acertadamente la identidad del usuario, manteniendo así la integridad de la información.

3.1.3. Control de tráfico

Garantiza solidez, calidad de servicio y buen desempeño. Cuando la conexión vía Internet proporcione una transmisión lenta, convertirá a este componente en una solución adecuada, por que utiliza parámetros como prioridad de datos y así garantizar el uso del ancho de banda.

3.1.4. Manejo empresarial

En situaciones que requieran integración de políticas de seguridad de empresas, por ejemplo para el caso de extranet VPN este componente es muy importante, debido a que el control tiene un manejo central desde un punto inicial hasta el final. Otra característica de este componente es permitir la escalabilidad en una organización.

3.2. Modelos de tunelamiento

Tunneling es una técnica que usa una infraestructura entre redes para transferir datos de una red a otra. Los datos o la carga pueden ser transferidas como tramas o protocolo. El protocolo de tunneling encapsula las tramas con una cabecera adicional, en vez de enviarla como lo produjo el nodo original. La cabecera adicional proporciona información de ruteamiento para que la carga pueda atravesar la red intermedia. Las tramas encapsuladas son enrutadas a través de un túnel que tiene como puntos finales los dos puntos entre la red intermedia. El túnel es un enlace lógico a través del cual se encapsulan paquetes viajando entre la red intermedia. Cuando una trama encapsulada llega a su destino en la red

intermedia, se desencapsula y se envía a su destino final dentro de la red. El proceso de entunelamiento incluye todo el proceso de encapsulado, desencapsulado y transmisión de tramas. Algunas tecnologías de entunelamiento son:

- DLSW – Data Link Switching (SNA over IP)
- IPX for Novell Netware over IP
- GRE – Generic Routing Encapsulation (rfc 1701/2)
- ATMP – Ascend Tunnel Management Protocol
- Mobile IP – For mobileusers
- IPSec – Internet Protocol Security Tunnel Mode
- PPTP – Point to Point Tunneling Protocol
- L2F – Layer 2 Forwarding
- L2TP – Layer 2 Tunneling Protocol

Los terminadores de los túneles son aquellos donde se toman decisiones de autenticación y las políticas de control de acceso, donde los servicios de seguridad son negociados y otorgados. En la práctica hay tres tipos posibles de servicios de seguridad que dependen de la ubicación de los terminadores. El primero es cuando el terminador esta en el mismo host, el segundo caso el terminador esta en el gateway VPN, el tercer caso es cuando el terminador esta localizado fuera de la red corporativa, es decir en un punto de presencia (POP) de la ISP. Un túnel VPN se compone de dos terminadores, con esto obtenemos seis tipos de modelos de entunelamiento, como se muestra en la Fig.3.1.

1.- Modelo End-to-End.- El túnel va de un extremo a otro, por lo que sus servicios de seguridad son negociados y obtenidos en la fuente y en el destino de la comunicación; lo que representa el mas alto nivel de seguridad dado que los datos siempre están seguros en todos los segmentos de la red, bien sea pública o privada. Sin embargo, el total de túneles que pueden haber en una organización, dificulta el manejo de los servicios de seguridad requeridos por dichos host, este modelo de seguridad es comúnmente implementado en capas superiores, como es el caso de SSL.

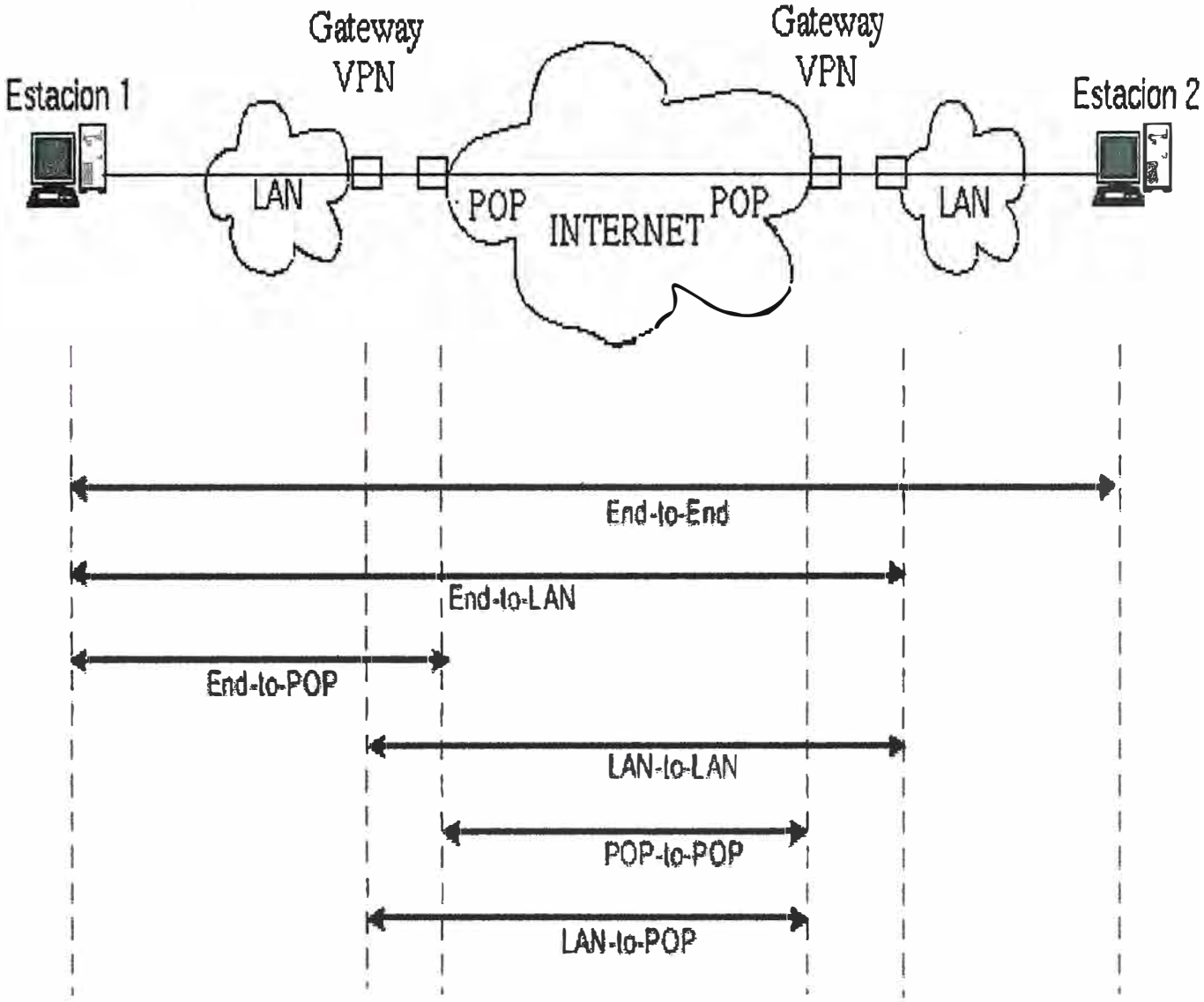

Fig.3.1 Servicios de seguridad

2.- Modelo End-to-LAN.- El túnel comienza en un host y termina en una LAN en la cual reside el host destino. Un dispositivo VPN localizado en el perímetro de la red es responsable de la negociación y obtención de los servicios de seguridad de los host remotos. De esta manera, la seguridad de un gran numero de dispositivos en una red corporativa puede ser manejada en un único punto, facilitando así la escalabilidad del mismo. Dado que la red corporativa es considerada un sitio seguro, comúnmente no hay necesidad de encriptar la información que transita dentro de ella. La mayoría de implementaciones de acceso VPN trabajan con este modelo.

3.- Modelo de End-to-POP.- Es aquel que va desde un host remoto y termina el túnel en un POP de la ISP. Un equipo VPN con funciones de terminador que se encuentra en la red de la ISP es el responsable de la negociación y concesión de los servicios de seguridad. La entrega de los datos desde el POP hasta el host destino es por lo general asegurada con infraestructura física, la cual separa del resto de la red pública. Por lo general en este caso el ISP administrar los permisos y controla el acceso según las directivas de los administradores de red de las empresas clientes. La arquitectura de acceso remoto VPN también usa este modelo.

4.- Modelo LAN-to-LAN.- Ambos host usan dispositivos VPNs situados en la frontera de la red corporativa para negociar y conceder servicios de seguridad. De esta manera, las funciones de seguridad no necesitan ser implementadas en los host finales donde los datos son generados y recibidos. Esta implementación de los servicios de seguridad es completamente transparente para los hosts. Esta implementación reduce drásticamente la complejidad en el manejo de las políticas de seguridad. La arquitectura Intranet VPN encaja en este modelo.

5.- Modelo LAN-to-POP.- El túnel comienza en un dispositivo VPN localizado a la frontera de la red corporativa y termina en un dispositivo VPN el cual se encuentra en un POP de la ISP. En la actualidad prácticamente este modelo de entunelamiento no es aplicado.

6.- Modelo POP-to-POP.- Ambos dispositivos VPN son localizados en la propia red de la ISP. Por lo tanto los servicios de seguridad son completamente transparentes para los usuarios finales del túnel. Este modelo permite a los proveedores de servicio implementar valores agregados a los clientes sin que estos alteren la infraestructura de sus redes.

3.3. Ventajas y desventajas de implementación

Las siguientes son las ventajas:

- Integridad, confidencialidad y seguridad de los datos.- Permitiendo unir las distintas redes que conforman a una organización, inclusive a redes de otras organizaciones gozando de la apariencia y seguridad de los enlaces privados, la información es transmitida completamente en forma confidencial usando técnicas de autenticación y cifrado.

- Reducción de costos.- El uso de las VPNs con el desarrollo de la internet se ha convertido en una alternativa bastante económica y segura, para la interconexión y la transmisión de información de una organización.
- Herramientas de diagnostico remoto.- La administración de las interconexiones depende solamente de la organización, lo que obliga a que la administración sea en forma remota.
- Control de acceso basado en políticas de la organización.- La creación de políticas de seguridad es adicionalmente dependiente la administración de la organización, incrementando de esta forma la seguridad de su información.
- Los algoritmos de compresión optimizan el tráfico del cliente.- El uso del ancho de banda propio de la organización se hace eficiente con técnicas de compresión de la información que es transmitida.
- La facilidad y seguridad para los usuarios remotos de conectarse las redes corporativas.- Los accesos remotos desde cualquier punto del globo son muy sencillos para usuarios pertenecientes a la organización, permitiendo de esta manera ingresar y hacer uso de los recursos de la red corporativa, manteniéndose seguro el enlace lógico de ataques durante toda la duración de la conexión remota.

Podemos considerar como desventaja de las VPN que primero deben establecerse correctamente las políticas de seguridad y de acceso por que si esto no esta bien definido pueden existir consecuencias de perdida de información, acceso de usuarios no autorizados y acceso a información restringida.

3.4. Mecanismos de seguridad en las VPNs

Para la implantación de las VPN previamente deben establecerse mecanismos de seguridad que nos van a garantizar que la información y el acceso a la red de la organización sea debidamente administrada y controlada.
Entre los mecanismos mas utilizados en VPN tenemos:

3.4.1. Autenticación

Integra dos entidades: un usuario que afirma su identidad y un autenticador que es quien realiza la verificación. El usuario o cliente entrega información que incluye identidad

programada e información que soporta dicha identidad al autenticador, en cuanto a la verificación aplica una función de autenticación comparando información recibida con el resultado de operaciones de dicha función. Si hay concordancia la identidad del usuario es considerada verificada.

La información enviada por el cliente puede ser desde una contraseña a un juego completo de parámetros y mensajes. La función puede solo comparar claves o aplicar algoritmos complejos.

Un factor importante en la integridad y confidencialidad de la información de autenticación, es que la información a ser usada para autenticación sea segura y no sea obtenida de participantes no autorizados. Estas medidas de seguridad no solo deben ser tomadas en el establecimiento del túnel, sino durante el transcurso del intercambio de datos. En el caso de las VPNs esto es muy importante ya que la información de autenticación es transmitida a través de Internet.

a) Pap

Protocolo de autenticación de contraseñas de dos vías, funciona cuando un host que se conecta envía un nombre de usuario y contraseña al sistema destino con el cual trata de establecer su comunicación, y el sistema destino(el autenticador) responde si es el caso, que el computador remoto esta autenticado y aprueba o no su comunicación. Puede ser usado al comienzo del establecimiento de un enlace PPP, o bien durante el transcurso de la sesión PPP para re-autenticar el enlace, PAP no es seguro por que la información es transmitida en texto plano.

b) Chap

Similar a PAP pero más seguro para autenticar enlaces PPP, es un protocolo de tres vías y puede ser usado al comienzo de un enlace PP y ser repetido cuando el enlace ya se haya establecido, los pasos para autenticar son los siguientes:

- EL autenticador envía un mensaje al nodo remoto.
- El nodo remoto calcula un valor usando una función HASH y lo envía de regreso al autenticador.
- El autenticador avala la conexión si la respuesta concuerda con el valor esperado.

Este proceso puede repetirse en cualquier momento del enlace PPP para asegurarse que la

conexión no ha sido tomada por otro nodo. A diferencia de PAP, en CHAP el servidor controla la re-autenticación.

c) Radius

Es una arquitectura cliente servidor, incluye dos componentes: un servidor de autenticación y un protocolo cliente. El servidor es instalado en un computador central, el protocolo cliente es implementado en el servidor de acceso a la red(RAS o NAS), siguiendo el siguiente proceso:

- Usuario marca a un RAS, luego de completarse la conexión al modem, el servidor de acceso pregunta por un usuario y contraseña.
- Recibido el requerimiento del RAS, este crea un paquete de datos llamado requerimiento de autenticación, incluyendo además del usuario y contraseña, el modem de conexión, entre otros datos. El RAS actúa como un cliente del RADIUS, cifrando el mensaje con una clave compartida predeterminada entre el RAS y el servidor RADIUS.
- El requerimiento de autenticación es enviado por la red desde el cliente hasta el servidor RADIUS. Esta comunicación puede ser hecha sobre una red de área local o global. Si el servidor RADIUS no puede ser alcanzado, el cliente RADIUS puede rutear el requerimiento a un servidor alternativo.
- Recibido el requerimiento de autenticación el servidor RADIUS valida el requerimiento y verifica la información del nombre de usuario y contraseña. Esta información también puede ser transmitida a un sistema de seguridad apropiado que soporte los archivos de autenticación, por lo general bases de datos.
- Si el nombre de usuario y el contraseña son correctos, el servidor envía un reconocimiento de autenticación que puede incluir información del usuario en la red y los servicios que el requiere.

Si hasta este punto el proceso de autenticación no ha tenido éxito, el servidor RADIUS envía un mensaje de desconexión al RAS y al usuario se le niega el acceso a la red.

3.4.2. Cifrado

Consiste en transformar un texto plano(inteligible por todos) mediante un mecanismo de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado. Se distinguen dos métodos generales de cifrado:

a) Cifrado simétrico

Cuando se emplean la misma clave en las operaciones de cifrado y descifrado, se dice que el sistema criptográfico es simétrico o de clave secreta. Estos sistemas son mucho mas rápidos que los de clave pública, y resultan apropiados para el cifrado de grandes volúmenes de datos.
Esta es la opción utilizada para cifrar el cuerpo del mensaje. Pare ello se emplean algoritmos como IDEA, RC5, DES, etc.

b) Cifrado asimétrico

Cuando se utilizan una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el sistema criptográfico es asimétrico o de clave publica. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la publica, es conocida por todos. De forma general, las claves publicas se utilizan para cifrar y las privadas para descifrar. El sistema posee la propiedad de que a partir del conocimiento de la clave publica no es posible determinar la clave privada ni descifrar el texto con ella cifrado. Los sistemas criptográficos de clave publica, aunque mas lentos que los simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión y firmas digitales, como se explicara posteriormente. Se utilizan los algoritmos de RSA, Diffie-Hellman, etc. En general, el cifrado asimétrico se emplea para cifrar las claves de sesión utilizadas para cifrar el documento, de modo que puedan ser transmitidas sin peligro a través de la red junto con el documento cifrado, para que en recepción éste pueda ser descifrado. La clave de sesión se cifra con la clave pública del destinatario del mensaje, que aparecerá normalmente en una libreta de claves públicas. El cifrado asimétrico se emplea también para firmar documentos y autenticar entidades.

c) Firma digital

En principio, basta con cifrar un documento con la clave privada para obtener una firma digital segura, puesto que nadie excepto el poseedor de la clave privada puede hacerlo. Posteriormente, cualquier persona podría descifrarlo con la clave pública, demostrándose así la identidad del firmante. En la práctica, debido a que los algoritmos de clave pública son muy ineficaces a la hora de cifrar documentos largos, los protocolos de firma digital se

implementan junto con funciones unidireccionales de resumen (hash), de manera que en vez de firmar un documento, se firma un resumen del mismo. Este mecanismo implica el cifrado del resumen de los datos mediante la clave privada del emisor, que serán transferidos junto con el mensaje. Éste se procesa una vez en el receptor, para verificar su integridad, los pasos del protocolo son:

1. A genera un resumen del documento.

2. A cifra el resumen con su clave privada, firmando por tanto el documento.

3. A envía el documento junto con el resumen firmado a B.

4. B genera un resumen del documento recibido de A, usando la misma función unidireccional de resumen. Después descifra con la clave pública de A el resumen firmado. Si el resumen firmado coincide con el resumen que él ha generado, la firma es válida.

De esta forma se ofrecen conjuntamente los servicios de no repudio, ya que nadie excepto A podría haber firmado el documento; y de autenticación, ya que si el documento viene firmado por A, podemos estar seguros de su identidad, dado que sólo él ha podido firmarlo. Además mediante la firma digital se garantiza asimismo la integridad del documento, ya que en caso de ser modificado, resultaría imposible hacerlo de forma tal que se generase la misma función de resumen que había sido firmada.

3.5. Control de acceso

El control de acceso constituye una poderosa herramienta para proteger la entrada a una red o un ordenador completamente o sólo a ciertos directorios e incluso a ficheros o programas individuales. Este control consta generalmente de dos pasos:

- La autenticación, que identifica al usuario o a la máquina que trata de acceder a los recursos, protegidos o no.
- Cesión de derechos o autorización, que dota al usuario de privilegios para poder efectuar ciertas operaciones con los datos protegidos, tales como leerlos, modificarlos, crearlos, etc.

Hoy en día, tecnológicamente han cambiado ciertas cosas, pero en el fondo persisten las razones y motivos para mantener mecanismos de control de acceso sobre áreas e información que se desea proteger. Los mecanismos de validación han sufrido

modificaciones: controles biométricos, magnéticos, visuales, etc.

Los mecanismos buscan identificar y autenticar a los usuarios, de tal manera que no exista la posibilidad que un usuario sea copiado o clonado. Estos mecanismos garantizan una relación costo / beneficio y menor cantidad de esfuerzo en su implantación y uso.
En la actualidad, cada computador que se adquiere en una tienda, por lo general ya viene equipado con alguna forma o mecanismo de control de acceso el cual es provisto por el sistema operativo. Partiendo de esta base, siempre existirá un esquema (framework) sugerido que mejore el nivel de seguridad que existe para un momento determinado, y que tiene un mínimo efecto sobre los costos y el esfuerzo de uso. En este sentido, los "servicios de seguridad" podrían incluir: integridad, confidencialidad, disponibilidad y control de acceso. En cuanto al control de acceso, tradicionalmente se considera que comprende los siguientes "mecanismos de seguridad":

- **Identificación de usuarios;** proceso por el cual se identifica a una persona, ejemplo: la cédula de identidad para el caso de un país, o el código de identificación (User ID) para el caso de un computador.
- **Autenticación de usuarios;** proceso que tiene por objeto la confirmación que la persona que se identificó es quien dice ser; ejemplo de este proceso es la utilización de palabras claves.
- **Autorización de usuarios;** proceso que determina quién tiene acceso a qué objetos, y qué tipo de acceso tiene.

Cada uno de estos mecanismos esta apoyado por una **"tecnología de seguridad"**, por ejemplo: palabras claves (contraseñas), los tokens inteligentes o de seguridad, certificados digitales, los dispositivos de reconocimiento de huellas digitales, palma de la mano, iris del ojo, etc. Estas tecnologías están presentes en una gran variedad de **productos de seguridad**.

Aun cuando los conceptos y cultura de seguridad en tecnología de información han venido evolucionando en las empresas, todavía existen gerentes de sistemas que se satisfacen en mantener un nivel de seguridad básico. Esto se evidencia cuando observamos que no se cuenta con políticas y estrategias definidas para evolucionar en elementos y mecanismos como: procesos de control de respaldos y recuperación, así como el control de acceso integral a las diferentes plataformas tecnológicas con las cuales cuenta la Compañía. Hoy en día, la mayoría de los sistemas operativos y sistemas de información incluyen funciones y procesos automáticos de control de acceso, como facilidad y como un aspecto de venta.

Es por esta razón que es importante examinar la efectividad de los mecanismos de control de acceso. El mejorar u optimizar el enfoque, administración y monitoreo del control de acceso, puede reducir el riesgo de accesos no autorizados. Por tanto, el mantener mecanismos de seguridad sobre la información y los datos, ayudan a crear un ámbito de confianza y permiten minimizar errores.

En la medida que se ha avanzado en los conceptos de seguridad, se puede observar que nos vemos obligado a profundizar en términos tecnológicos. Es así como nuevas condiciones deben ser identificadas para poder establecer los mejores mecanismos de seguridad y de control de acceso a la información. En tal sentido, podemos reconocer que existen, al menos, cuatro (4) mecanismos complementarios de un sistema de control de acceso: (a) identificación de usuario, (b) autenticación de usuario, (c) la verificación de la autenticación, y (d) re-autenticación.

El primer mecanismo de un sistema de control de acceso está diseñado para identificar a un usuario que se encuentra registrado en un determinado sistema. Esto se realiza mediante un "User ID".

El segundo mecanismo de un sistema de control de acceso consiste de la autenticación de un usuario, es decir, determinar que un usuario es quien dice ser. Esto se realiza por medio de "algo que se conoce", representado básicamente por: (a) una contraseña o clave de acceso (contraseña), (b) número de identificación personal (PIN), (c) entrada asociativa, en la que el sistema autentica al usuario mediante la secuencia de palabras o conceptos asociados que el sistema debe almacenar, y (d) respuesta desafiante, en la que el sistema proporciona una o una serie de preguntas que sólo el usuario identificado puede presumiblemente responder. Asimismo, este mecanismo se puede caracterizar por "algo que el usuario posee", como por ejemplo: (a) tarjetas inteligentes, (b) tarjetas de crédito o débito, (c) un token, (d) algún dato como la cédula de identidad o pasaporte, entre otros.

El tercer mecanismo de un sistema de control de acceso está diseñado debido a la debilidad inherente que tiene una contraseña o clave de acceso (contraseña). Su propósito u objetivo es el probar la autenticidad del usuario mediante la utilización de, por ejemplo, "algo que se es", pudiendo utilizar características inherentes al cuerpo del agente externo o usuario: (a) tono de voz, es decir, el reconocimiento de la voz, (b) las huellas dactilares, (c) patrones de la retina o iris del ojo, (d) el ADN, el reconocimiento de los surcos de los labios, (e) reconocimiento facial, entre otros. Este mecanismo se refiere a la verificación de autenticación.

El cuarto mecanismo de un sistema de control de acceso contempla los procesos que

aseguran que un usuario permanece autenticado, mediante la re-autenticación. Esto se puede llevar a cabo mediante procesos automáticos que se "despiertan" según la permanencia del usuario que está interactuando con un determinado sistema.

3.6. Resumen

La implementación de una VPN nos presenta ventajas, alcanzando el éxito de estas ventajas al realizar una adecuada elección de tecnología(Tecnicas de entunelamiento, autenticación, control de acceso y seguridad de los datos) y escenario de implementación(Intranet VPN, Acceso remoto VPN y Extranet VPN).

Garantizando que la información goce de seguridad y confidencialidad, además de lograr reducir los costos, disponer de herramientas de diagnostico remoto, controlar acceso, utilizar algoritmos de compresión y que los usuarios remotos tengan la facilidad y seguridad de conectarse a las redes corporativas

CAPITULO IV
TECNOLOGÍAS VPNs EXISTENTES MÁS USADAS PARA CREAR TÚNELES Y ENLACES

En el presente informe veremos las dos tecnologías más conocidas PPTP e Ipsec y que técnicamente presentan las mejores características de seguridad, rendimiento, facilidad y económica.
Desde el punto de vista OSI, se pueden crear VPNs desde la capa 2 (nivel de enlace de datos) como lo hace PPTP y desde la capa 3 (nivel de red) como lo hace Ipsec.

4.1. Pptp

EL Point-to-Point Tunneling Protocol del foro PPTP está destinado a la creación de redes privadas virtuales VPN. Las VPN pueden incluir o soportar otros protocolos de red como IPX o NetBEUI dentro del protocolo TCP/IP. También pueden formar conexiones permanentes o de acceso telefónico entre diversos sitios.

Para establecer una conexión permanente PPTP hay que utilizar el servicio Routing and Remote Access Service (RRAS). Las VPN se suelen utilizar en situaciones de acceso telefónico a redes en las que el usuario final establece de forma manual la red virtual para conectarse de forma temporal a una red remota.

Un empleado que se encuentre fuera de la oficina, por ejemplo, puede conectarse a Internet a través de su proveedor de Internet y, a continuación, utilizar una VPN para establecer una conexión segura con la oficina de su empresa. El protocolo PPTP permite utilizar enlaces de Internet económicos para crear conexiones seguras entre ordenadores. PPTP no es el único protocolo de red que puede utilizarse para crear redes virtuales privadas, aunque sin duda PPTP resulta fácil de adquirir y de utilizar. De hecho, los sistemas Windows 95, 98, NT, 2000 y 2003 incluyen PPTP. La ventaja del protocolo PPTP es que es ampliamente soportado por plataformas Windows, pudiendo un ordenador

Linux trabajar como servidor PPTP y los ordenadores Windows (95 en adelante) conectarse como clientes, o en el caso de Windows NT, 2000 y XP se daría el caso inverso, entonces se puede usar PPTP para crear redes privadas virtuales entre distintos sistemas operativos.

PPTP es un protocolo basado en PPP y GRE (Generic Routing Encapulation) que se usa para establecer túneles a nivel IP, permitiendo armar redes privadas virtuales (VPNs).

La gran desventaja de este protocolo reside en su diseño, que no es del todo seguro: antes que el túnel GRE se establezca, parte del inicio de sesión, autenticación y demás se hace por protocolo TCP en forma de texto plano, parte de la información que pasa de este modo es el IP del cliente y el servidor, el nombre de usuario, la contraseña cifrada. datos que cualquiera que esté en el medio puede llegar a usar para intentar entrar.

Además, la implementación de Microsoft agrega un poco mas de fallas a su implementación del protocolo; usando un sistema de clave simétrico para la autenticación: RC4 de 40 y 128 bits. La versión de 40 bits es demasiado débil para poder ser considerada segura, pero además de todo, la clave la basa en la contraseña del usuario (de esta manera el usuario puede tener múltiples sesiones con su propia clave). El problema de esto es que la clave debería cambiarse cada cierto tiempo(mas aún cuando las sesiones PPTP son prolongadas) y esto realmente no sucede casi nunca.

4.1.1. Distribución Standard del PPTP

En la práctica general hay normalmente tres ordenadores involucrados en una distribución:

- Un cliente PPTP
- Un servidor de acceso a la red
- Un server PPTP

NOTA: El servidor de acceso a la red es opcional, y no es necesario para la distribución PPTP. En la distribución normal algunas veces quizás, están presentes.

En una distribución típica de PPTP comienza por un PC remoto o portátil que será el cliente PPTP. Este cliente PPTP necesita acceso a la red privada (private network) utilizando un ISP (Internet service provider). Los clientes que usan Windows como S.O. usaran el Dial-up networking y el protocolo PPP para conectar a su ISP. Son también conocidos como Front-End Processors (FEP's) o Point-Of-Presence servers (POP's). Una

vez conectado, el cliente tiene la capacidad de extraer datos de Internet. Los "network access servers" usan el protocolo TCP/IP para el mantenimiento de todo el tráfico.
Después que el cliente ha hecho la conexión PPP inicial al ISP, la segunda llamada Dial-up es hecha a través de la conexión PPP ya establecida. Los datos enviados usando la segunda conexión son en forma de datagramas IP que contienen paquetes PPP. Es la segunda llamada la que crea la conexión VPN a un servidor PPTP en la red privada de la compañía. Esto es conocido como TUNEL.
El Tunneling es el proceso de intercambio de datos de un ordenador en una red privada de trabajo enrutándolos sobre otra red. Los otros enrutamientos de la otra red no pueden acceder porque esta en la red privada. Sin embargo, el tunneling activa el enrutamiento de la red para transmitir el paquete a un ordenador intermediario, como un servidor PPTP. Este servidor PPTP esta conectado a ambas, a la red privada de la compañía y a la red de enrutamiento, que en este caso es Internet. Ambos ,el cliente PPTP y el servidor PPTP usan el tunneling para transmitir paquetes de forma segura a un ordenador en la red privada.
Cuando el servidor PPTP recibe un paquete de la red de enrutamiento (Internet) lo envía a través de la red privada hasta el ordenador de destino. El servidor PPTP hace esto procesando el paquete PPTP para obtener el nombre del ordenador de la red privada o la información de la dirección que esta encapsulada en el paquete PPP.
El paquete PPP encapsulado puede contener datos multiprotocolo como TCP/IP,IPX/SPX o NetBEUI.
Debido a que el servidor PPTP esta configurado para comunicar a través de la red privada usando protocolos de esta red privada ,es capaz de entender Multi-Protocolos.

PPTP encapsula al paquete PPP encriptado y comprimido en datagramas IP para su transmisión a través de Internet. Estos datagramas IP son enrutados a través de Internet como un paquete PPP y después son desencriptados usando el protocolo de red de la red privada. Como mencionamos antes, los protocolos soportados por el PPTP, son TCP/IP, IPX/SPX y NetBEUI.

a) Pptp clients

Un ordenador que es capaz de usar el protocolo PPTP puede conectarse a un servidor PPTP de dos maneras diferentes:

- Usando un ISP que soporte las conexiones PPP

- Usando una red con soporte para TCP/IP para conectar a un servidor PPTP

Los clientes PPTP que quieran usar un ISP deben estar perfectamente configurados con un módem y un dispositivo VPN para hacer las conexiones al ISP y al servidor PPTP .La primera conexión es dial-up usando el protocolo PPP a través del módem a un ISP. La segunda conexión requiere la primera conexión porque el túnel entre el dispositivo VPN es establecido usando el módem y las conexiones PPP a Internet.

La excepción a estos dos procesos de conexión es usar PPTP para crear una VPN entre ordenadores físicamente conectados a una LAN. En este escenario, el cliente esta de hecho conectado a una red y solo usa dial-up networking con un dispositivo VPN para crear la conexión a un servidor PPTP en la LAN.

Los paquetes PPTP remotos de un cliente PPTP y una LAN local PPTP son procesados de manera diferente. Un paquete PPTP de un cliente remoto es puesto en el dispositivo de telecomunicación de medio físico, mientras que el paquete PPTP de la LAN PPTP es puesto en el adaptador de red de medio físico.

4.1.2. Arquitectura PPTP

La siguiente área expone la arquitectura del PPTP sobre Windows. La siguiente sección abarca:

- Protocolo PPTP
- Control de conexión PPTP
- Tunneling de datos PPTP

Vista por encima de la arquitectura:

La comunicación segura que es establecida usando PPTP involucra tres procesos, cada uno de los cuales requiere la realización completa del proceso anterior:

1) **Conexión y Comunicación PPTP:** Un cliente PPTP utiliza PPP para conectarse a un ISP usando una línea telefónica normal o una línea RDSI. Esta conexión usa el protocolo PPP para establecer la conexión y encriptar los paquetes de datos.

2) **Control de Conexión PPTP:** Usando la conexión a Internet establecida por el protocolo PPP, el PPTP crea una conexión controlada del cliente PPTP al servidor PPTP en Internet. Esta conexión usa TCP para establecer la comunicación y esta llamada PPTP Tunnel.

3) **Tunneling de datos PPTP:** El protocolo PPTP crea datagramas IP conteniendo paquetes PPP encriptados que son enviados a través del Tunnel PPTP al PPTP servidor. El servidor PPTP desensambla los datagramas IP y desencripta los paquetes PPP, y enruta los paquetes desencriptados a la red privada.

4.1.3. Ppp Protocol

No trataremos información profunda sobre el PPP. sino sobre el papel que juega el PPP en el medio PPTP. El PPP es un protocolo de acceso remoto usado por el PPTP para enviar datos a través de redes basadas en TCP/IP. El PPP encapsula paquetes IP, IPX y NetBEUI entre marcos PPP y envía los paquetes encapsulados creando un enlace punto a punto entre los ordenadores de origen y destino.
Muchas de las sesiones PPTP comienzan con la llamada de un cliente y un ISP. El protocolo PPP es usado para crear la conexión entre el cliente y el servidor de acceso a la red y presenta las siguientes funciones:

1) **Establece y termina la conexión física.** El protocolo PPP usa una secuencia definida en el RFC 1661 para establecer y mantener la conexión entre dos ordenadores remotos.
2) **Autentifica usuarios.** Los clientes PPTP son autentificados usando PPP. Texto en plano, encriptado o MS-CHAP pueden ser usados por el protocolo PPP.
3) **Crea datagramas PPP.** Que contienen paquetes IPX,NetBEUI o TCP/IP

4.1.4. Control de conexión PPTP

El protocolo PPTP especifica una serie de mensajes que son usados para la sesión de control. Estos mensajes son enviados entre el cliente PPTP y el servidor PPTP. Los mensajes de control establecen, mantienen y terminan el Túnel PPTP. La siguiente lista presenta el control primario de mensajes usados para establecer y mantener la sesión PPTP:

PPTP_START_SESSION_REQUEST Inicio de sesión
PPTP_START_SESSION_REPLY Respuesta al inicio de sesión
PPTP_ECHO_REQUEST Notificación de sesión de mantenida
PPTP_ECHO_REPLY Respuesta a la sesión de mantenimiento
PPTP WAN ERROR NOTIFY Notificación de errores de conexión

PPTP_SET_LINK_INFO Configuración de conexión PPTP Cliente/Servidor
PPTP_STOP_SESSION_REQUEST Sesión finalizada
PPTP_STOP_SESSION_REPLY Respuesta a la petición de termino de sesión

Los mensajes de control son enviados dentro de los paquetes de control en un datagrama TCP. Una conexión TCP es activada entre el cliente PPTP y el servidor. Este path es usado para enviar y recibir mensajes de control. El datagrama contiene una cabecera PPP y TCP, un mensaje de control PPTP y sus reglas. La construcción es como muestra la Tabla **N°** 4.1:

PPP Delivery Header
IP Header
PPTP Control Message
Trailers

Tabla **N°** 4.1 Datagrama contiene una cabecera PPP y TCP

4.1.5. Transmisión de datos PPTP

Después de que el Túnel PPTP ha sido creado, los datos del usuario son trasmitidos entre el cliente y el servidor PPTP. Los datos son enviados en datagramas IP conteniendo paquetes PPP. El datagrama IP es creado usando una versión modificada de la versión de Generic Routing Encapsulation (GRE) protocolo (RFC1701-2). La estructura de datagrama IP es como muestra la Tabla **N°** 4.2:

PPP Delivery Header
IP Header
GRE Header
PPP Header
IP Header
TCP Header
Data

Tabla **N°** 4.2 Datagramas IP conteniendo paquetes PPP

Prestando atención a la construcción del paquete, se puede ver como es capaz de ser transmitido a través de Internet interpretando las cabeceras. La cabecera de envío del PPP proporciona información necesaria para el datagrama para atravesar Internet. La cabecera GRE es usada para encapsular el paquete PPP sin el datagrama IP. El paquete PPP es creado por RAS. El paquete PPP es encriptado y si es interceptado, será ilegible.

4.1.6. Seguridad PPTP

El PPTP usa la autentificación y encriptación de seguridad disponible por los ordenadores que corren RAS bajo WindowsNT Server v4.0. El PPTP puede también proteger el servidor PPTP y la red privada ignorando todo excepto el trafico PPTP. A pesar de esta seguridad es fácil configurar un firewall para permitir al PPTP acceder a la red interna.

Autentificación:

La autentificación inicial en la llamada puede ser requerida por un ISP de servidor de acceso a la red. Un servidor PPTP es un gateway a la red, y necesita la base estándar de "login" de WindowsNT. Todos los clientes PPTP deben proporcionar un usuario y contraseña. De todas formas, el usuario o login de acceso remoto usando un PC bajo NT server o Workstation es tan seguro como hacer un login en un PC conectado a una LAN (teóricamente). La autentificación de los clientes remotos PPTP es hecha usando los mismos métodos de autentificación PPP usados para cualquier cliente RAS llamando directamente en un NT Server. Porque esto, soporta completamente MS-CHAP.

Control de acceso:

Después del logeo, todo el acceso a la LAN privada continúa usando las estructuras de seguridad basadas en NT. El acceso a recursos en dispositivos NTFS o otros recursos de la red requieren los permisos correctos, tal como si estuviese conectado dentro de la LAN.

Encriptación de los datos:

Para la encriptación de datos, el PPTP usa el proceso de encriptación RAS "shared secret". Referido a un "shared-secret" porque ambos terminan la conexión "sharing" the encryption

key. Bajo la implementación del RAS de MS, el secreto "shared" es la contraseña del usuario (Otros métodos incluyen llave pública de encriptación. El PPTP usa la encriptación PPP y los métodos de compresión PPP. El CCP (Compression Control Protocol) es usado para negociar la encriptación usada. El nombre de usuario y el contraseña esta disponible al servidor y es sustituida por el cliente. Una llave de encriptación es generada usando una mínima parte del contraseña situados en cliente y servidor. El RSA RC4 standard es usado para crear estos 40 bits (128 dentro de EEUU y Canada) de llave de sesión basada en la contraseña de un cliente. Esta llave es después usada para encriptar y desencriptar todos los datos intercambiados entre el servidor PPTP y el cliente. Los datos en los paquetes PPP son encriptados. El paquete PPP que contiene un bloque de datos encriptados es metido en un largo datagrama IP para el ruteo.

Filtrado de paquetes PPTP:

La seguridad de la red contra intrusos puede ser mejorada activando el filtro PPTP en el servidor PPTP. Cuando el filtro PPTP esta activado, el servidor PPTP en la red privada acepta y rutea solo paquetes PPTP. Esto previene de todos los tipos de paquetes de la red entera. El tráfico PPTP usa el puerto 1723 como predeterminado.

4.2. IPsec

IPSec trata de remediar algunos problemas que el IP presenta, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

4.2.1. Modos de funcionamiento de Ipsec

El modo de transporte es diseñado para proteger los protocolos de capas superiores tales como TCP y UDP. En modo túnel, el paquete IP original se convierte en la carga útil de un nuevo paquete IP.

Lo que permite al paquete IP inicial "ocultar" su cabecera IP para que sea encriptada, considerando que el paquete externo sirve de guía a los datos a través de la red.

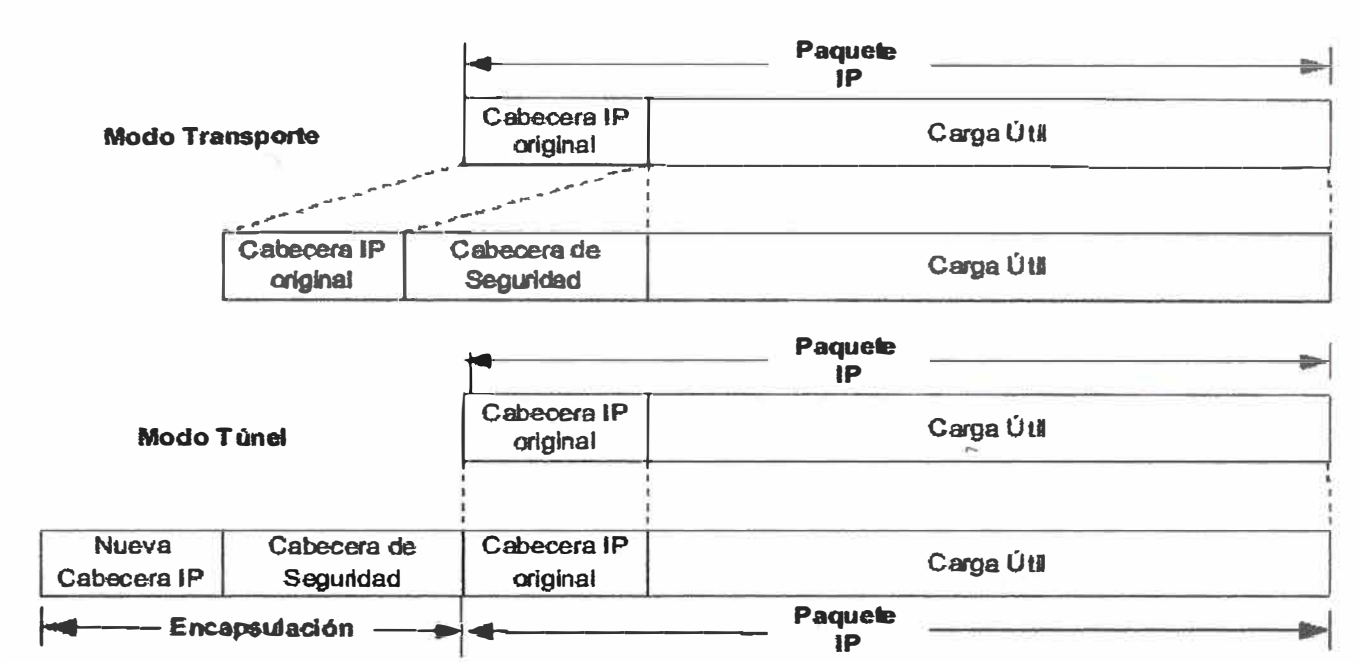

Fig.4.1 Modos de funcionamiento IPsec

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

- Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.

- Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

- Por autenticidad se entiende por la validación del remitente de los datos.

- Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino. ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header. AH sigue al header IP y contiene características criptográficas tanto en los datos como en la información de identificación. Las características criptográficas

pueden también cubrir las partes invariantes del header IP.

El header de ESP permite reescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.

Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway:

- El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.
- El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

Los enlaces seguros de IPSec son definidos en función de Security Associations (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varios SA, cada uno de los cuales aplica cierta transformación. Grupos de SA son denominados SA Bundles. Paquetes entrantes pueden ser asignados a un SA específico por los tres campos definitorios: la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad. El SPI puede ser considerado una cookie que es repartido por el receptor del SA cuando los parámetros de la conexión son negociados. El protocolo de seguridad debe ser AH o ESP. Como la dirección IP de destino es parte de la tripleta antes mencionada, se garantiza que este valor sea único.

Un ejemplo de paquete AH en modo túnel se muestra en la Fig.4.2:

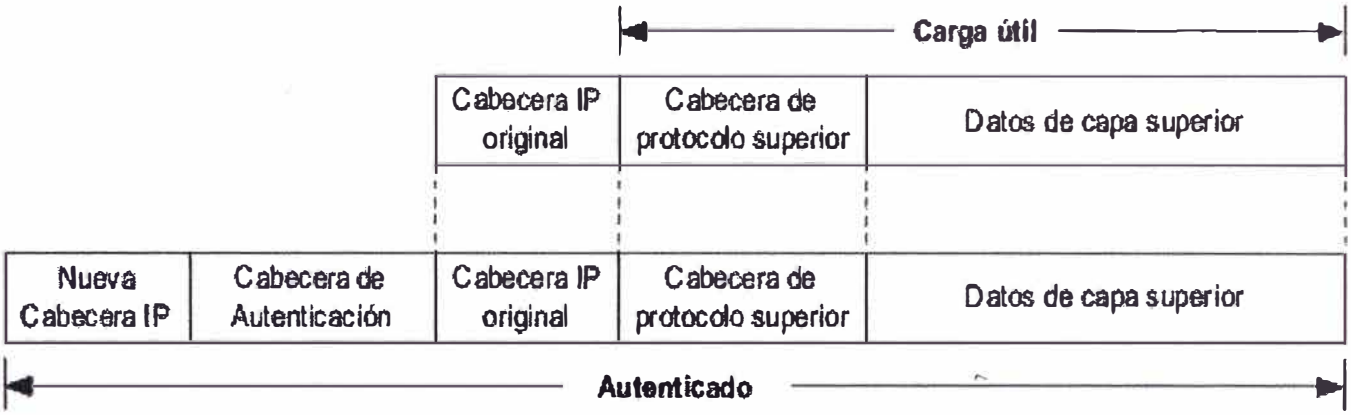

Fig.4.2 Paquete AH en modo túnel

Un ejemplo de paquete AH en modo transporte se muestra en la Fig.4.3:

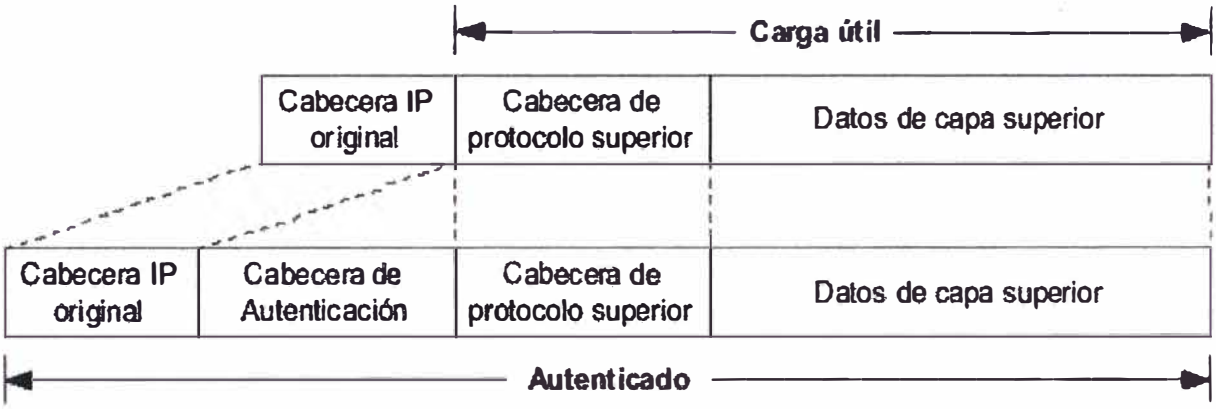

Fig.4.3 Paquete AH en modo transporte

4.3. Resumen

Las tecnologías VPN de entunelamiento PPTP e IPsec presentan mejores características de seguridad, rendimiento, facilidad y económicas.

Los modos en los cuales un protocolo de seguridad puede operar son: transporte y túnel.

La diferencia radica en la manera como cada uno de ellos altera el paquete IP original.

Mas detalles de las tecnologías de entunelamiento se detallan este capitulo.

CAPITULO V
IMPLEMENTACIONES VPN

5.1. Acceso remoto utilizando PPTP

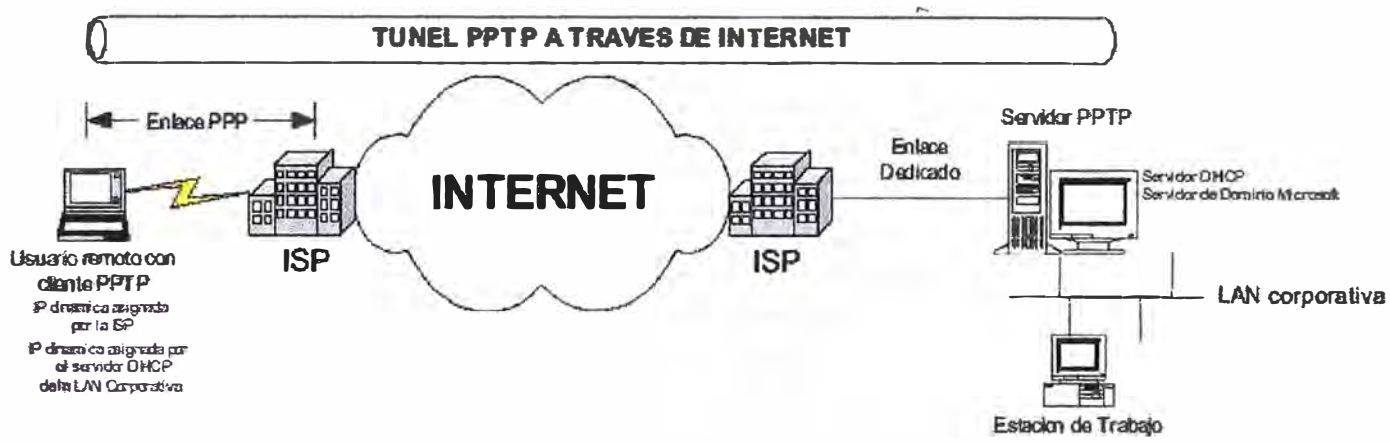

Fig.5.1 Acceso remoto PPTP

5.1.1. Instalación y configuración de servidor PPTP

En la fig.5.1 tenemos un servidor con conexión a internet vía enlace dedicado y el cliente tiene un enlace PPP, el servidor tiene como sistema operativo Windows2000 instalado como servidor de dominio. El objetivo es realizar el túnel en windows 2000 mediante servidor de acceso y ruteo (RRAS) que esta instalado por defecto.

Ingresamos al entorno de configuración mediante **inicio / programas / herramientas administrativas / acceso remoto y ruteo**, luego click derecho en el nombre del servidor elegimos la opción **configuración y habilitación de ruteo y acceso remoto (Fig. 5.2)**

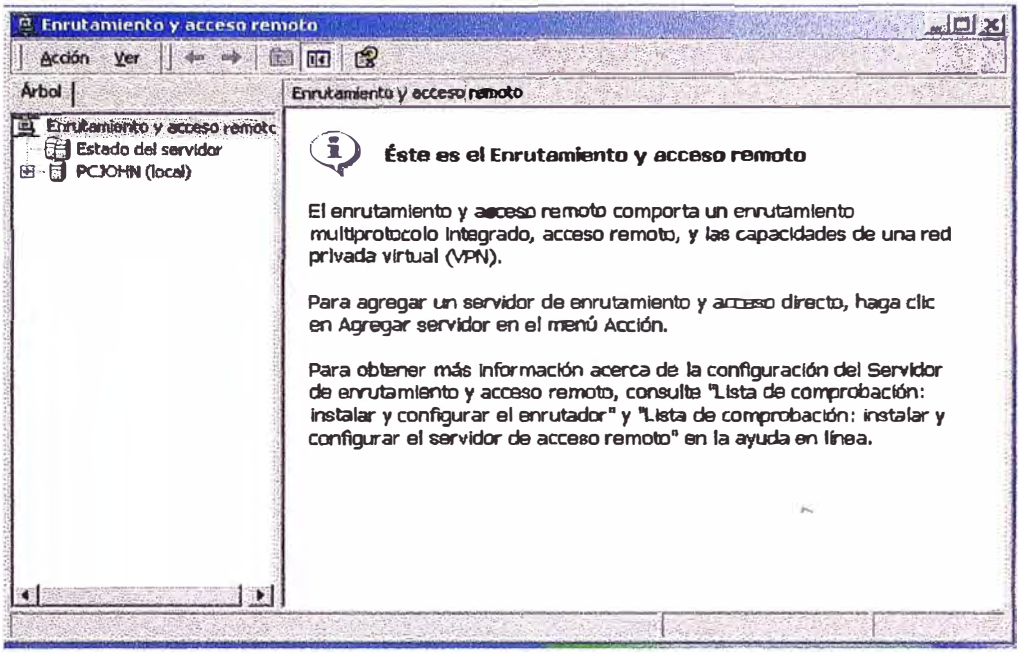

Fig.5.2 Configuración y Habilitación de ruteo

A continuación aparece el **asistente para instalación del servidor de enrutamiento y acceso remoto** click en siguiente para continuar Fig.5.3

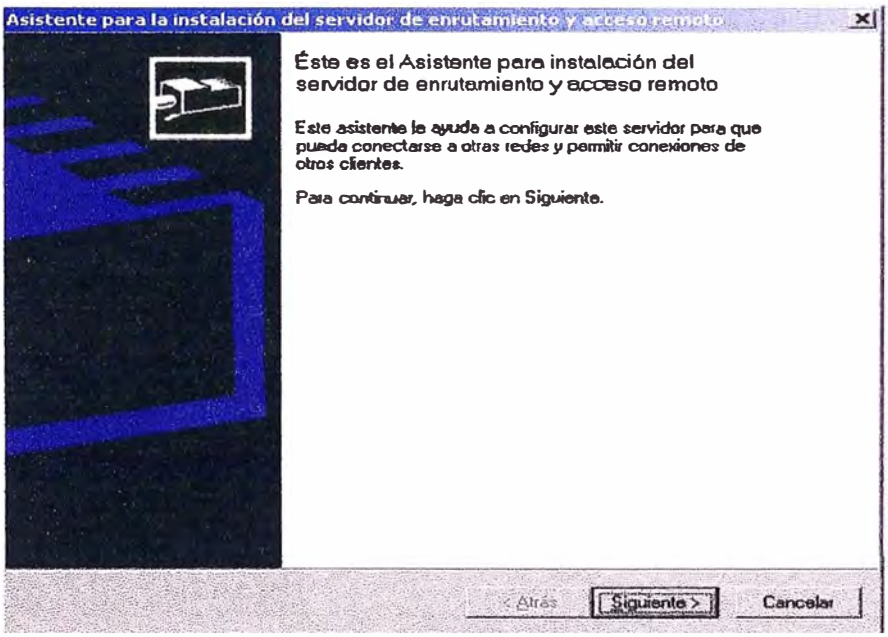

Fig.5.3 Instalación del servidor de enrutamiento

Ahora aparece la siguiente ventana, para un mejor entendimiento elegimos **servidor configurado manualmente** y siguiente Fig.5.4

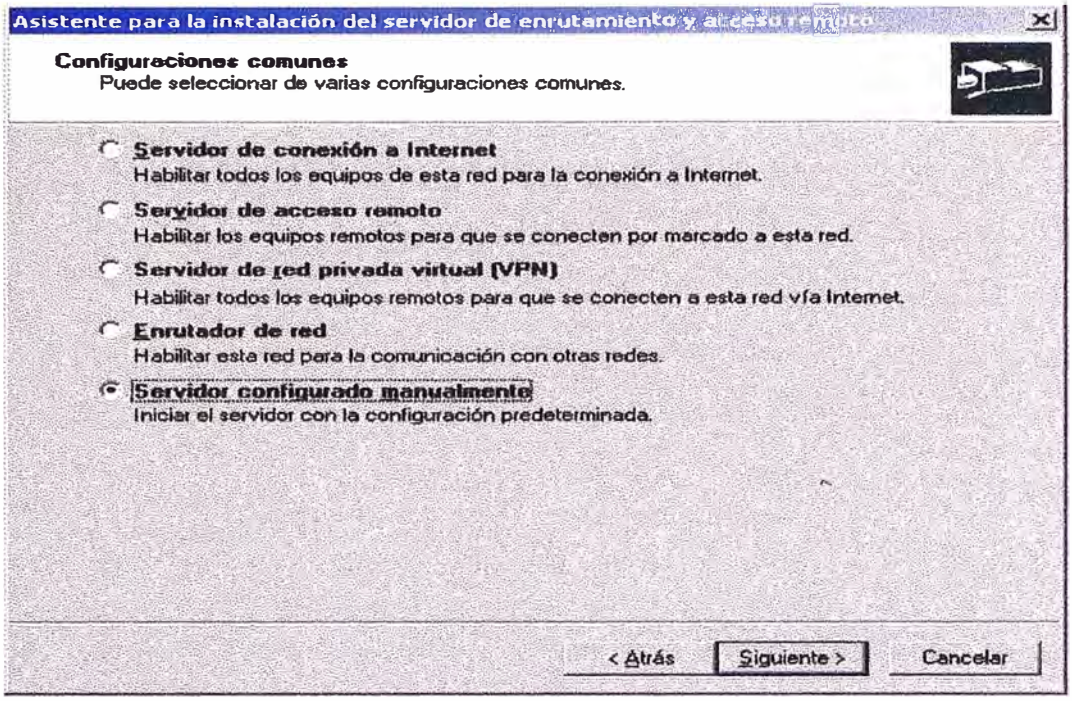

Fig.5.4 Selección de servidor configurado manualmente

Terminamos con el asistente con click en finalizar Fig. 5.5

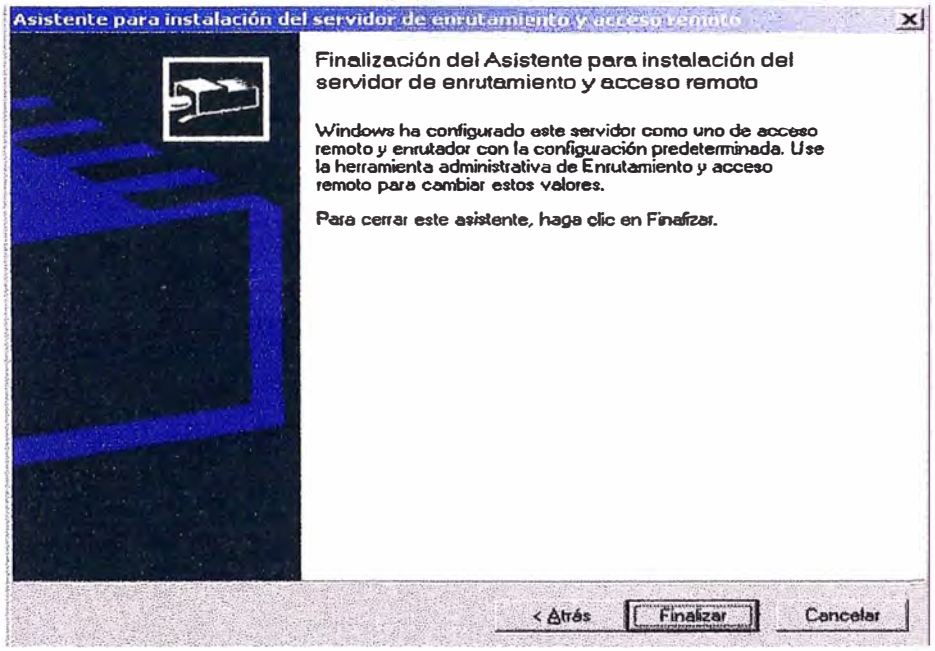

Fig.5.5 Asistente del servidor de enrutamiento y acceso remoto

Iniciamos la configuración del servidor PPTP son necesarias configurar algunas opciones generales del RRAS, en la ventana similar a la Fig.10 seleccionamos el servidor PCJOHN

click derecho y elegimos propiedades, click en la pestaña IP verificamos **Habilitar enrutamiento IP** y **Permitir conexiones de marcado a petición y acceso remoto basado en IP(Fig.5.6).**

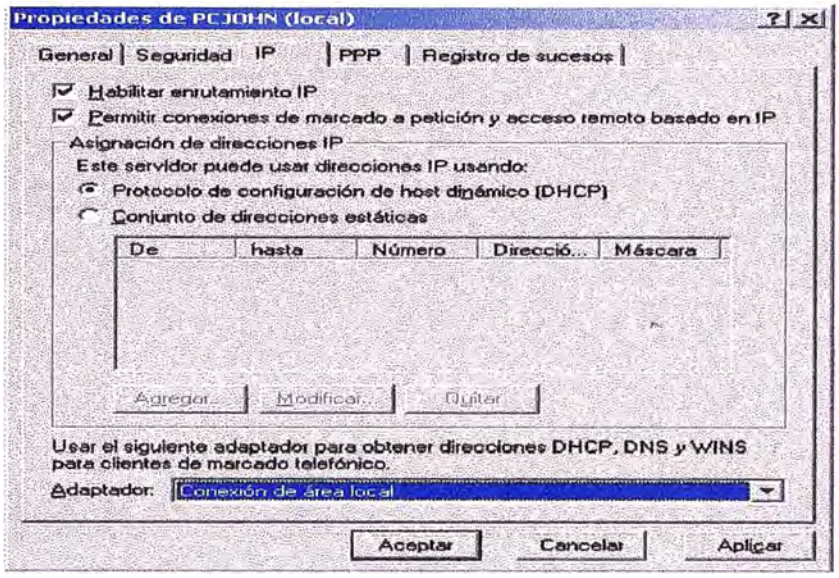

Fig.5.6 Habilitación de enrutamiento IP

RRAS asigna IP a los clientes remotos(Dial-up y VPN) de forma estática o mediante un servidor DHCP, por eso se selecciono la opción **conexión de área local** en adaptador en el paso anterior, en la pestaña **registro de sucesos** y seleccionamos Registrar la máxima cantidad de información(Fig.5.7).

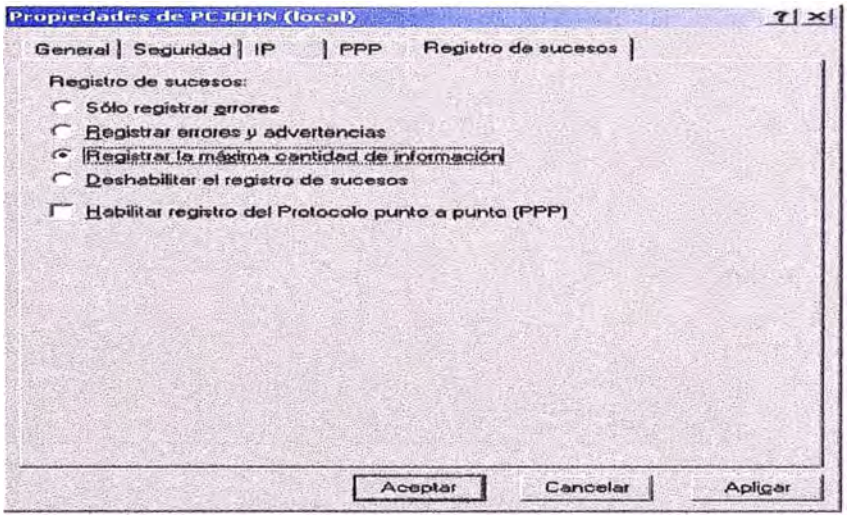

Fig.5.7 Registro de sucesos de max. cantidad de información

Luego se configura los puertos PPTP. Seleccionar la opción **puertos,** en la ventana derecha se mostrara todos los puertos instalados con el RRAS, luego click derecho en

puertos y propiedades (Fig.5.8).

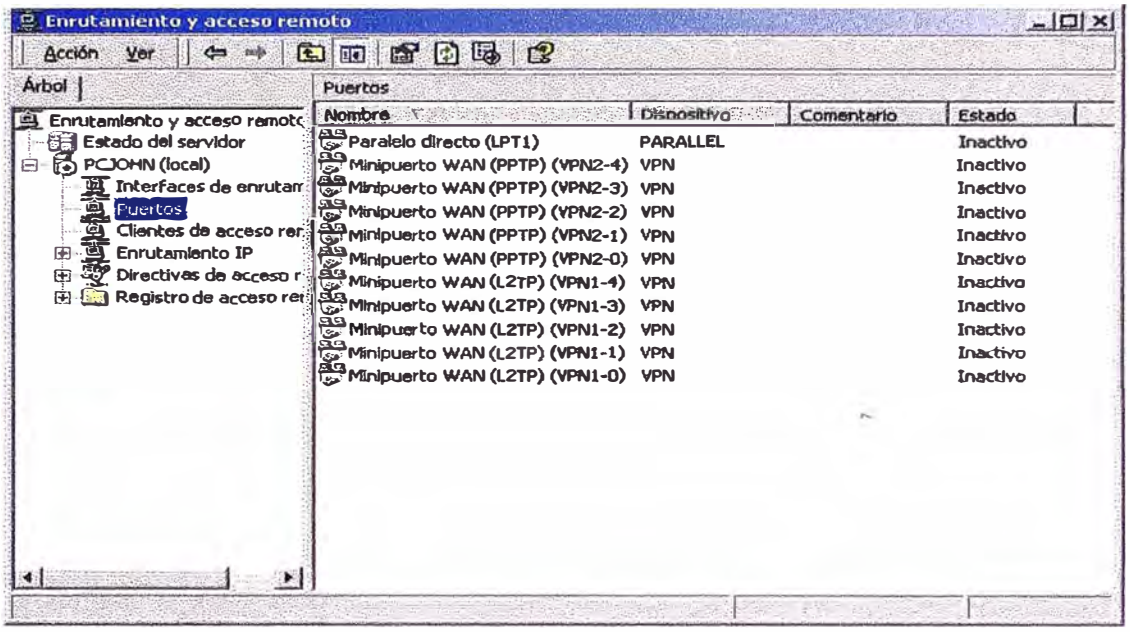

Fig.5.8 Puertos instalados con el RRAS

Configuración de puertos PPTP, seleccionar **Minipuerto WAN(PPTP)**, ver Fig.5.9:

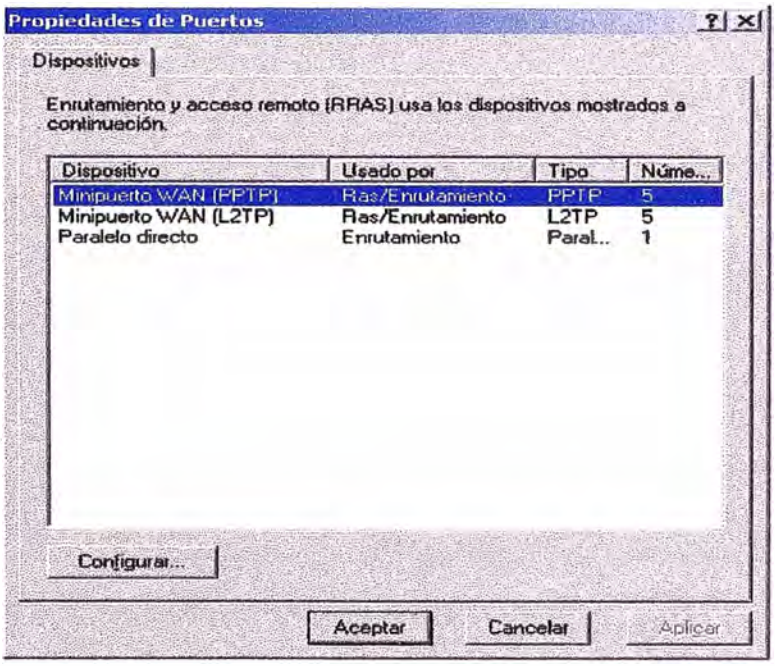

Fig.5.9 Selección de puerto WAN(PPTP)

Habilitar las siguientes opciones mostradas y luego aceptar(Fig.5.10).

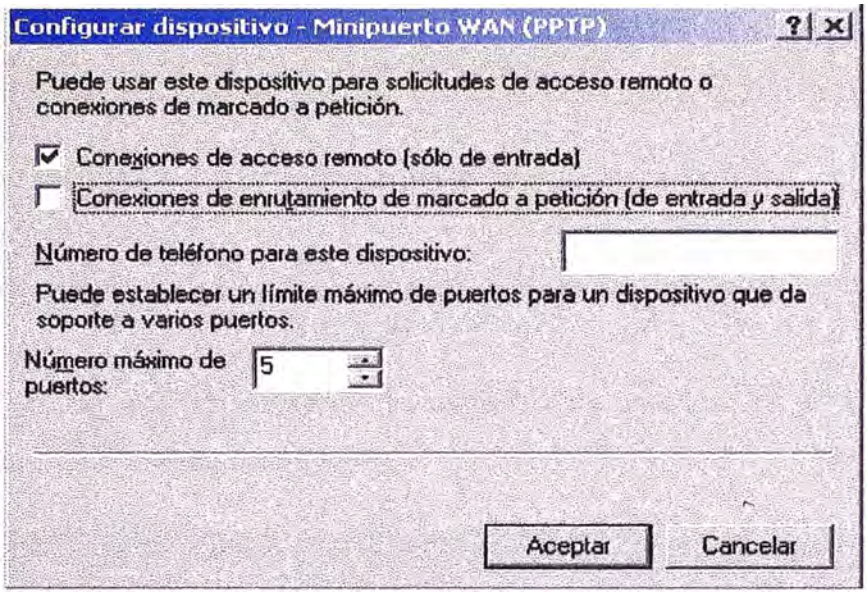

Fig.5.10 Opciones de conexión de acceso remoto

Los puertos L2TP los deshabilitamos eligiendo **Minipuerto WAN (L2TP)**siguiendo el mismo proceso, en el numero max. de puertos ponemos 0 y aceptar(Fig.5.11)

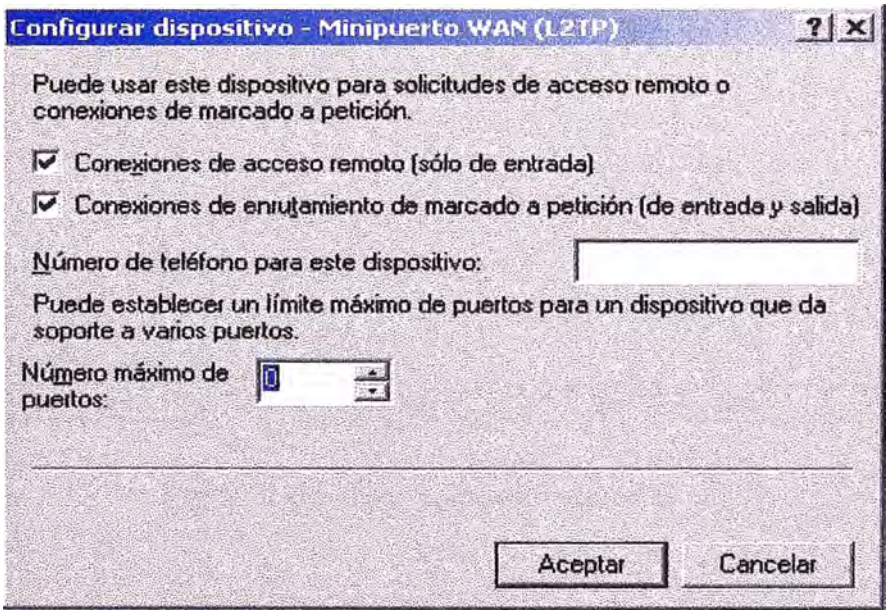

Fig.5.11 Configuración de minipuerto WAN(L2TP)

A continuación se mostrara el siguiente mensaje de advertencia, anunciando que se desconectaran los puertos existentes para poder configurar, responder si(Fig.5.12):

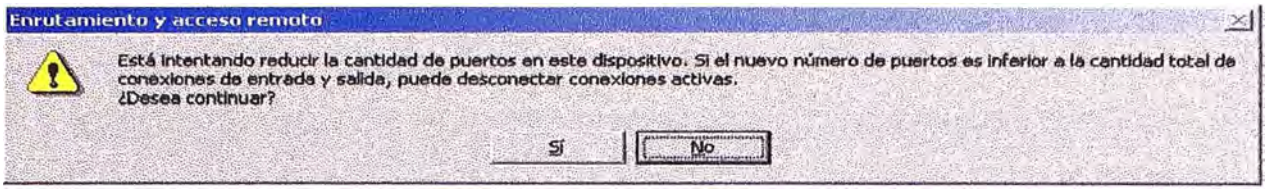

Fig.5.12 Alerta de enrutamiento y acceso remoto

Retornando el dialogo de propiedades de puertos, seleccionar aceptar.

En la ventana de del RRAS mostrara la cantidad de puertos PPTP y L2TP que se configuraron (el L2TP esta en cero) como en la Fig.5.13:

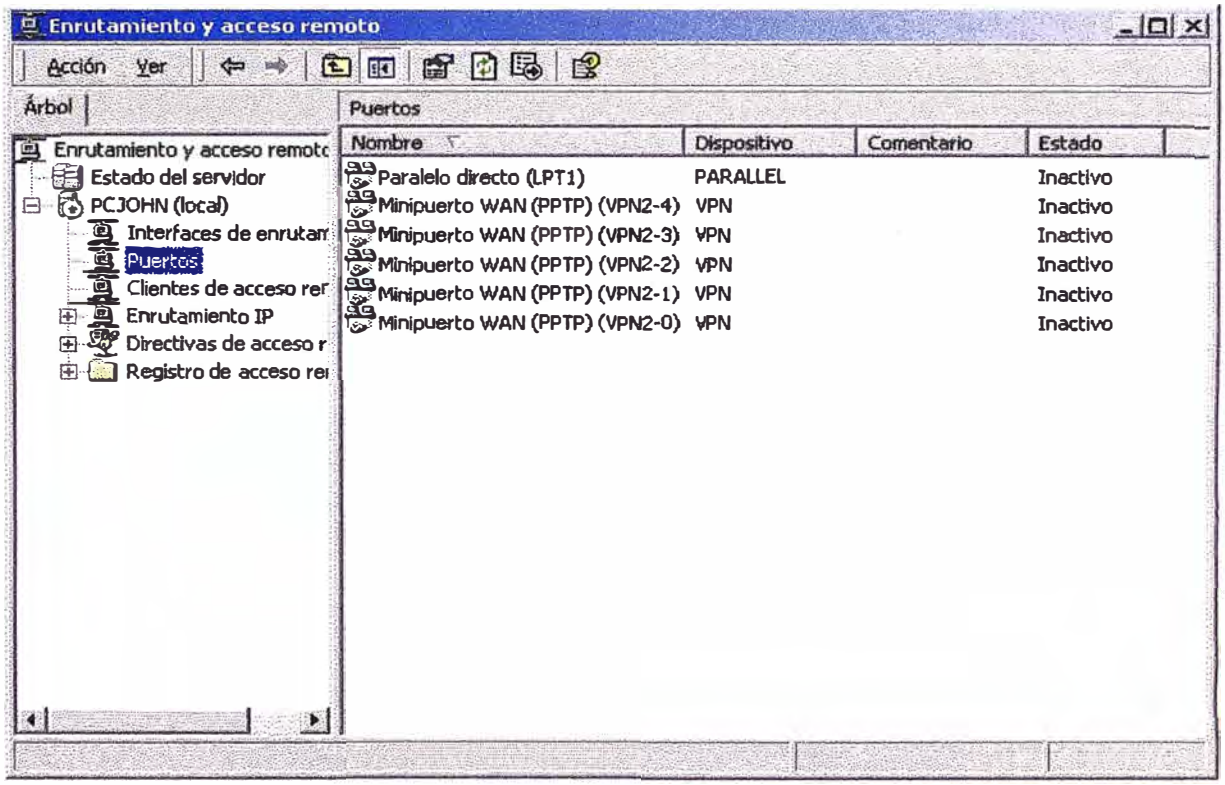

Fig.5.13 Configuraciones realizadas

Acontinuación en los **registros de acceso remoto,** en la parte derecha click derecho en **archivo local y propiedades(Fig.5.14):**

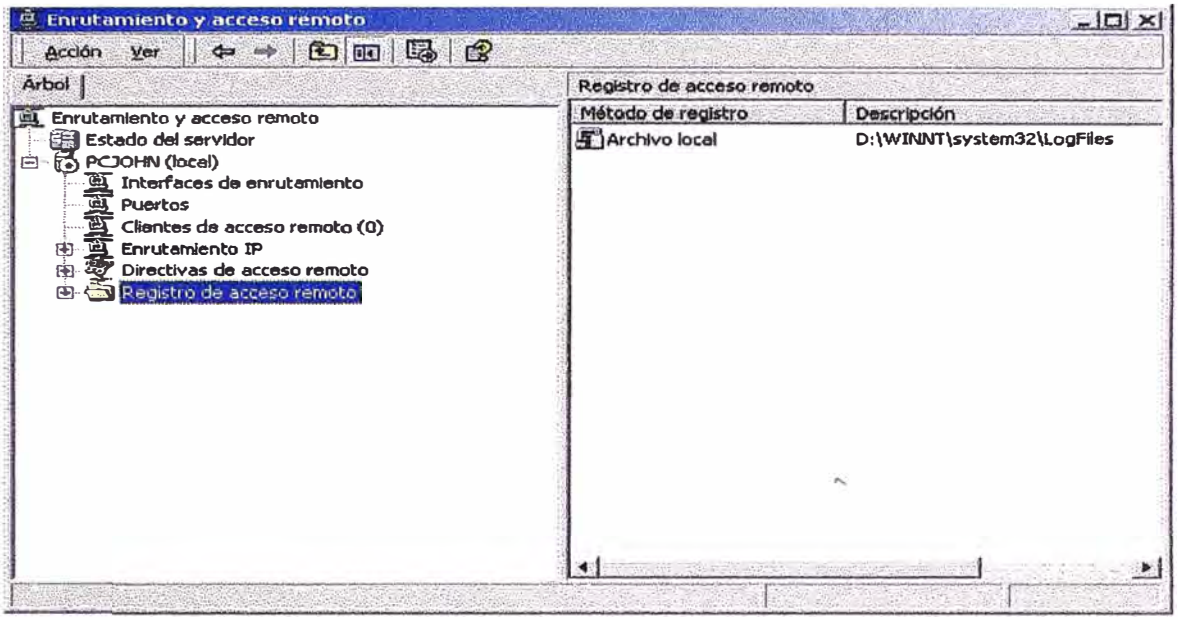

Fig.5.14 Propiedades de archivo local

Luego mostrara un cuadro titulado **propiedades de archivo local,** verificamos que este habilitada la opción, **solicitudes de autenticación de registro** y luego aceptar(Fig.5.15).

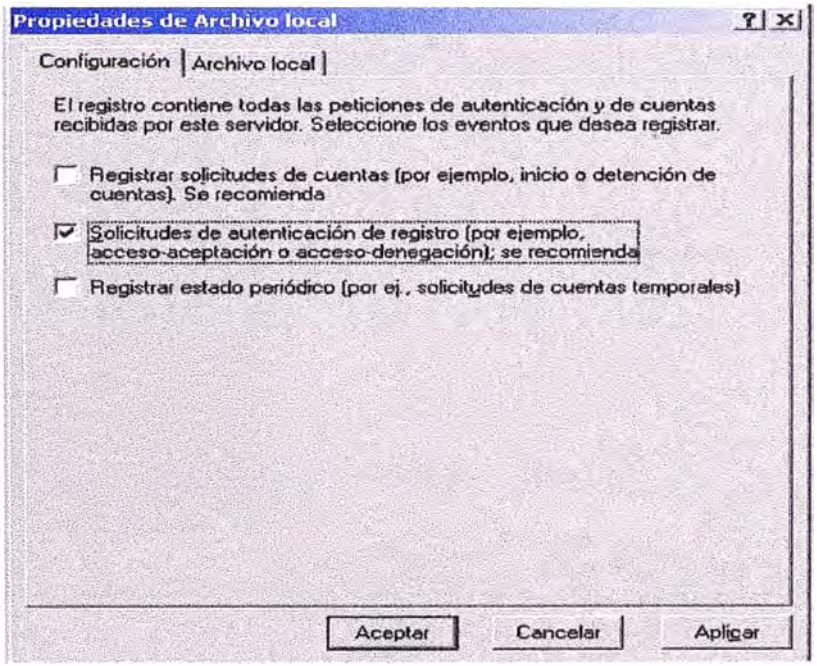

Fig.5.15 Propiedades de archivo local

5.1.2. Instalación y configuración del cliente PPTP

El cliente que tendremos tiene Windows XP como S.O. a continuación veremos los pasos para instalar y configurar un cliente PPTP remoto.

Hacemos click derecho en **equipos de red / propiedades,** luego en la parte superior ir a **archivo / nueva conexión (Fig.5.16)**

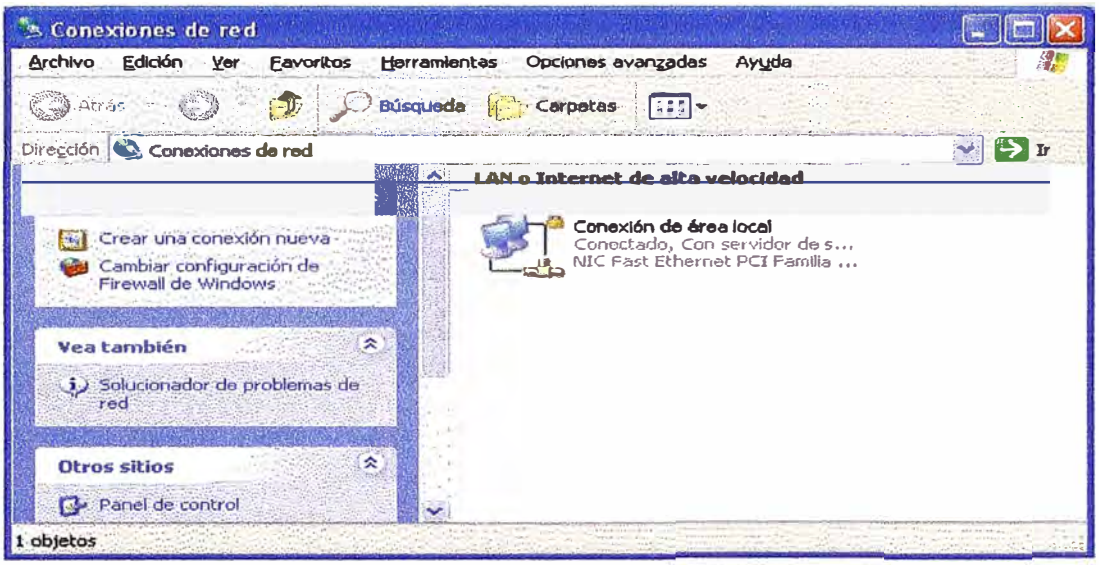

Fig.5.16 Realizar nueva conexión

Tendremos ahora un cuadro de dialogo para iniciar el asistente que crea la nueva conexión de tipo VPN(Fig.5.17):

Fig.5.17 Asistente a nueva conexión

Seguidamente click en siguiente(Fig.5.18), se despliega otra ventana donde se escoge el tipo de conexión nueva que se requiere crear, seleccionar **Conectarse a la red de mi lugar de trabajo** (que hace alusión a una red privada).

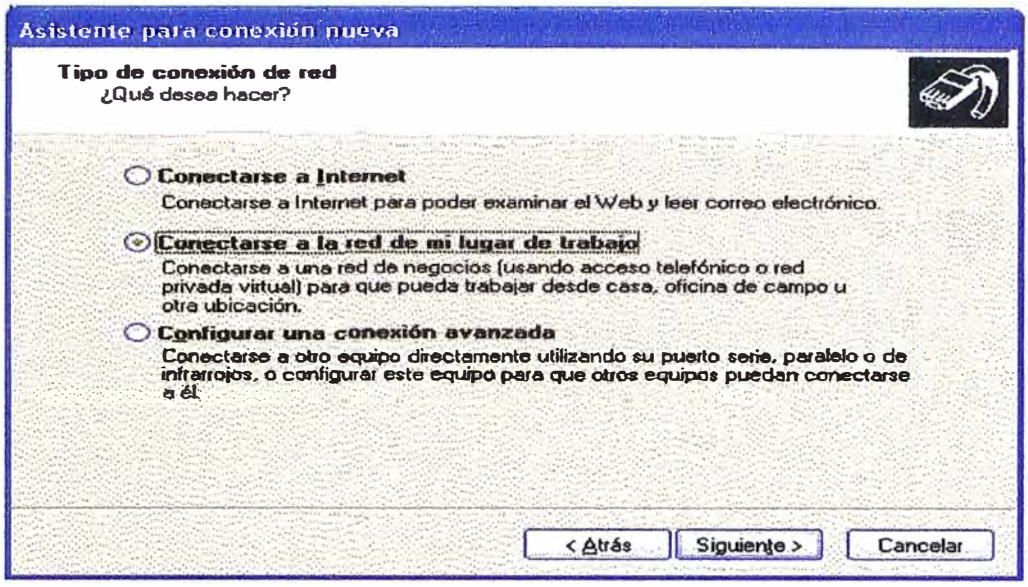

Fig.5.18Conectarse a la red mi lugar de trabajo

Dar click en siguiente(Fig.5.19) y mostrara otra ventana donde seleccionar **Conexión de red privada virtual**, y dar click en **siguiente**:

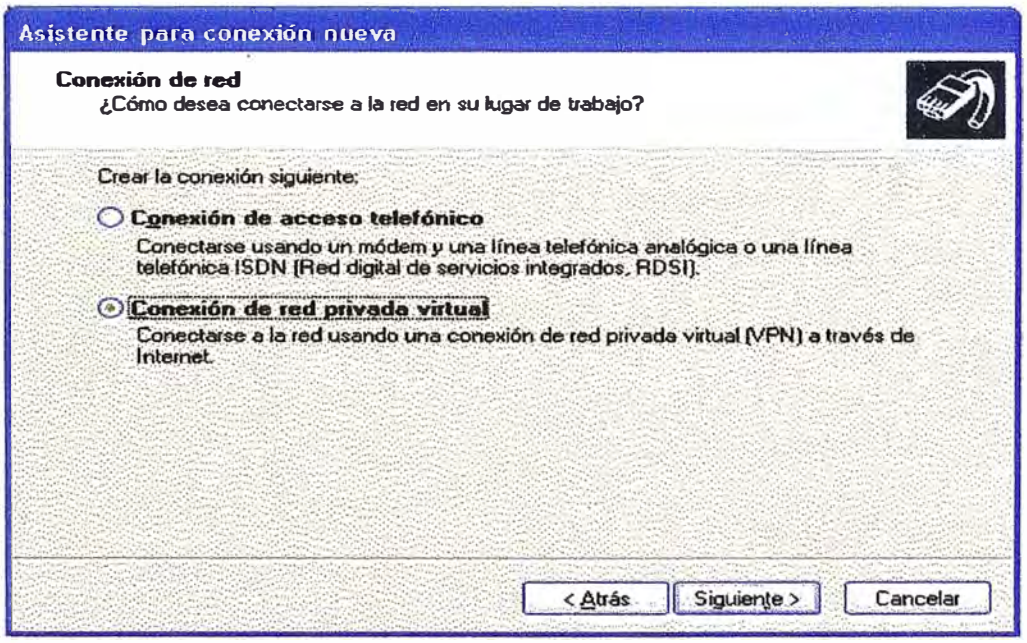

Fig.5.19 Conexión a red privada virtual

Aparece una nueva ventana donde se escribe el nombre que identifique la compañía remota a la que se desea acceder por medio la VPN en nuestro caso usamos red-mahy como nombre de una compañía ficticia, y click en siguiente(Fig.5.20):

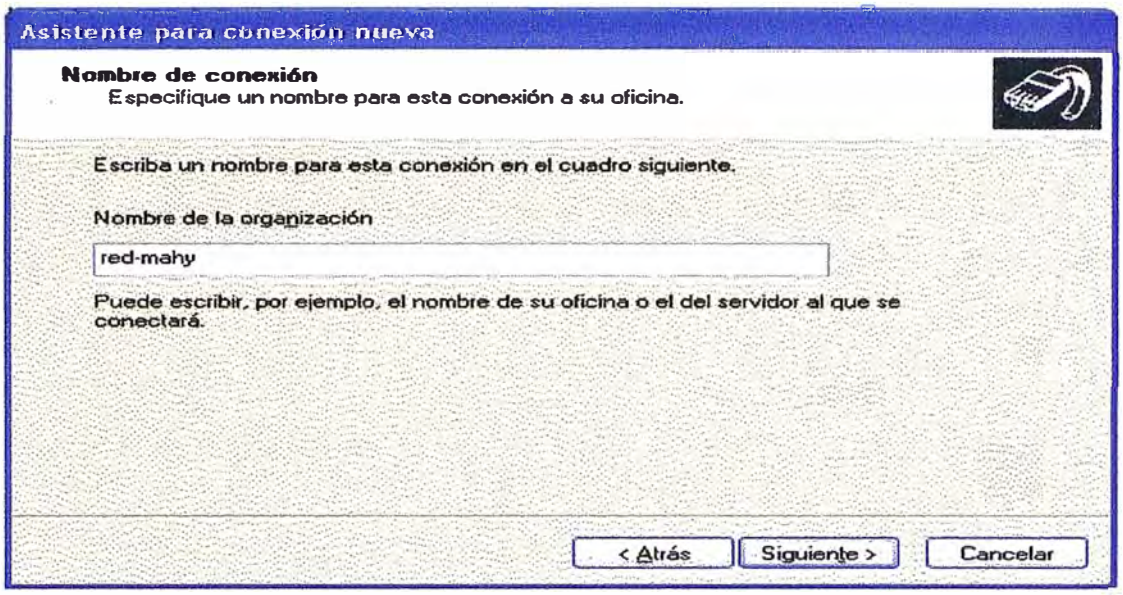

Fig.5.20 Nombre de identificación

Luego pregunta si queremos ejecutar una conexión telefónica antes de lanzar la conexión PPTP. Elegimos no usar la conexión inicial, ya que la primera conexión PP se hará manualmente(Fig.5.21)

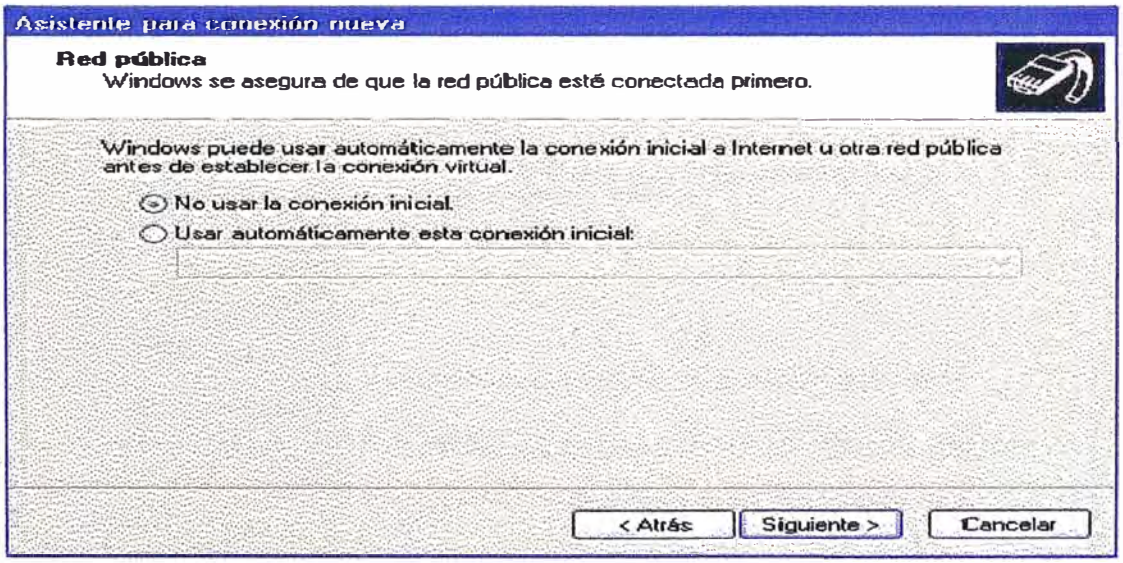

Fig.5.21 Selección de no usar conexión inicial

Digitar el IP o nombre de la compañía remota, en nuestro caso 66.128.33.25 que es el IP que la ISP le ha dado al servidor PPTP(Fig.5.22).

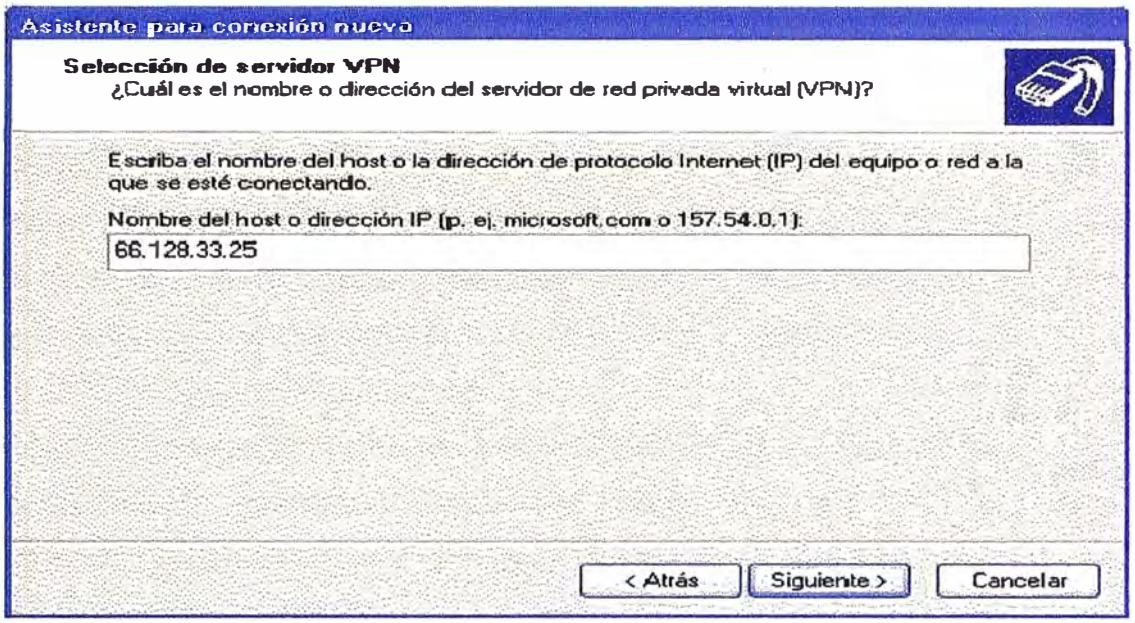

Fig.5.22 Ingreso de IP de compañía remota

Terminamos con el asistente, click en **siguiente(Fig.5.23)** y en la ventana de finalización **finalizar.**

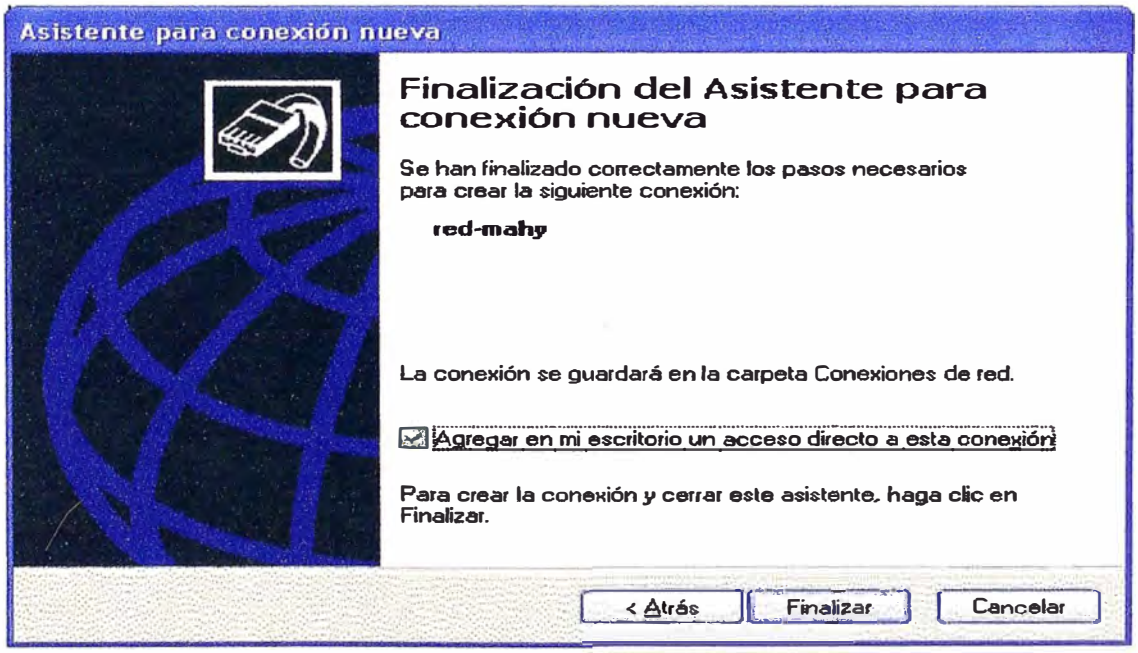

Fig.5.23 Finalización de asistente para conexión nueva

Para lanzar la conexión PPTP, configurar ciertos parámetros que el asistente deja por defecto, como la asignación del gateway y del servidor WINS.

Para que nuestra PC que se va conectar ala VPN no pierda su conexión a Internet es necesario especificar en la propiedades TCP/IP que no use la puerta de enlace predeterminada en la red remota, esto es necesario para que no se creen dos rutas por defecto distintas, la de la conexión PPP y de la conexión PPTP.

Para realizar este cambio, damos click derecho en la conexión PPTP recién creada y seleccionamos propiedades luego se selecciona la pestaña Funciones de red, en el tipo de red privada virtual (VPN) se puede dejar en automático o se puede escoger PPTP, la otra opción es L2TP/IP sec pero no la usamos.

Lo siguiente es seleccionar el Protocolo Internet (TCP/IP) damos click en propiedades, en el cuadro de dialogo aparecido lo dejamos por defecto, osea IP y DNS sean asignados dinámicamente. Damos click en Opciones Avanzadas, aparece una ventana con tres pestañas: General , DNS y WINS.

En general se desactiva la opción Usar la puerta de enlace predeterminada en la red remota(Fig.5.24):

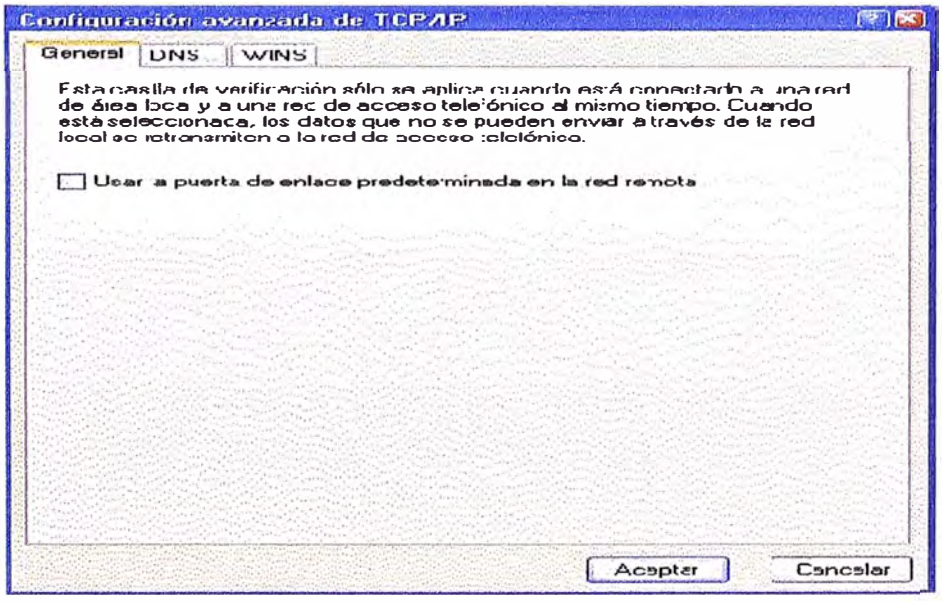

Fig.5.24 Configuración avanzada TCP

Luego en la pestaña WINS adicionamos manualmente el IP del servidor WINS que 192.168.4.1, en este caso es mismo IP del servidor de dominio el cual también hace las veces de servidor PPTP luego click en **aceptar(Fig.33)** en todas las ventanas hasta el punto de llegar a la ventana de **conexiones de red.** Damos doble click en el icono de red-mahy y aparece un cuadro de dialogo con el nombre de usuario y contraseña con el cual el

usuario se va a autenticar en el servidor PPTP, luego **conectar**

Fig.5.25 Conexión a red remota

Verificamos la conectividad haciéndole un ping al servidor PPTP(Fig.5.26):

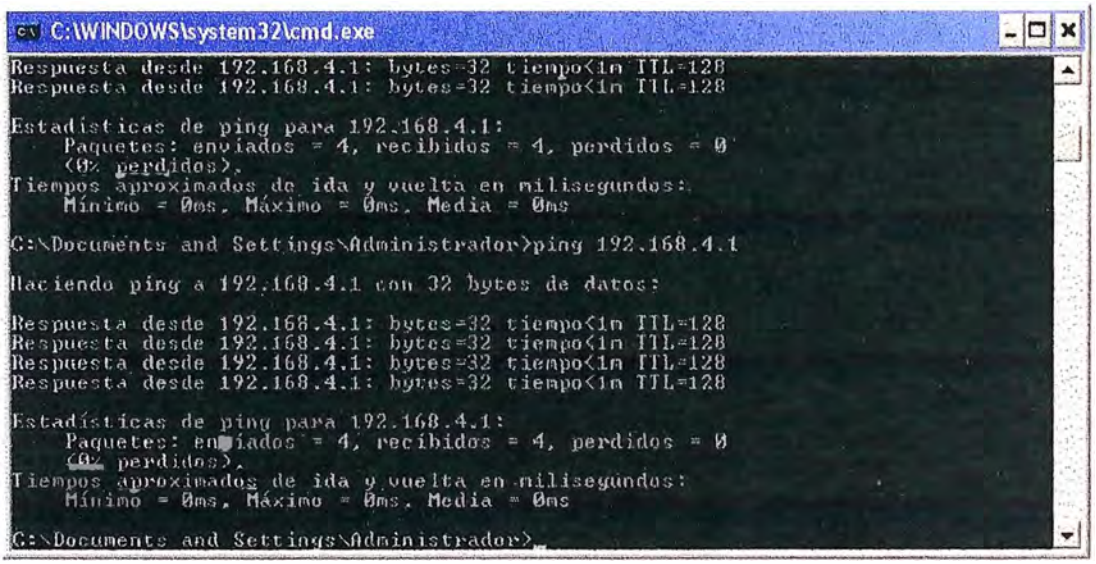

Fig.5.26 Verificación de conectividad

O ver en el entorno de red los computadores conectados en la red-remota y realizar las tareas comunes dentro de una LAN, transferencia de archivos, carpetas compartidas, acceso a impresoras, etc.

5.2. Lan-to-lan Ipsec usando tecnología LINUX/FREESWAN

El siguiente será el escenario instalado y configurado Fig.5.27:

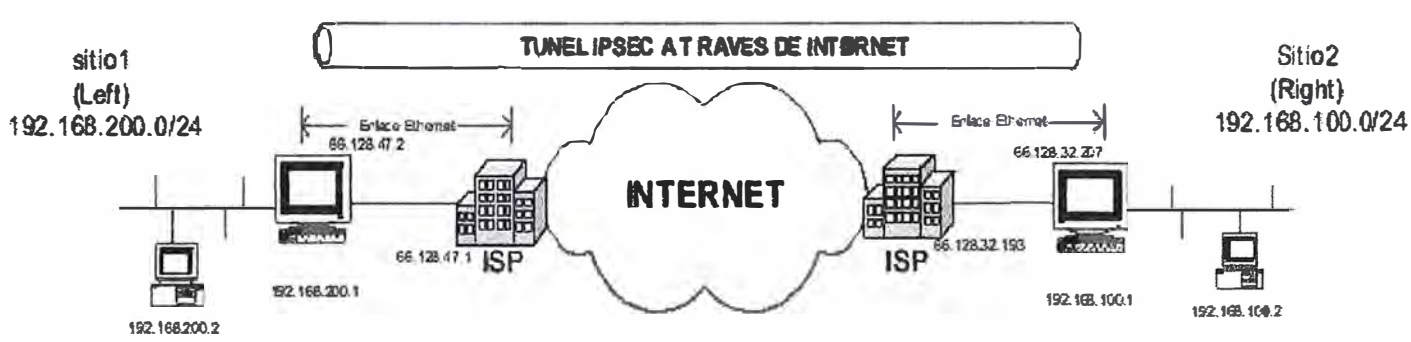

Fig.5.27 VPN LAN to LAN usando FREESWAN

EL software libre en los últimos años esta siendo tomado en cuenta por las organizaciones, debido a que les permiten obtener un programas o aplicaciones muy sólidos y estables; además que no necesita pagar licencias por el uso, traduciendo esto en ahorro en costos.
FreesWan es una implementación de Ipsec bajo el sistema operativo linux, que autentica y cifra las conexiones IP. La versión Frees/WAN 2.0, permite usar las PCs Linux como gateways VPN, de este modo podemos implementar la topología LAN-to-LAN VPN o acceso remoto VPN.
Para evitar ataques FreesWAN maneja dos tipos de autenticación para hacer túneles:

- Manual Keying.- Ambas partes comparten llave secreta para encriptar mensajes. Freeswan almacena esta llaves en el archivo /etc/ipsec.conf. Con el peligro de ser accesado se volvería vulnerable.
- Automatic Keying.- Ambos sistemas se autentican el uno con el otro por medio de sus propias llaves secretas. Estas llaves son cambiadas automáticamente de una manera periódica. Este método de autenticación es mucho mas seguro, debido a que si un intruso obtiene la llave, solo los mensajes entre la renegociación anterior y la siguiente serán expuestos.

Instalación:

Usaremos los paquetes que vienen en **debian-sid** freeswan-2.04-11.1 y freeswan-modules-2.04-11.1.

Procedemos a realizar la instalación:

pcmiguel:~#apt-get install freeswan freeswan-modules

Nos hará unas preguntas, marcarlas por defecto para posteriormente reconfigurarlas.

El servicio los iniciamos con

pcmiguel:~#/etc/init.d/ipsec Start

Probamos la instalación y nos saldrá las primeras 4 líneas de la forma:

pcmiguel:~#ipsec verify

Version check and ipsec on-path [OK]
Linux FreeS/WAN U2.04/K(no kernel code presently loaded)
Checking for KLIPS support in kernel [OK]
Checking for RSA private key (/etc/ipsec.secrets) [OK]
ipsec showhostkey: no default key in "/etc/ipsec.secrets"
Checking that pluto is running [OK]

La configuración la realizaremos en los archivo /etc/ipsec.conf y etc/ipsecrets

Los gateways deben tener IP estáticos dado por la ISP, bien sea una interfaz ppp (ppp0) o una interfaz ethernet (eth0).

A cada gateway se le debe asignar por nomenclatura como righ o left, indistintamente cual se escoja para cada nombre. EL gateway Ipsec left tiene IP publico 66.128.47.2 y el gateway Ipsec right IP publico 66.128.32.207, esto para tener una congruencia en al nomenclatura a lo largo del proceso de configuración del archivo /etc/ipsec.conf.

Este archivo se divide en dos secciones: la primera donde se configuran las opciones generales Ipsec, llamada **config setup** y la segunda se define cada pareja Ipsec llamada **conn**, en esta ultima sección puede aparecer una llamada **%default** que es donde se definen las características que se aplican por defecto a cada pareja de gateways Ipsec.

La parte mas importante del archivo /etc/ipsec.conf es la que define cada conexión IPSEC, de hecho todas las opciones en la seccion **config setup** son opcionales. Los campos básicos que define cada pareja IPSEC son:

left=
leftcert=

leftsubnet=
right=
rightid=
rightsubnet=
auto=

Los campos left y right son las IPs publicas de cada gateway, los campos leftsubnet y rightsubnet son las subredes que se encuentran detrás de cada gateway (la red privada).
Los campos leftnexthop y rightnexthop son las direcciones IP del equipo que recibe la conexión en el ISP, en la puerta de enlace de cada maquina linux.
Los campos leftrsasigkey y rigthsasigkey son las llaves publicas de cada gateway IPSEC, y se obtienen con los comandos:

pcmiguel:~#ipsec showhostkey –left (pc left)

pcmiguel:~#ipsec showhostkey –rigth (pc rigth)

En caso de no contar con estas llaves, se puede generar cada una de ellas con:

pcmiguel:~#ipsec newhostkey --output /etc/ipsec.secrets –hostname

Adicionalmente en el archivo /etc/ipsec.conf la linea auto=start hace que el túnel se establezca durante el proceso de boot de la maquina. Inicialmente, para propositos de de troublesbooting, se recomienda que la línea auto tenga el valor add, lo cual obliga a que cada vez el administrador inicie el túnel de manera manual y así detectar errores en el establecimiento de SA(asociación de seguridad). Una vez hecho este procedimiento, la línea auto deberá quedar con el valor start para que el túnel se establezca sistemáticamente cada vez que la maquina se reinicie.

EL comando para establecer el túnel de forma manual es:

pcmiguel:~#ipsec auto -up server1-to-server2

Donde server1-to-sever2 es el nombre dado a al pareja IPSEC en el archivo /etc/ipsec.conf y auto indica que las llaves se negocian de forma automática (no manual).

No es necesario ejecutar este comando en las dos maquinas, en una es suficiente.
La salida de este comando es:

pcmiguel:~#ipsec auto -up server1-to-server2

104 "server1-to-server2" &1: STATE MAIN r1: iniciate
106 "server1-to-server2" &1: STATE_MAIN_r2: sent MR2, expecting MR2
108 "server1-to-server2" &1: STATE_MAIN_r3: sent MR3, expecting MR3
004 "server1-to-server2" &1: STATE_MAIN_r4: ISAKMP SA established
112 "server1-to-server2" &2: STATE_QUICK_r1: iniciate
004 "server1-to-server2" &2: STATE_QUICK_r2: sent Q12, Ipsec Saestablished

Otro comando para obtener mas información sobre asociaciones de seguridad que están establecidas en un gateway Ipsec es:

pcmiguel:~#ipsec look

La implementación Frees/WAN no permite realizar ping desde los gateways Ipsec hasta las maquinas de la red privada remota, las pruebas de conectividad IP se tienen que realizar desde las maquinas que se encuentran detrás de cada gateway Ipsec. Las pruebas de ping se realizaron desde el equipo con IP 192.168.100.2 hasta el equipo con IP 192.168.0.2 con respuestas mutuas.

5.3. Resumen

Las instalaciones y configuraciones de VPN usando PPTP y LINUX/FreesWAN(IPsec), se han detallado en este capitulo,
La implementación de PPTP proporciona ventaja adicional de soporte por parte de Microsoft pero desventaja por el costo de licencias.
Mientras la implementación de LINUX/FreesWAN nos muestra reducción de costos por no pagar licencias, pero como un adicional de ser un clon de UNIX, que se caracterizan por su solides.

CONCLUSIONES Y RECOMENDACIONES

1.- El crecimiento del Internet y la reducción de tarifas por su acceso, han permitido que se desarrollen aplicaciones que se ejecuten sobre la misma.

2.- Aplicaciones que antes solo se daban en redes locales, hasta tal punto de que se ha logrado realizar enlaces privados a través de la Internet, los llamados túneles que forman parte de la implementación de una VPN realizan el enlace privado, este desarrollo es consecuencia del mejoramiento del IPv4(Protocolos de encriptación, de túnel PPTP) y el desarrollo de IPv6(IPsec).

3.- El crecimiento que ha tenido el uso de las VPN, se ha dado debido a la cobertura de la Internet y disminución de precios de implementación de dicho aplicativo.

4.- Actualmente los proveedores de transporte de datos, que se encuentran en un auge económico son los ISPs, ya que están explotando las VPNs para realizar conexiones privadas.

5.- Para una implementación de una VPN se debe tener bien en cuenta la tecnología a usar y el escenario de implementación(presupuesto, usuarios a atender y el desplazamiento de ellos, tipos de aplicaciones a manejar y velocidad de conexión a Internet).

6.- Las Redes Privadas Virtuales VPN proporcionan las siguientes ventajas:

6.1. Forma de reducir costos ya que con las VPN se eliminan las largas líneas de costo elevado. Con las VPN las organizaciones solo necesitan una conexión relativamente pequeña al proveedor de servicio.

6.2. Disminuir la carga de teléfono para accesos remotos, los clientes VPN solo necesitan llamar al proveedor del servicio mas cercano, que en la mayoría de los casos será una llamada local.

7.- Las VPN evitan el problema que existía en el pasado al aumentar las redes de un determinada compañía, gracias a Internet. Internet simplemente deriva en accesos distribuidos geográficamente.

8.- Podemos considerar como desventajas:

8.1. Las VPN requieren un reconocimiento en profundidad de la seguridad en las redes publicas y tomar precauciones en su desarrollo

8.2.Las VPN Dependen de un área externa a la organización, Internet en particular, y por tanto depende de factores externos al control de la organización.
8.3.Las diferentes tecnologías de VPN podrían no trabajar juntas.
8.4.Las VPN necesitan diferentes protocolos que los de IP.
9.- Se estima que las soluciones VPN para una determinada organización puede reducir costos entre un 30% y un 50% comparada con conexiones punto a punto.

Las redes privadas virtuales VPN se pueden aplicar en:

- Teletrabajo.- Una solución ideal por su efectividad y sus bajos costos, para aquellas organizaciones que necesiten que sus empelados accedan ala red desde cualquier ubicación.
- VPN Empresa.- Solución de conectividad entre sucursales de la empresa o entre la empresa y sus socios, proveedores, etc. Debido a su flexibilidad se adapta al tamaño y necesidades de cualquier organización.

ANEXO A
INDICE DE FIGURAS

ANEXO B
INDICE DE TABLAS

ANEXO C
GLOSARIO DE TERMINOS

1. Secure Sockets Layer (SSL) y Transport Layer Security (TLS), su sucesor, son protocolos criptográficos que proporcionan comunicaciones seguras en Internet. Existen pequeñas diferencias entre SSL 3.0 y TLS 1.0, pero el protocolo permanece sustancialmente igual. El término "SSL" según se usa aquí, se aplica a ambos protocolos a menos que el contexto indique lo contrario.
2. International Telecommunication Union(ITU),es una organización internacional del sistema de las Naciones Unidas en la cual los gobiernos y el sector privado coordinan los servicios y redes mundiales de telecomunicaciones.

BIBLIOGRAFIA

Libros

1. Andrew S. Tanenbaum. Redes de Computadores,. 3ed.
2. William Stalling. Comunicaciones y Redes de Computadores, 7a ed,

Enlaces web

3. Comprendiendo PPTP y VPNs http://www.rhino9.org
4. Documentación grupo alarmas Telefónica Investigación y desarrollo
5. Documentación ATM servicios de formación Telefónica de España
6. Introducción a las VPNs www.entarasys.com/la
7. PPTP en las siguientes direcciones:
8. PPTP en www.cisco.com/warp/public/44/solucions/network/vpn.shtml
9. PPTP en http://www.poptop.org
10. PPTP en http://www.polbox.com/h/hs001
11. PPTP en http://www.google.com
12. PPTP en http://bulma.net
13. PPTP en http://www.linuxdoc.org/HOWTO/VPN-HOIWTO.html
14. PPTP en http://www.linuxpowered.com/html/links/networking.html
15. Acceso remoto por VPN http://www.uv.es/ciuv/cat/vpn
16. PPTP http://www.cas.mcmaster.cal/wmfarmer/SE-ACO3/papers/Silva-PPTP.html