3

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES

CUAUTITLAN

"IMPLEMENTACION DE UNA RED VIRTUAL"

TRABAJO DE SEMINARIO

QUE PARA OBTENER EL TITULO DE

LICENCIADO EN INFORMATICA

P R E S E N T A :

ALFREDO ARRIAGA MILLAN

ASESOR: ING. MIGUEL ALVAREZ PASAYE

CUAUTITLAN IZCALLI, EDO. DE MEX. 200

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

UNIDAD DE LA ADMINISTRACION ESCOLAR

DEPARTAMENTO DE EXAMENES PROFESIONALES

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN: Q. Ma. del Carmen García Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 51 del Reglamento de Exámenes Profesionales de la FES-Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario:

Redes de Computadoras. Implementación de una Red Virtual.

que presenta el pasante: Alfredo Arriaga Millán

con número de cuenta: 9555999-1 para obtener el título de :

Licenciado en Informática.

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXÁMEN PROFESIONAL correspondiente, otorgamos nuestro VISTO BUENO.

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Méx. a 27 de Octubre de 2000.

MODULO	PROFESOR	FIRMA
III	Ing. Miguel Alvarez Pasaye	
II	Ing. Carlos Vázquez Cruz	
IV	M.C.C. Araceli Nivon Zaghi	

Agradecimientos

A mis padres Jesus Arriaga Perez y Angelina Millán Granados por su apoyo incondicional en todas las etapas de mi vida.

A mis Hermanos Jesus, Carmen, Margarita, Ricardo y Jorge por demostrarme que ocupo un lugar especial en sus vidas.

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

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

CONTENIDO

CAPÍTULO 2. DESCRIPCION GENERAL DE LAS REDES PRIVADAS VIRTUALES

CAPÍTULO 3. PROTOCOLO DE TUNEL PUNTO A PUNTO

CAPÍTULO 4. SEGURIDAD DE LAS VPN´S

CAPÍTULO 5. DIRECCIONAMIENTO PARA VPN´S

CAPÍTULO 6. RESOLUCIÓN DE PROBLEMAS DE LAS VPN´S

CAPÍTULO 7. PROYECTO: INSTALACIÓN, CONFIGURACIÓN Y PUESTA A PUNTO DE UNA CONEXIÓN VPN

IMPLEMENTACION DE UNA RED VIRTUAL

Objetivo General:

Implementación de una Red Virtual para el acceso remoto de un usuario móvil a la red local de la empresa Moore de México S.A de C.V.

Objetivos Particulares:

- Facilitar al usuario el acceso a los recursos de la red local.
- Mantener la confidencialidad de información que maneja la empresa, así como la que se proporcione a los usuarios móviles.
- Fomentar una cultura empresarial nivel usuario implementando las nuevas tecnologías.

Justificación :

Debido a la importancia que tiene la información hoy en día es de suma importancia que llegue a su destino de la manera más segura, rápida y con menos costos, implementando nuevas tecnologías y aprovechando al máximo su capacidad como lo son las redes virtuales.

INTRODUCCIÓN

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

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

La novedad en estas conexiones, o intercambios de paquetes PPP (Protocolo Punto a Punto) es que se realiza a través de una red pública de datos, como Internet y no a través de enlaces directos o lineas dedicadas. Lo que se trata es de encapsular protocolos de red ya existentes (IPX, IP y Netbeui) en paquetes PPP y éstos a su vez son encapsulados en protocolos de Tunneling, PPTP, proporcionado por Microsoft en Windows 95 y Windows NT 4.0. Resultado: de una manera sencilla, podremos compartir redes locales remotas a través de VPN a coste de llamada local (ISP) y sin necesidades de contratar costosas líneas dedicadas.

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

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

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

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

CAPITULO I

ESQUEMA GENERAL DE REDES

CAPÍTULO I

I. ESQUEMA GENERAL DE REDES.

1.1. Que es una red local.

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

Según su ubicación, se pueden distinguir tres tipos distintos:

- Si se conectan todas las computadoras dentro de un mismo edificio, se denomina LAN (Local Area Network).
- Si se encuentran distribuidos en distancias no superiores al ámbito urbano, MAN (Metropolitan Area Network).
- Si están instalados en ciudades diferentes, WAN (Wide Area Network).

Según la forma en que estén conectados las computadoras, se pueden establecer varias categorias:

- **Redes sin tarjetas.** Utilizan enlaces a través de los puertos serie o paralelo para transferir archivos o compartir periféricos.
- **Redes punto a punto.** Un circuito punto a punto es un conjunto de medios que hace posible la comunicación entre dos computadoras determinados de forma permanente.
- **Redes entre iguales,** en las cuales todas las computadoras conectadas pueden compartir información con los demás.
- **Redes basadas en servidores** centrales utilizando el modelo básico cliente, servidor.

1.2. Ventajas de las redes locales.

Entre las ventajas de utilizar una red se encuentran:

- Posibilidad de compartir periféricos costosos como impresoras láser, módem, fax, etc.
- Posibilidad de compartir gran cantidad de información a través de distintos programas, bases de datos, etc., de manera que sea mas fácil de uso y actualización.
- Reduce e incluso elimina la duplicidad de trabajos.
- Permite utilizar el correo electrónica para enviar o recibir mensajes de diferentes usuarios de la misma red e incluso de redes diferentes.
- Reemplaza o complementa minicomputadoras de forma eficiente y con un costo bastante más reducido
- Permite mejorar la seguridad y control de la información que se utiliza, permitiendo la entrada de determinados usuarios, accediendo únicamente a cierta información o impidiendo la modificación de diversos datos.

Inicialmente, la instalación de una red se realiza para compartir los dispositivos periféricos u otros dispositivos de salida caros, por ejemplo , las impresoras láser, los fax, etc.

Pero a medida que va creciendo la red, el compartir dichos dispositivos pierde relevancia en comparación con el resto de las ventajas. Las redes enlazan también a las personas proporcionando una herramienta efectiva para la comunicación a través del correo electrónico. Los mensajes se envían instantáneamente a través de la red, los planes de trabajo pueden actualizarse tan pronto como ocurran cambios y se pueden planificar las reuniones sin necesidad de llamadas telefónicas.

1.3. Arquitectura cliente/servidor.

Con el paso del tiempo, los usuarios de computadoras fueron necesitando cada vez más acceder a mayor cantidad de información y de forma más rápida, por lo que fue aumentando también la necesidad de un nuevo tipo de computadora : el servidor.

Un servidor (del inglés SERVER) es una computadora que permite compartir sus periféricos con otras computadoras. Éstos pueden ser de varios tipos y entre ellos se encuentran los siguientes:

- **Servidor de archivos.** Mantienen los archivos en subdirectorios privados y compartidos para los usuarios de la red.
- **Servidor de impresión.** Tiene conectadas una o más impresoras que comparte con los demás usuarios.
- **Servidor de comunicaciones.** Permite enlazar diferentes redes locales o una red local con grandes computadoras o minicomputadoras.
- **Servidor de correo electrónico.** Proporciona servicios de correo electrónico para la red.
- **Servidor de Web .** Proporciona un lugar para guardar y administrar los documentos HTML que pueden ser accesibles por los usuarios de la red a través de los navegadores.
- **Servidor FTP.** Se utiliza para guardar los archivos que pueden ser descargados por los usuarios de la red.

Según el sistema operativo de red que se utilice puede ocurrir que los distintos tipos de servidores residan en la misma computadora o bien se encuentren distribuidos entre aquellos que forman parte de la red.

Así mismo, los servidores de archivos pueden ser dedicados o no dedicados, según se dediquen sólo a la gestión de la red o, además, se puedan utilizar como estación de trabajo. La conveniencia de utilizar uno u otro va estar indicada por la cantidad de estaciones de trabajo de que se vaya a disponer; cuanto mayor sea el número de ellas, más conveniente será disponer de un servidor dedicado.

No es recomendable utilizar un servidor no dedicado como estación de trabajo, ya que, en caso de que esta computadora tenga algún problema, la totalidad del sistema puede dejar de funcionar, con los consiguientes inconvenientes y pérdidas irreparables que se pueden producir.

El resto de las computadoras de la red se denominan estaciones de trabajo o clientes, y desde ellos se facilita a los usuarios el acceso a los servidores y periféricos de la red.

Cada estación de trabajo consiste, por lo general, en una computadora que funciona con su propio sistema operativo. A diferencia de una computadora aislada, la estación de trabajo tiene una tarjeta de red y esta físicamente conectada por medio de cables con el servidor.

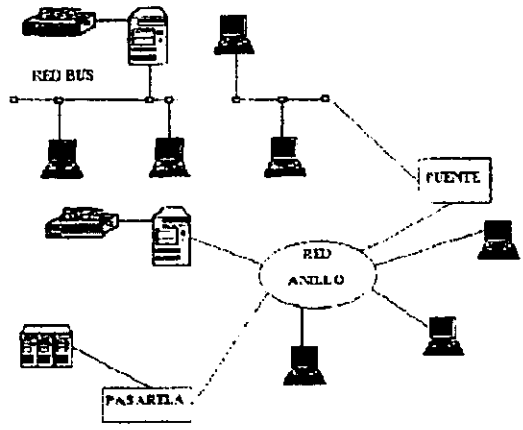


Figura 1. Representación esquemática de una red local.

1.4. Elementos de conexión.

Se consideran elementos de conexión los cables, tarjetas de red y otros equipos necesarios para conectar entre sí las computadoras. Dentro de los cables de conexión utilizados se encuentran:

- **Par de hilos sin apantallar** (UTP), que consiste en pares de hilos sin trenzar y recubiertos de una capa aislante externa. Es de fácil instalación y ofrece poca protección contra las interferencias externas. Se utiliza principalmente para la transmisión de voz.
- **Par trenzado apantallado** (STP), que consiste en pares de hilos trenzados de forma independiente y luego trenzados entre sí y recubierto de una capa aislante externa. Es de fácil instalación y ofrece cierta protección contra las interferencias externas.
- **Cable coaxial,** que es un hilo de cobre envuelto en una malla trenzada. Entre ambos se encuentra una capa de material aislante. Hay dos tipos en función del grosor. Ofrece mayor protección que el par trenzado apantallado frente a las interferencias externas.
- **Fibra óptica** que esta formada por un núcleo de material transparente muy fino rodeado de otro material con distinto índice de refracción. De esta forma, las señales luminosas que viajan por el núcleo son reflejadas por la capa externa, llegando al extremo del cable. Permite

mayor velocidad de transmisión de los datos aunque resulta muy cara su instalación.

1.5. Técnicas de transmisión.

Entre las más comunes están: banda base y banda ancha.

1.5.1 Banda base.

Es el método más común dentro de las redes locales. Transmite las señales en forma digital sin emplear técnicas de modulación, en cada transmisión se utiliza todo el ancho de banda y, por tanto, solo puede transmitir una señal simultáneamente.

Esta especialmente indicada para cortas distancias, ya que en grandes distancias se producirían ruidos e interferencias (pueden utilizarse repetidores que vuelven a regenerar la señal)

Los elementos de conexión que se pueden utilizar son : el cable de par trenzado y el cable coaxial de banda base.

1.5.2 Banda ancha.

Consiste en transmitir las señales en forma digital modulando la señal sobre ondas portadoras que pueden compartir el ancho de banda del medio de transmisión mediante multiplexación por división de frecuencia. Es decir, actúa como si en lugar de un único medio se estuvieran utilizando líneas distintas.

La velocidad de transmisión de los datos depende del ancho de banda.

Este método hace imprescindible la utilización de un módem para poder modular y demodular la información.

La distancia máxima puede llegar hasta los 50 Kms, y permite usar además los elementos de conexión de la red para transmitir otras señales distintas de las propias de la red como pueden ser señales de televisión o señales de voz.

Los elementos de conexión que se pueden utilizar son: el cable coaxial de banda ancha y el cable de fibra óptica.

1.6. Topologías.

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

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

Las formas más utilizadas son:

1.6.1. Configuración de bus.

En ella todas las estaciones comparten el mismo canal de comunicaciones, toda la información circula por ese canal y cada una de ellas recoge la que le corresponde. Esta configuración es fácil de instalar, la cantidad de cable a utilizar es mínima, tiene una gran flexibilidad a la hora de aumentar o disminuir el número de estaciones y el fallo de una estación no repercute en la red aunque la ruptura de un cable la dejará totalmente inutilizada.

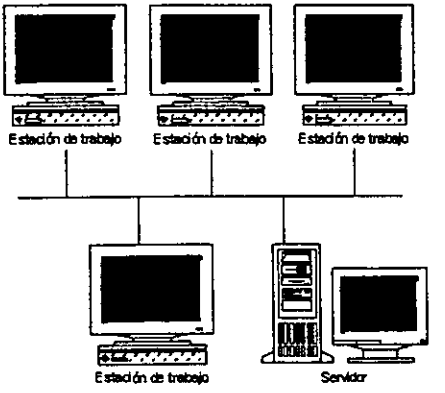


Figura 2. Configuración en bus.

Entre sus inconvenientes destacan:

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

Es la configuración mas extendida actualmente y esta usada por la red ETHERNET.

1.6.2. Configuración en anillo.

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

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

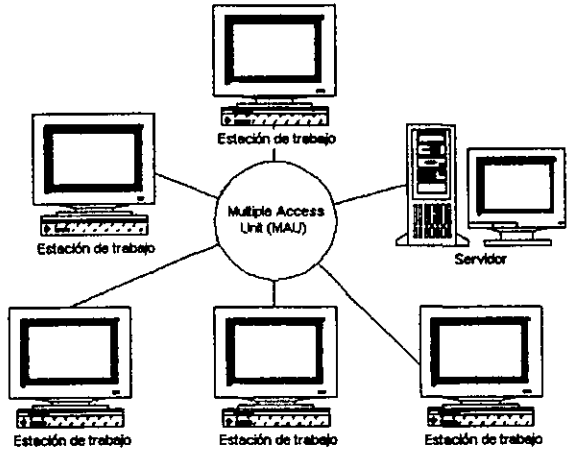


Figura 3. Configuración en anillo

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

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

1.6.3. Configuración en estrella.

Esta forma de configuración es una de las mas antiguas. Todas las estaciones están conectadas directamente a un hub (concentrador) y esté al servidor , todas las comunicaciones se han de hacer necesariamente a través de él.

Permite incrementar y disminuir fácilmente el numero de estaciones.

Si se produce un fallo en una de ellas no repercutirá en el funcionamiento general de la red; pero, si se produce un fallo en el servidor, la red completa se vendrá abajo.

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

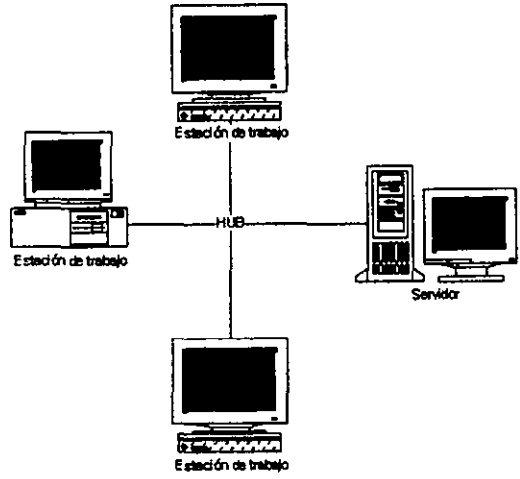


Figura 4. Configuración en estrella.

No es muy conveniente para grandes instalaciones y su coste es caro debido a la gran cantidad de cableado y a la complejidad de la tecnología que se necesita para el servidor.

1.6.4. Topología física y lógica.

Toda las configuraciones vistas hasta ahora son llamadas topologías físicas porque describen cómo está extendido el cableado.

Además, cada red designa una topología lógica que describe la red desde la perspectiva de las señales que viajan a través de ella.

Un diseño de red puede tener distinta topología física y lógica (es decir, la forma en que esté cableada una red no tiene por qué reflejar necesariamente la forma en que viajan las señales a través de ella).

Por ejemplo, la figura 5, se muestra una disposición física de configuración en *estrella*.

Cada estación envía y recibe señales por el mismo cable. En el concentrador (hub) se mezclan las señales de todas las estaciones y son transmitidas a todas ellas (es decir, actúa igual que si estuviera en una configuración en bus).

Por tanto, es una topología física de estrella que funciona como una topología lógica de bus.

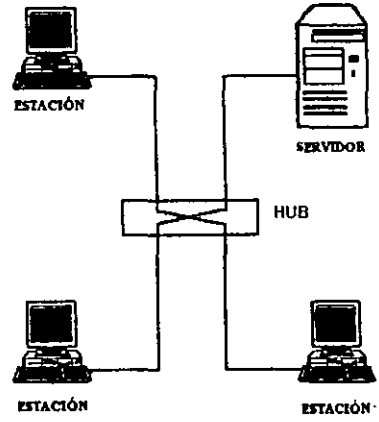


Figura 5. Topología física de estrella.

Muchas redes nuevas utilizan este modelo, ya que es fácil de modificar la situación de cada estación (sólo hay que desconectar un cable) sin perjuicio para la red entera, y además incrementa las posibilidades de detección de problemas de red.

1.7. Paquetes de datos.

La transmisión de datos de gran extensión en formato de un único bloque no es conveniente y, por tanto, los datos a enviar se dividirán en segmentos más pequeños llamados paquetes.

Éstos se dividen en cuatro partes:

- Cabecera, que esta formada por el identificativo del bloque de comienzo, el identificativo del lugar del destino del paquete, el identificativo del origen del paquete y la información referente al protocolo que se está utilizando.
- Información, que contiene el texto o la parte del texto que se va a transmitir.
- Control de errores, que contiene la información necesaria para que el sistema pueda verificar si los datos del paquete se han recibido correctamente.
- Bloque final, que contiene la información que indica que el paquete ha finalizado.

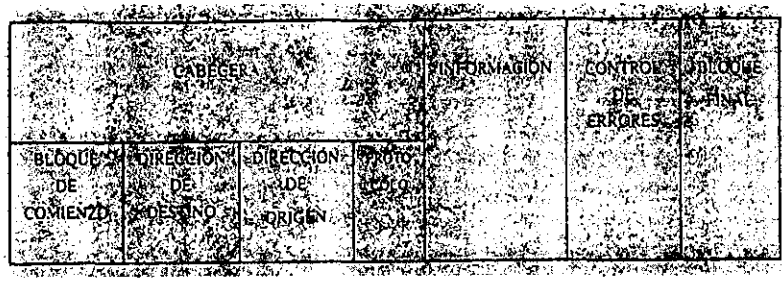


Figura 6. Formato de paquete según el protocolo IP.

Además de estas cuatro partes, también se incluye , en cada paquete de datos, un numero de secuencia que sirve para que todos los paquetes recompongan el mensaje completo en el orden correcto, y otra información de control que permite evitar el envío de paquetes duplicados y/o la perdida de uno de ellos.

1.8. Transmisión de los datos.

Se entiende por transmisión de los datos al proceso de transporte de la información codificada de un punto a otro.

En toda transmisión de datos se ha de aceptar la información, convertirla a un formato que se pueda enviar rápidamente y de forma fiable, transmitir los datos a un determinado lugar y, una vez recibidos de forma correcta, volverlos a convertir al formato que el receptor pueda reconocer y comprender.

Todas esas acciones forman el proceso de transmisión, que puede dividir el proceso de transmisión de datos en tres funciones: edición, conversión y control.

- **Las funciones de edición** dan el formato adecuado a los datos y se encargan de controlar los errores.
- **Las funciones de conversión** se encargan de convertir los datos al formato recepción de los mensajes.
- **Las funciones de control** se ocupan del control de la red y del envio y recepción de los mensajes.

Todas estas funciones se implementan por medio de protocolos.

Entre los equipos que se utilizan para llevar a cabo una transmisión de datos, se encuentran :

- **MODEM.** Es un equipo que convierte las señales digitales del computadora a las analógicas de la línea telefónica (modulación), las envía a otro computadora y, cuando las recibe este, las vuelve a convertir de analógicas a digitales (demodulacion).

Los módems pueden ser internos (si van colocados dentro de la computadora) o externos (es un equipo independiente). Asi mismo, pueden comunicarse utilizando el puerto paralelo de la computadora (permite una mayor velocidad de transmisión pero a distancias muy cortas) o el puerto serie (permite una mayor distancia pero a cambio de disminuir la velocidad de la transmisión).

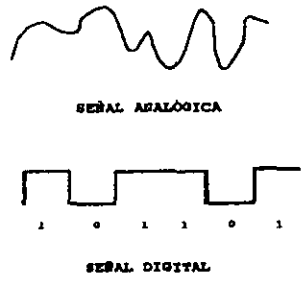


Figura 7. Señalización de un módem.

Además, se diferencian por la velocidad de transmisión de datos y por las formas de modulación.

- **La velocidad de transmisión de datos** es el numero de bits por segundos (bps) que puede modular y enviar por la línea telefónica (esta velocidad de transmisión de datos no es igual a la velocidad de transmisión serie que representa la cantidad de bits de información y control que la computadora envía al módem cada segundo).

- **Las formas de modulación que existen son tres**:

- **Modulación de amplitud** (ASK), en la que a cada valor de la señal digital se le hace corresponder una amplitud distinta de la señal analógica (para un valor binario 0 se envía una amplitud cero y para un valor binario 1 se envía una amplitud distinta de cero). Se emplea muy poco para enviar datos y siempre a muy bajas velocidades de transmisión, ya que es muy susceptible a las interferencias de la línea.
- **Modulación de frecuencia** (FSK), en la que a cada valor de la señal digital se le hace corresponder una frecuencia de la señal analógica (para un valor binario 0 se envía una frecuencia determinada y para un valor binario 1 se envía otra frecuencia distinta). Se emplea para velocidades de transmisión iguales o inferiores a 1200 bps.
- **Modulación de fase** (PSK), en la que a cada valor de la señal digital se le hace corresponder con un desfase de la señal analógica (para un valor binario 0 se modifica la fase y para un valor binario 1 no se modifica). Se emplea para velocidades superiores a 1.200 bps.

Para velocidades elevadas se utiliza la modulación de fase combinada con la modulación de amplitud.

- Para que una comunicación se pueda realizar, ambos módems deben transmitir a la misma velocidad y utilizar la misma forma de modulación. Así mismo, deben estar coordinadas la transmisión y la recepción de los datos (sincronización de la transmisión).

Hay tres factores que se han de tener en cuenta para la sincronización de la comunicación:

a) Sincronismo de bit. Los bits son enviados por el módem origen de forma secuencial y con una determinada cadencia. Este factor es responsabilidad del módem.

Hay dos métodos de sincronización de bit:

1. **Asincrona.** El método de sincronización asincrona hace que por cada carácter emitido sea necesario transmitir un bit de arranque (bit 0) seguido de 7 u 8 bits de información que identifican al carácter según el código ASCII y termina con el bit de parada (bit 1). El inconveniente de este método es que se aumenta mucho la cantidad de bits que se envían en cada comunicación.

2. **Sincrona.** El método de sincronización sincrona lleva a cabo la sincronización utilizando los mismos cambios de estado de las señales transmitidas. Al empezar una transmisión, se envían una serie de caracteres de sincronismos (llamados SYN) que están formados por una combinación de 0 y 1 . La principal ventaja de este método es que permite una mayor velocidad de transmisión.

b) Sincronismo de carácter. El módem receptor, al recibir los bits, debe tener algún procedimiento para diferenciar los caracteres que componen la información recibida. Este factor es responsabilidad del protocolo de comunicaciones utilizado.

c) Sincronismo de trama. Como la información no se transmite toda de una vez, sino que se realiza en secciones denominadas paquetes o tramas, es necesario establecer un procedimiento que permita identificar que carácter de los recibidos es el primero de la trama. Este factor es responsabilidad del protocolo de comunicaciones utilizado.

- **INTERFAZ.** Es el cable que une el computadora con el módem. En función del puerto al que estén conectados se denomina RS232 (puerto serie) o Centronics (puerto paralelo).

- **MULTIPLEXOREX.** Son equipos que permiten mantener mas de una comunicación simultanea por una sola línea. Cada una de las comunicaciones opera como si tuviera la línea de forma exclusiva pudiendo utilizar diferentes velocidades y protocolos en cada una de ellas.

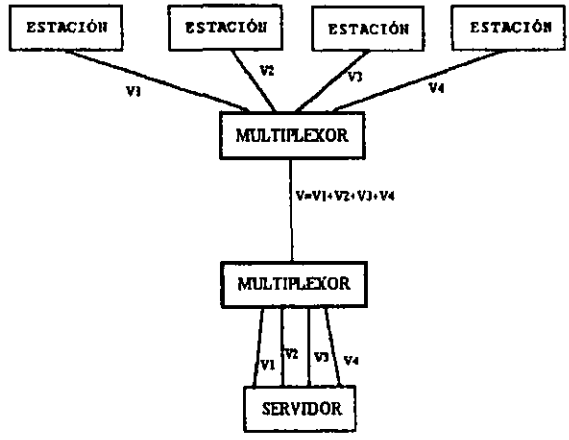


Figura 8. Representación esquemática de multiplexores.

- **CONCENTRADORES** (HUBS). Son equipos que permiten compartir el uso de una línea entre varias computadoras. Todas las computadoras conectadas a los concentradores pueden usar la línea, aunque no de forma simultánea ni utilizando distintos protocolos ni distintas velocidades de transmisión.

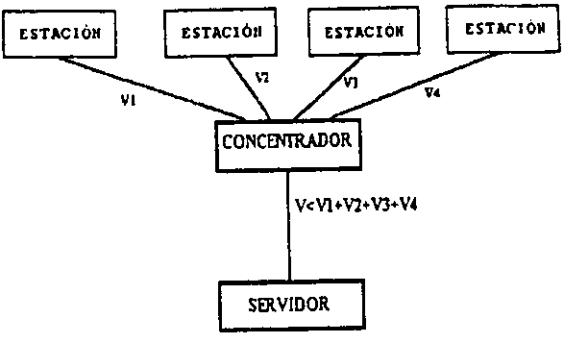


Figura 9 . Representación esquemática de un concentrador.

- **PROCESADORES DE COMUNICACIONES.** Son equipos que están diseñados para realizar las tareas especificas de control de las comunicaciones con el objeto de descargar de esta tarea al resto de las computadoras.

- **MULTIPLICADORES DE INTERFAZ.** Son equipos que se sitúan entre el módem y el computadora, permitiendo conectar varias computadoras a un único módem pero de forma que únicamente pueda transmitir datos simultáneamente uno de ellos.

- **ACOPLADORES ACÚSTICOS.** Son equipos formados por un módem que va acoplado a la línea telefónica a través del auricular del teléfono. Actualmente no son muy utilizados (con la excepción de su uso con portátiles) por las interferencias que pueden recibir.

1.9. Tipos de redes locales.

Hay muchos tipos distintos de redes locales, pudiéndose realizar múltiples combinaciones distintas al seleccionar el tipo de cableado, la topología, el tipo de transmisión e incluso los protocolos utilizados. Estos factores van a determinar la arquitectura de la red local.

Sin embargo, de todas las posibles soluciones hay tres que ya están establecidas y que , al mismo tiempo, cuentan con una gran difusión dentro del mundo de las redes locales:

- Ehernet
- Token Ring
- Arcnet

1.9.1. Ethernet.

Esta arquitectura de red fue desarrollada por Xerox Corporation para enlazar un grupo de microcomputadoras, que estaban distribuidos por los laboratorios de investigación de Palo Alto en California, para poder intercambiar programas y datos, así como compartir los periféricos.

En un principio se creó para ser utilizada con cable coaxial de banda base, aunque actualmente se pueden utilizar otros tipos de cable.

Si se utiliza cable coaxial grueso, se pueden tener hasta cuatro tramos de cable (unidos con repetidores) y las computadoras se conectan al cable por medio de transceptores (la distancia máxima entre el computadora y el transceptor ha de ser de 15 metros). Se puede conectar computadoras en tres tramos únicamente, con un máximo de 100 estaciones en cada tramo.

Si se utiliza cable coaxial fino, no es necesario utilizar transceptores, pudiéndose conectar el cable al computadora por medio de una conexión BNC en forma de T. El numero máximo de tramos es de cinco y la longitud máxima de cada tramo es, aproximadamente, de un tercio de la longitud máxima conseguida con el cable coaxial grueso (550 metros). Así mismo, el número máximo de estaciones es de 30 por cada uno de los tres tramos en los que se pueden conectar computadoras.

Los datos se transmiten a una velocidad de 10 Mbps a una distancia máxima de dos kilometros.

Utiliza una topología en bus con protocolo de contienda CSMA/CD (Acceso múltiple por detección de portadora con detección de colisiones). Cualquier estación puede intentar transmitir en cualquier momento, pero, como todas utilizan un canal único, solo una estación puede transmitir datos simultáneamente.

El tamaño del bloque de datos puede oscilar desde 72 hasta 1526 bytes (con un tamaño normal de 256 bytes).

Todas las estaciones tienen asignada una dirección de 84 bytes que permite que, cuando se cambia de lugar una estación, no haya posibilidad de conflictos y, por tanto, se puede reconfigurar completamente la red local con unos mínimos cambios en el sistema operativo.

1.9.1.1 Fast Ethernet.

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

1. Está construida con hubs distribuidos que utilizan líneas dedicadas para cada computadora.
2. Los cables utilizados son : 100 BaseTX y 100 BaseT4. La diferencia entre estos dos tipos de cables está en que el cable 100 BaseTX usa dos de los cuatro pares de hilos (igual que un cable UTP normal) que deben de ser de categoría 5 (por su mayor calidad) mientras que el cable 100 BaseT4 utiliza los cuatro pares de hilos que pueden ser de categoría 3 ó 5.
3. Necesita tarjetas de red especificas para la velocidad de transmisión de 100 Mbps.

Al igual que la arquitectura de red Ethernet, utiliza el protocolo de contienda CSMA/CD (Acceso múltiple por detección de portadora con detección de colisiones) y su coste de instalación es similar.

1.9.2. Token Ring.

Esta arquitectura de red fue creada por IBM en octubre de 1985 aunque anteriormente había comercializado dos tipos de redes locales: una red de banda base a 3758 Kbps y para un máximo de 64 computadoras y una red de banda ancha a 2 Mbps para un máximo de 72 computadoras.

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

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

No obstante, como se pueden conectar hasta 12 unidad de acceso multiestación (MAU), tanto el numero de computadoras conectadas como la distancia máxima pueden aumentar considerablemente.

1.9.3. Arcnet.

Este tipo de arquitectura comenzó siendo un sistema de proceso distribuido de Datapoint aunque fue potenciado en el mundo de los microcomputodores por Standar Microsystems.

En una red en banda base que utiliza una topología mixta estrella/bus con protocolo de paso de testigo.

Transmite a una velocidad de 2.5 Mbps y todas las computadoras han de estar conectadas a un concentrador (HUB activo). La distancia máxima entre el computadora y el HUB activo no puede sobrepasar los 660 metros.

A cada HUB activo se le pueden conectar HUB pasivos (a cada HUB pasivo únicamente se pueden conectar tres computadoras con una distancia máxima entre el HUB pasivo y cada computadora de 17 metros).

No obstantes, se puede conectar mas de un HUB activo (con una separación entre ellos de 660 metros), por lo que el numero máximo de estaciones puede llegar a ser de 255.

1.9.4. Otros Tipos de Redes.

Entre otros tipos de arquitecturas de redes se encuentran las redes inalámbricas. Una red local se denomina inalámbrica cuando los medios de unión entre las estaciones no son cables.

Ventajas :

- Permiten una amplia libertad de movimientos.
- Sencillez en la reubicación de las estaciones de trabajo evitando la necesidad de establecer un cableado.
- Rapidez en la instalación.

Desventajas :

- Dudas sobre si afecta a la salud de los usuarios.
- Faltan normas estándar.
- Poca compatibilidad con las redes fijas.
- Problemas con la obtención de licencias para aquellas que utilizan el espectro radioelectrico.

Su utilización esta especialmente recomendada para la instalación de redes en aquellos lugares donde no pueda realizarse un cableado o en lugares con una movilidad de las estaciones de trabajo muy grande.

1.10. Comunicación con el exterior.

Cuando se esta trabajando en una red local puede ser necesario enviar o recibir determinada información al exterior de la red.

Estos datos pueden proceder de otro computadora, de otra red, por tanto, antes de proceder a establecer conexión con ellos, se han de resolver los problemas que existen en las comunicaciones (direccionamiento, control de errores, método de transmisión, formato, etc.).

Dentro de los equipos necesarios para realizar la transmisión de datos con el exterior de la red se encuentran:

- **Un repetidor**, si se necesita regenerar la señal entre dos segmentos de red que se interconectan.
- **Una tarjeta RDSI** (Red Digital de Servicios Integrados), si se va a acceder al exterior desde una computadora utilizando RDSI.
- **Un módem**, si se va a acceder a un microcomputador independiente o a otro sistema que esta lejos y no se accede a el de forma periódica.

- **Un puente** (bridge) para conectar dos redes.
- **Un encaminador** (router) que dirige el paquete de datos determinando la ruta hacia su destino
- **Una pasarela** (gateway) para establecer un enlace con un minicomputador o con un mainframe.

1.10.1. Repetidor.

Un repetidor es un dispositivo encargado de regenerar la señal entre los dos segmentos de una red homogénea que se interconectan ampliando su cobertura. Operan en el nivel físico del modelo de referencia OSI.

Su forma de actuar es la siguiente: recogen la señal que circula por la red y la reenvían por la misma red o por otra distinta sin efectuar ningún tipo de interpretación de dicha señal.

Son capaces de conectar diferentes medios físicos de transmisión. Sin embargo, no suelen utilizarse para conectar redes de banda base con redes de banda ancha, ya que los métodos de descodificación de la información son muy diferentes.

1.10.2. Tarjeta RDSI.

Se utiliza para conectar una computadora con el exterior utilizando el sistema de comunicaciones RDSI. Tiene la ventaja con respecto a un módem de enviar los datos con mayor rapidez. Es lo más avanzado actualmente en comunicaciones digitales. Utiliza dos **routers** (uno en cada extremo) y una línea telefónica digital para enviar los datos a 128 **kilobits** por segundo.

1.10.3. Módem.

La función básica que desarrolla un módem es aceptar datos de una computadora y convertir las señales digitales en señales analógicas para que se transmitan a través de la línea telefónica.

Cuando los datos llegan al punto de destino, el módem receptor realiza la función inversa, es decir, vuelve a transformar las señales analógicas en señales digitales para que el computadora las pueda entender.

La comunicación se puede establecer en ambos sentidos, pero no simultáneamente (semidúplex), o en ambos sentidos simultáneamente (duplex). Es independiente el numero de hilos de que consta el cableado de la forma de establecer la comunicación.

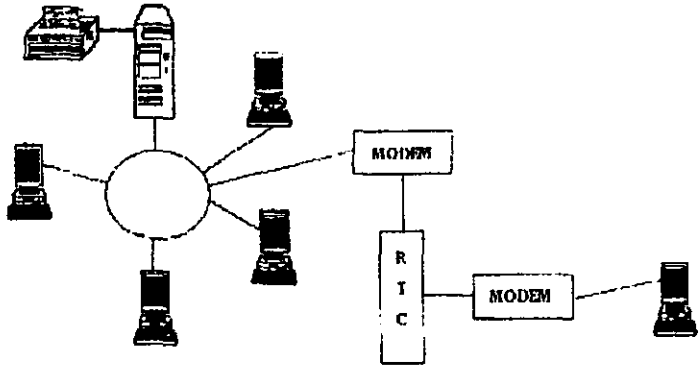


Figura 10. Representación esquemática de una Estación unida a la red por un módem a través de la red telefónica conmutada (RTC).

Es necesario destacar que para la velocidad del proceso es importante que el módem cuente con una velocidad alta, ya que cuanto mayor sea la velocidad menor será el tiempo que invertirá en el proceso (por ejemplo, un módem a 2400 bps tarda en transmitir los datos 8 veces menos tiempo que uno de 300 bps.

De todas formas, si se transmite por la red telefónica conmutada (RTC) la velocidad máxima que se puede conseguir actualmente es de , aproximadamente, 33,000 bps; por tanto , si se desean conseguir velocidades mayores será necesario disponer de líneas dedicadas.

Entre sus características mas importantes esta la de poseer listin telefónico donde almacena los números de teléfono y donde puede marcarlos automáticamente en el momento o bien hacerlo en una fecha y hora programada. En el caso de estar la línea ocupada, vuelven a intentar la llamada al cabo de un tiempo preestablecido.

También cuentan con respuesta automática a una llamada y la posibilidad de que se devuelva la llamada una vez comprobado que el emisor esta autorizado para solicitarlo.

Su mayor utilidad par ala expansión de una red es para el acceso remoto e una estación de trabajo móvil.

1.10.4. Puente (Bridge).

Es un sistema formado por hardware y software que permite conectar dos redes locales entre si. Se pueden colocar en el servidor de archivos, o , mejor, en el servidor de comunicaciones.

Cuando dos redes locales necesitan comunicarse entre si, necesitan contar con un puente en cada una de ellas para poder conectarse.

Ambas redes han de usar el mismo protocolo de comunicaciones.

A diferencia de un repetidor, un puente actúa sobre los paquetes de datos o tramas que se transfieren en los niveles de enlace de datos, particularmente sobre el nivel de Control de Acceso al Medio (MAC).

Sus funciones básicas son las de autoaprendizaje, filtreado y reenvío. Es decir, si necesita reenviar un paquete de datos a una dirección de red que no esta incluida en su tabla de destinos, examina los campos de dirección del paquete (filtreado) y las dirige a la dirección que ha localizado (reenvío). A continuación, la añade a su tabla de destinos (autoaprendizaje).

La utilización de puentes para unir dos redes es mas aconsejable que la configuración de una red grande que englobe a ambas. La razón esta en que las redes van perdiendo rendimiento al aumentar el trafico y se va perdiendo tiempo de respuesta, de este modo, al estar dividida la red se reduce el trafico y el tiempo de respuesta.

Otra razón es el limite de expansión de la red grande. Todas las redes cuentan con un numero máximo de estaciones que pueden soportar; si se desea sobrepasar ese numero, la única alternativa pasa por crear otra red conectada por un puente.

1.10.5. Encaminador (Router).

Un encaminador no solo incorpora la función de filtreado característica de los puentes sino que, además, determina la ruta hacia su destino. Se utiliza tanto en redes de área local como en redes de área extensa.

Los encaminadores se diferencian de los puentes en dos aspectos:

- Actúa sobre los paquetes transferidos entre los niveles de red de las estaciones, a diferencia de los puentes que lo hacen sobre el nivel de enlace de datos
- Ambos equipos son, teóricamente, transparentes a las estaciones finales que comunican. Sin embargo, normalmente las estaciones tienen definido el encaminador al que deben dirigirse.

Se basan en la utilización de un esquema de direccionamiento jerárquico (tablas de rutas) que distinguen entre la dirección del dispositivo entre de la red y la dirección de la red. Para ello incorporan protocolos de nivel de red.

Para realizar su función incorporan algún tipo de algoritmo, siendo uno de los mas básicos el Protocolo de Información de Encaminamiento (RIP) que calcula la distancia entre el encaminador y la estación receptora de una paquete como el numero de saltos requeridos, ignorando otros tipos de atributos como el tiempo de transferencia entre dos saltos, etc.

Los protocolos de encaminamiento varían en función de las diferentes arquitecturas de comunicaciones de red existentes, por lo que se diseñan para una arquitectura especifica.

Existen algunos dispositivos que poseen características tanto de los puentes (transparencia a los protocolos con aprendizaje) como de los encaminadores (selección del camino optimo) que se denominan brouters (es la unión de bridges y routers). Este dispositivo funciona normalmente como un encaminador siempre que los protocolos de nivel superior permitan el encaminamiento. En caso contrario funcionan como puentes.

1.10.6. Pasarela (Gateway).

Es un sistema formado por hardware y software que permite las comunicaciones entre una red local y una gran computadora (mainframe) o un minicomputador (porque utilizan protocolos de nivel de transporte, sesión, presentación y aplicación distintos). Se suelen colocar en el servidor de comunicaciones.

De este modo podrá obtener datos del mini o del mainframe o bien enviarles datos para su almacenamiento.

La pasarela realiza la traducción completa entre las familias de protocolos, proporcionando una conectividad completa entre redes de distinta naturaleza.

En enlace entre ambos protocolos necesitara algún tipo de emulación que haga que la estación de trabajo imite el funcionamiento de una terminal y ceda el control al mini o al mainframe. Esta emulación se puede conseguir por medio de software (con un programa), de hardware (con una tarjeta) o de ambos.

Al igual que los encaminadores, están definidos para un determinado escenario de comunicaciones.

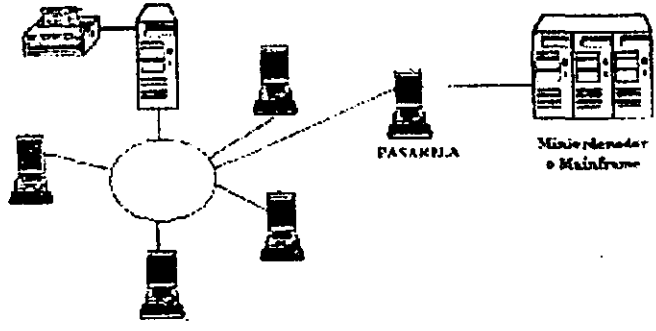


Figura 11. Representación esquemática de una red unida a un minicomputador o a un mainframe

Pero a cambio de sus ventajas, el retardo de propagación de un paquete que atraviesa una pasarela es mucho mayor que el experimentado en los otros dispositivos.

1.11. Tipos de comunicaciones.

En las redes de conmutación de paquetes existen tres formas de efectuar la comunicación de datos:

- Circuito Virtual Conmutado (CVC)
- Circuito Virtual Permanente (CVP)
- Datagrama

Un **Circuito Virtual Conmutado** (CVC) es el modo normal de conexión de terminales e indica que no existe un camino fijo entre el terminal origen y el de destino durante la comunicación, sino que los sucesivos paquetes enviados utilizan los medios de que dispone la red, conjuntamente con otros paquetes de otras comunicaciones llamadas virtuales.

Un **Circuito Virtual Permanente** (CVP) indica que existe una asociación permanente entre dos terminales, de forma que no requieren procedimientos de establecimiento o liberación de la comunicación entre ellos. Es similar a una conexión punto a punto pero virtual, ya que distintas parejas de terminales pueden compartir los mismos medios de comunicación dentro de la red, entrelazando sus paquetes de tal forma que, virtualmente, únicamente exista un circuito permanente entre ellos.

Un **datagrama** permite que cada paquete recibido por la red se entregue en la dirección de destino especificada con independencia de cualquier otro paquete que dicha terminal envíe o haya enviado formando parte del mismo mensaje.

CAPITULO II

DESCRIPCIÓN GENERAL DE LAS REDES PRIVADAS VIRTUALES

2. DESCRIPCION GENERAL DE LAS REDES PRIVADAS VIRTUALES

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

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

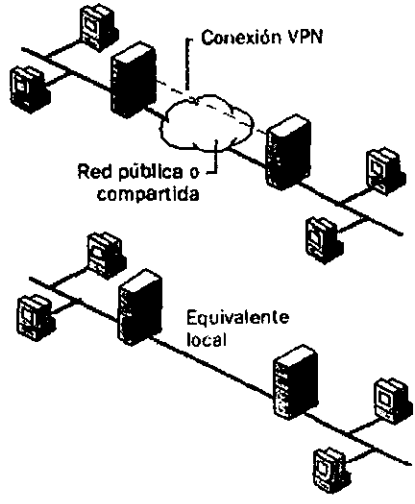


Figura 1. Red Privada Virtual (*Virtual Private Network*, VPN).

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

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

2.1. Elementos de una conexión VPN.

Una conexión VPN de Windows NT 4.0 incluye los siguientes componentes, tal como se ilustra en la **figura 2**.

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

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

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

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

Protocolos de túnel. Se utilizan para administrar los túneles y encapsular los datos privados. (Los datos que son enviados por el túnel también deben de ser encriptados para que sea una conexión VPN). Windows NT 4.0 incluye el protocolo de túnel PPTP.

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

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

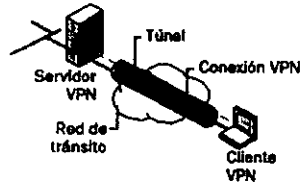


Figura 2. Componentes de una conexión VPN

2.2. Conexiones VPN.

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

2.2.1. Conexión VPN de acceso remoto.

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

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

2.2.2. Conexión VPN de enrutador a enrutador.

Una conexión VPN de enrutador a enrutador es hecha por un enrutador y conecta dos porciones de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la cual el servidor VPN está conectado.

El enrutador que llama (el cliente VPN) se autentifica a sí mismo ante el enrutador que responde (el servidor VPN), y para autentificación mutua, el enrutador que responde se autentifica a sí mismo ante el enrutador que llama.
Propiedades de la VPN.

2.3. Propiedades de la conexión VPN utilizando PPT.

- Encapsulación
- Autentificación
- Encriptación de datos

2.3.1. Encapsulación.

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

2.3.2. Autentificación.

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

2.3.3. Encriptación de datos.

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

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

Además, entre más información esté encriptada con la misma clave, más fácil es descifrar los datos encriptados.

2.4. Conexiones VPN sobre Internet.

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

2.4.1. Acceso remoto sobre Internet.

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

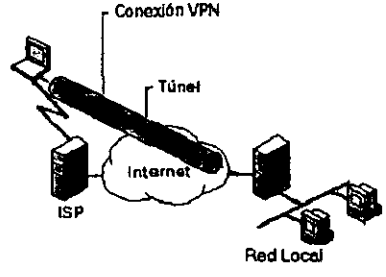


Figura 3. Ilustra el acceso remoto sobre Internet.

2.5. Administrando las redes privadas virtuales.

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

- ¿Dónde se almacenarán los datos de la cuenta del usuario?
- ¿Quién puede crear conexiones VPN?
- ¿Cómo verificará el servidor VPN la identidad del usuario que esté tratando de hacer la conexión VPN?
- ¿Cómo registrará el servidor VPN la actividad de la VPN?
- ¿Cómo puede el servidor VPN ser administrado utilizando protocolos de administración de redes e infraestructura estándar?

2.5.1. Administrando a los usuarios.

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

2.5.2. Administrando los accesos.

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

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

2.5.3. Administrando la autentificación.

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

2.5.4. Autentificación de Windows NT 4.0 .

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

2.5.5. Administración de red.

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

CAPITULO III

PROTOCOLO DE TUNEL PUNTO A PUNTO

3. PROTOCOLO DE TUNEL PUNTO A PUNTO.

El Protocolo de Túnel Punto a Punto (*Point-to-Point Tunneling Protocol*, PPTP) encapsula los paquetes (*frames*) del Protocolo Punto a Punto (*Point-to-Point Protocol*, PPP) con datagramas IP para transmitirlos por una red IP como Internet.

El PPTP utiliza una conexión TCP conocida como la conexión de control de PPTP para crear, mantener y terminar el túnel, y una versión modificada de la Encapsulación de Enrutamiento Genérico (*Generic Routing Encapsulation*, GRE) para encapsular los paquetes (*frames*) PPP como datos para el túnel. Las cargas de los paquetes encapsulados pueden estar encriptadas o comprimidas o ambas cosas.

El PPTP supone la disponibilidad de una red IP entre un *cliente PPTP* (un cliente de túnel que utiliza el protocolo PPTP) y un *servidor PPTP* (un servidor de túnel que utiliza el protocolo PPTP). El cliente PPTP podría estar ya conectado a una red IP por la que puede tener acceso al servidor PPTP, o el cliente PPTP podría tener que llamar telefónicamente a un servidor de acceso de red (*Network Access Server*, NAS) para establecer la conectividad IP como en el caso de los usuarios de accesos telefónicos para Internet.

La autentificación que ocurre durante la creación de una conexión VPN con PPTP utiliza los mismos mecanismos de autentificación que las conexiones PPP, tales como el Protocolo de Autentificación Extendible (*Extensible Authentication Protocol*, EAP), el Protocolo de Autentificación con Reto/Negociación de Microsoft (Microsoft *Challenge-Handshake Authentication Protocol*, MS-CHAP), el CHAP, el Protocolo de Autentificación de Claves Shiva (*Shiva Password Authentication Protocol*, SPAP) y el Protocolo de Autentificación de Claves (*Password Authentication Protocol*, PAP). El PPTP hereda la encriptación, la compresión o ambas de las cargas PPP del PPP. Para Windows NT 4.0, debe de utilizarse Seguridad de Nivel de Transporte EAP (*EAP-Transport Level Security*, EAP-TLS) o MS-CHAP para que las cargas PPP sean encriptadas utilizando la Encriptación Punto a Punto de Microsoft (Microsoft *Point to Point Encryption*, MPPE).

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

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

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

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

Esto incluye la transmisión periódica de mensajes *PPTP Echo_Request* y *PPTP Echo_Reply* para detectar fallas en la conexión entre el cliente y el servidor PPTP. Los paquetes de control de conexión PPTP consisten de una cabecera IP, una cabecera TCP y un mensaje de control PPTP como se ilustra en la **figura 1**. El paquete de control de conexión PPTP en la figura 7 también incluye una cabecera de la capa de enlace de datos y una cola.

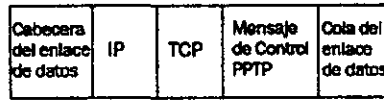


Figura 1. Paquete de control de conexión PPTP

La **tabla 1** lista los principales mensajes de control PPTP que son enviados sobre la conexión de control PPTP. Para todos los mensajes de control, el túnel PPTP específico es identificado por la conexión TCP.

Tabla 1. Mensajes de administración y control de llamada del PPTP

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

3.2. Envio de datos con PPTP.

El envío de datos con PPTP se logra con múltiples niveles de encapsulación.

La **figura 2.** Muestra la estructura resultante de los datos enviados por el túnel de PPTP.

Figura 2. Datos del túnel PPTP.

3.3. Encapsulación del paquete PPP.

La carga inicial PPP es encriptada y comprimida con una cabecera PPP para crear un paquete (*frame*) PPP. El paquete PPP es luego encapsulado con una cabecera GRE modificada. El GRE fue diseñado para proporcionar mecanismos de propósito general, ligeros y simples, para encapsular datos sobre redes IP. El GRE es un protocolo cliente de IP que usa el protocolo IP 47.

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

- Un bit de confirmación (*acknowledgement bit*) que es utilizado para indicar que un campo de confirmación de 32 bits está presente y es significativo.
- El campo de clave (*key*) es reemplazado con un campo de Longitud de Carga (*Payload Length*) de 16 bits y un campo de identificación de llamada (*Call ID*). El campo de identificación lo establece el cliente PPTP durante la creación de un túnel PPTP.
- Se agrega un campo de confirmación de 32 bits.

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

3.4. Encapsulando el paquete GRE.

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

3.4.1. Encapsulación de en la capa del enlace de datos.

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

3.5. Procesamiento de los datos enviados con PPTP.

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

1. Procesa y elimina la cabecera y la cola del enlace de datos.
2. Procesa y elimina la cabecera IP.
3. Procesa y elimina las cabeceras GRE y PPP.
4. Desencripta, descomprime, o ambas, la carga PPP (si se requiere).
5. Procesa la carga para recepción o reenvío.

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

La **figura 3**. ilustra el camino que toman los datos enviados por el túnel a través de la arquitectura de redes de Windows NT 4.0 desde un cliente VPN en una conexión VPN de acceso remoto utilizando un módem analógico. Los siguiente pasos describen el proceso:

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

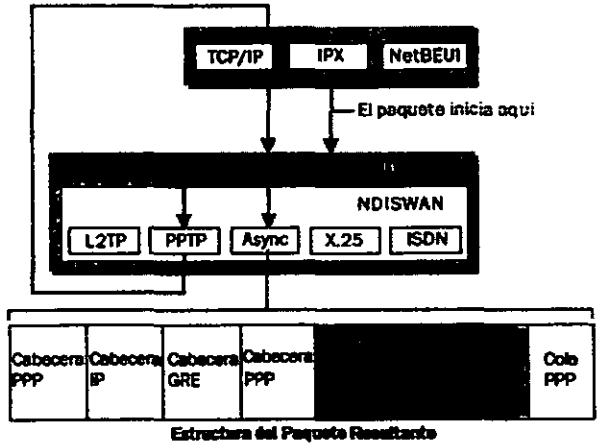


Figura 3. Desarrollo del paquete PPTP

CAPITULO IV

SEGURIDAD DE LAS VPN´S

4. SEGURIDAD DE LAS VPNS.

La seguridad es una parte importante de una VPN. En las siguientes secciones se describe las funciones de seguridad de las conexiones VPN con PPTP.

4.1. Conexiones PPTP.

PPTP ofrece autentificación de usuario y encriptación.

4.2. Autentificación de usuario con PPP.

El usuario que intenta hacer una conexión PPTP es autentificado utilizando protocolos de autentificación para PPP tales como MS-CHAP, CHAP, SPAP y PAP. Para conexiones PPTP, es altamente recomendable usar MS-CHAP versión 2 ya que proporciona autentificación mutua y es el método más seguro de intercambiar credenciales.

4.3. Encriptación con MPPE.

PPTP hereda la encriptación MPPE, la cual utiliza el cifrador de flujos (*streams*) RSA RC4. El MPPE está disponible solamente cuando se utiliza el protocolo de autentificación MS-CHAP (versión 1 o versión 2).

El MPPE puede utilizar claves de encriptación de 40 o de 128 bits. La clave de 40 bits está diseñada para uso internacional y se adhiere a las leyes de exportación de encriptación de los Estados Unidos. La clave de 128 bits está diseñada para su uso en Norte América. Por defecto, la clave que ofrece la mayor seguridad que soporten el cliente y el servidor VPN es la que se negocia durante el establecimiento de la conexión. Si el servidor VPN requiere una clave que ofrezca mayor seguridad que la que soporta el cliente VPN, el intento de conexión es rechazado.

El MPPE fue originalmente diseñado para encriptación a través de enlaces punto a punto donde los paquetes llegaban en el mismo orden en que eran enviados con poca pérdida de paquetes. Para este ambiente, la desencriptación de cada paquete depende de la desencriptación del paquete anterior.

Sin embargo, para los VPNs, los datagramas IP enviados a través de Internet pueden llegar en un orden diferente al que fueron enviados. Por lo tanto, el MPPE para las conexiones VPN cambia la clave de encriptación para cada paquete. La desencriptación de cada paquete es independiente del paquete previo. El MPPE incluye una secuencia de números en la cabecera MPPE. Si los paquetes se pierden o llegan en desorden, las claves de encriptación son cambiadas en relación al número de secuencia.

4.4. Filtreado de paquetes PPTP.

Un servidor VPN sobre PPTP típicamente tiene dos interfaces físicas: una interface hacia la red pública o compartida como Internet y otra a la red local. También tiene una interface virtual conectada a todos los clientes VPN. Para que el servidor VPN redirecciones el tráfico entre los clientes VPN, el redireccionamiento IP (IP forwarding) debe estar activado en todos los clientes. Sin embargo, la activación del redireccionamiento entre dos interfaces físicas provoca que el servidor VPN enrute todo el tráfico IP desde la red pública o compartida hacia la intranet. Para proteger a la intranet del tráfico que no es enviado al cliente VPN, debe de configurarse el filtreado de paquetes PPTP (*PPTP packet filtering*) para que el servidor solamente aplique el enrutamiento entre clientes VPN y la intranet, y no entre usuarios potencialmente mal intencionado en la red pública o compartida y la intranet.

El filtreado de paquetes PPTP puede configurarse en el servidor VPN.

CAPITULO V

DIRECCIONAMIENTO PARA VPN´S

5. DIRECCIONAMIENTO PARA VPNS.

Para comprender cómo funcionan las VPNs, debemos entender cómo se afecta el direccionamiento (*addressing*) y el enrutamiento (*routing*) para la creación de VPNs de acceso remoto y de VPNs de enrutador a enrutador. Una conexión VPN crea una interface virtual que debe de ser asignada a una dirección IP apropiada, y se deben de cambiar o agregar rutas para asegurar que el tráfico apropiado sea enviado a través de la conexión VPN segura, en lugar de ser enviado por la red de tránsito pública o compartida.

5.1. Conexiones VPN de acceso remoto.

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

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

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

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

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

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

Un ejemplo del direccionamiento de un cliente de acceso telefónico se muestra en la **figura 1.**, donde la organización utiliza direcciones privadas en al red local y los datos enviados por el túnel están dentro de un datagrama IP.

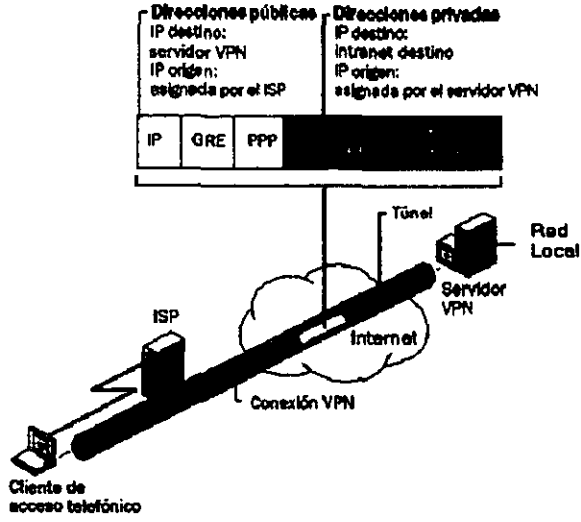


Figura 1. Direccionamiento público y privado en los datos del túnel PPTP.

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

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

5.4. Rutas por defecto y las VPN sobre Internet.

Cuando el cliente de acceso telefónico llama al ISP, agrega una ruta por defecto utilizando la conexión al ISP como se muestra en la **figura 2**. En este punto, puede accesar todas las direcciones de Internet a través del enrutador en el NAS del ISP.

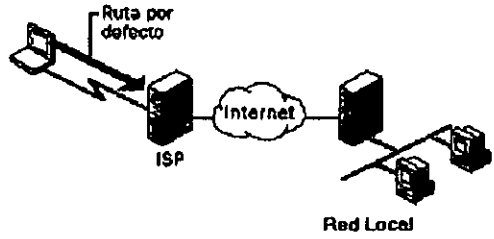


Figura 2. Ruta por defecto creada cuando se llama al ISP.

Una vez que el cliente VPN crea la conexión VPN, se agrega otra ruta por defecto y una ruta al servidor hacia la dirección IP del servidor del túnel, como se ilustra en la **figura 3**. La ruta por defecto previa es grabada pero ahora tiene una métrica superior. El agregar la nueva ruta por defecto significa que todas las direcciones de las localizaciones de Internet, excepto la dirección IP del servidor del túnel, no estarán accesibles mientras dure la conexión VPN.

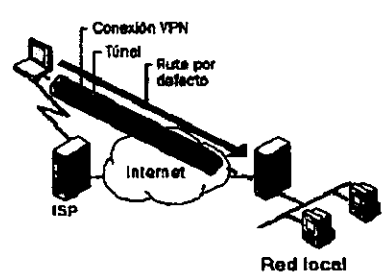


Figura 3. Ruta por defecto creada cuando se inicia la VPN.

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

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

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

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

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

5.5. Direcciones publicas.

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

5.6. Direcciones privadas.

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

En cada uno de estos casos, las rutas estáticas persistentes para los IDs de la red de la intranet necesitan ser agregadas al cliente VPN. Una vez que las rutas persistentes sean agregadas, se grabarán en el registro de configuraciones (*registry*). Con Microsoft® Windows NT® versión 4.0 Service Pack 3 o superior y con Windows NT 4.0 las rutas persistentes no son en realidad agregadas a la tabla de enrutamiento IP (y no son visibles con el comando **route print** en la interface de comandos de Windows NT

4.0) hasta que la dirección IP del *gateway* sean accesibles. La dirección IP del *gateway* estará accesible cuando se haga la conexión VPN.

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

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

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

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

CAPITULO VI

RESOLUCIÓN DE PROBLEMAS DE LAS VPN´S

6. RESOLUCIÓN DE PROBLEMAS DE LAS VPNS.

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

6.1. Problemas comunes de las VPNS .

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

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

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

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

- Usando el comando ping, verificar que el nombre del servidor o la dirección IP del servidor VPN es accesible. Si se está usando el nombre del servidor, verifique que el nombre del servidor es convertido a su dirección IP correcta. Si el comando ping no tiene éxito, el filtreado de paquetes del Protocolo de Mensajes de Control de Internet (*Internet Control Message Protocol*, ICMP) podría estar evitando el paso de los mensaje ICMP hacia y desde el servidor VPN.
- Verificar que el Servicio de Acceso Remoto o el Servicio de Acceso Remoto y Enrutamiento estén siendo ejecutados en el servidor VPN.
- Verificar que todos los puertos PPTP en el servidor VPN no estén ya siendo utilizados. Si es necesario, configurar las propiedades del Protocolo de Túnel Punto a Punto en **Control Panel-Network** y cambie el número de puertos PPTP para permitir más conexiones concurrentes.

- Verificar que el cliente VPN y el servidor VPN estén configurados para usar parámetros de autentificación comunes.
- Verificar que el cliente VPN y el servidor VPN estén configurados con parámetros de encriptación comunes.
- Verificar que los protocolos de la LAN que estén siendo usados por los clientes estén habilitados para acceso remoto.
- Verificar que las credenciales de los clientes que consisten de nombre de usuario, clave y nombre del dominio estén correctas y puedan ser validadas por el servidor VPN.
- Verificar que la cuenta de usuario correspondiente a las credenciales del usuario del cliente VPN tengan permiso de acceso telefónico.
- Verificar la configuración del agente de autentificación. Un servidor VPN con RRAS puede ser configurado para utilizar a Windows NT 4.0 o a RADIUS para autentificar las credenciales del cliente de acceso remoto.
- Para conexiones VPN de acceso remoto, verifique que los puertos PPTP estén configurados para recibir llamadas.

6.3. No se puede esablecer un túnel.

- Verificar que el filtreado de paquetes en la interface de algún enrutador entre el cliente y el servidor VPN no esté evitando la redirección del tráfico del protocolo de túnel. En un servidor VPN con Windows NT 4.0, el filtreado de paquetes IP puede configurarse desde las propiedades avanzadas TCP/IP y desde la herramienta **Administrador de RAS y Enrutamiento** (Routing and RAS Admin). Revisar ambas cosas en busca de filtros que podrían estar excluyendo e tráfico de la VPN
- Verificar que el cliente Windows Proxy no esté ejecutándose actualmente en el cliente VPN. Cuando el cliente Windows Proxy está activo, las llamadas al API de WinSocks que son utilizadas para crear túneles y enviar datos por el túnel son interceptadas y redirigidas al servidor proxy configurado. Una computadora con un servidor proxy permite a la organización accesar tipos específicos de recursos de Internet (generalmente Web y FTP) sin conectar directamente a esa organización a Internet. La organización puede utilizar identificadores de red IP privadas asignadas por InterNIC (tales como 10.0.0.0). Los servidores proxy son generalmente utilizados para que los usuarios privados en una organización puedan tener acceso a recursos públicos en Internet como si estuvieran directamente conectados a Internet. Las

conexiones VPN son utilizadas generalmente para que usuarios autorizados en Internet tengan acceso a los recursos privados de la organización. Una sola computadora puede actuar como servidor proxy (para los usuarios privados) y servidor VPN (para los usuarios autorizados en Internet) para facilitar ambos intercambios de información.

6.4. Herramientas para resolución de problemas.

Las siguientes herramientas, con las que puede recolectar información adicional acerca de la causa de su problema con la VPN, están incluidas con Windows NT 4.0.

6.4.1. Monitor de Red.

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

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

6.4.2. Registro y rastreo PPP.

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

CAPITULO VII

INSTALACIÓN, CONFIGURACIÓN Y PUESTA A PUNTO DE UNA CONEXIÓN VPN

CAPÍTULO VII

7. INSTALACIÓN, CONFIGURACIÓN Y PUESTA APUNTO DE UNA CONEXIÓN VPN

7.1. Conceptos Básicos :

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

7.2. Instalación y configuración de PPTP sobre un servidor.

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

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

- El servidor Windows NT, deberá tener instalada la versión 4.0.
- Uno o mas adaptadores de red instalados. En muchos casos, dos o más adaptadores de red son requeridos: uno para conectarse a Internet y uno o más para conectarse a la red de la empresa.
- El TCP/IP deberá estar instalado y conectado dentro del adaptador de red hacia la red privada de la empresa, y el adaptador conectado a Internet.
- El protocolo de red usado en la red privada de la empresa, (TCP/IP, NetBEUI, o IPX) debe estar instalado y cargado al adaptador(es) conectados hacia la red privada de la empresa.
- El servidor PPTP estará configurado con una dirección IP estática.
- RAS, con llamada automática (dial-up) de red, estará instalada y configurada.
- El numero de conexiones simultaneas con clientes PPTP remotos que prestara el servidor PPTP, por lo tanto se deberá configurar el numero correcto de dispositivos VPN.

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

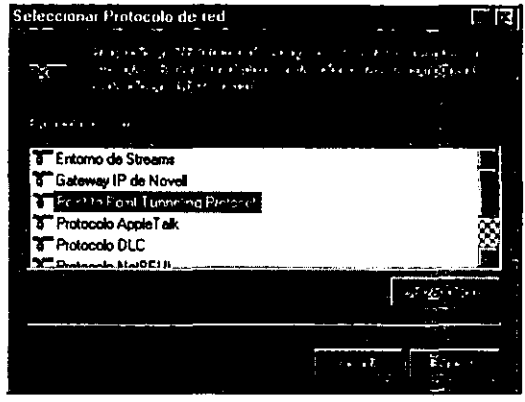
Implica tres procedimientos principales:

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

7.3.1. Instalación de PPTP sobre un servidor PPTP.

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

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



- Seleccionar la opción de **Protocolo Punto por Punto** y hacer **click** en **Aceptar.**
- Escribir el drive y la ubicación del directorio de los archivos de instalación de tu Servidor Windows NT versión 4.0 en el **Setup de Windows NT** en el cuadro de dialogo, y posteriormente hacer **click** en **Continuar.** Los archivos del PPTP serán copiados desde el directorio de instalación, y aparecerá el cuadro de dialogo de Configuración de PPTP, tal como se muestra en la siguiente figura:

- Hacer **click** en la flecha del **Numero de Red Privada Virtual**, para seleccionar el numero de VPNs simultaneas que se desee que soporte el servidor. Se puede seleccionar un numero entre un rango de 1 y 256. Normalmente, las VPNs múltiples son instaladas en un servidor PPTP para habilitar los cliente múltiples que se conectan simultáneamente al servidor PPTP. El servidor puede ser configurado para soportar como un numero máximo de 256 simultaneas conexiones VPN .
- Hacer **click** en **Aceptar**, y otra vez en **Aceptar** en el cuadro de dialogo de **Setup Message.**
- En el cuadro de dialogo del **Setup de Acceso Remoto**, se podra hacer mas tarde lo siguiente:

a) Temporalmente para la instalación de PPTP haciendo **click** en **Cancelar**, cerrando **Red**, y apagar o reiniciar la computadora. Nótese que se deberá ejecutar el procedimiento que se describe en la siguiente sección "adicionar los Dispositivos VPN tal como los puertos RAS sobre un servidor PPTP" para completar la instalación de PPTP.
b) Continuar la instalación de PPTP haciendo **click** en **Adicionar** para adicionar los dispositivos VPN instalados con PPTP para RAS. (Ver el paso 5 del siguiente procedimiento).

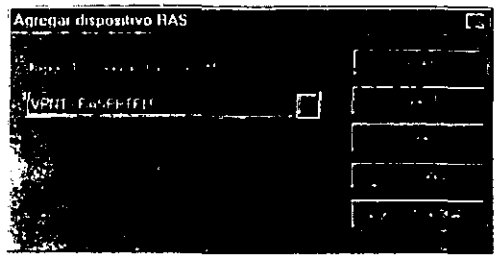
7.3.2. Adicionar un dispositivo VPN como puerto RAS sobre un servidor PPTP.

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

Para configurar dispositivos VPN sobre un servidor PPTP.

1. Hacer **click** en **Inicio**, en la opción **Configuración**, seleccionar **Panel de Control.**
2. Hacer doble **click** en el icono de **Red** dentro del **Panel de Control.**

3. Hacer **click** en la opción de **Servicios** y seleccionar **Servicio de Acceso Remoto.**
4. Hacer **click** en **Propiedades** para desplegar el cuadro de dialogo de **Instalación de Acceso Remoto.**
5. Hacer **click** en **Adicionar**. Aparecerá el cuadro de dialogo de **adicionar dispositivo RAS**, tal como se muestra en la siguiente figura:



6. Hacer **click** en **Dispositivos de RAS Cargados** y en la flecha que despliega la lista de dispositivos VPN, los cuales podrán ser adicionados y configurados como un puerto y dispositivo dentro del RAS.
7. Seleccionar un dispositivo VPN y hacer **click** en **Aceptar.** Repetir los pasos 5, 6 y 7 hasta que todos las VPNs sean adicionadas al cuadro de dialogo de **Instalación de Acceso Remoto**.
8. Seleccionar un puerto VPN y hacer **click** en **Configurar.** Verificar que la opción de **Llamadas solamente Recibidas** en el cuadro de dialogo de **Puerto Usado**, este seleccionada y hacer **click** en **Aceptar** para regresar al cuadro de dialogo de **Instalación de Acceso Remoto**. (Si también se desea usar este servidor como un cliente PPTP y se quiera usar el dispositivo VPN para hacer llamadas al exterior como un dispositivo PPTP, selecciona Llamadas-Exterior –**Dial-Out**-).
9. Repetir el ultimo paso para cada dispositivo VPN que se vaya desplegando en el cuadro de dialogo de **Instalación de Acceso Remoto**. (De hecho, los dispositivo VPN en una computadora con Windows NT Server versión 4.0, son configurados automáticamente con la opción de **Llamadas Recibidas Unicamente**, pero se debería verificar esta configuración adicionalmente.)
10. Hacer **click** en **Red** para que se despliegue el cuadro de dialogo de **Configuración de Red**. Verificar que se reconozca el TCP/IP dentro del cuadro de **Configuración de Servidor** en el cuadro de dialogo de **Configuración de Red**. Hacer **click** en

Aceptar para regresar al cuadro de dialogo de **Instalación de Acceso Remoto.**

11. Hacer **click** en **Continuar**.
12. Cerrar **Red**, salir de esta opción y reiniciar la maquina.

7.3.3. Configuración de las opciones de Encripacion y autentificación en un servidor PPTP.

Este apartado incluye procedimientos e información acerca de la configuración de un servidor PPTP. Estos son los 3 principales pasos:

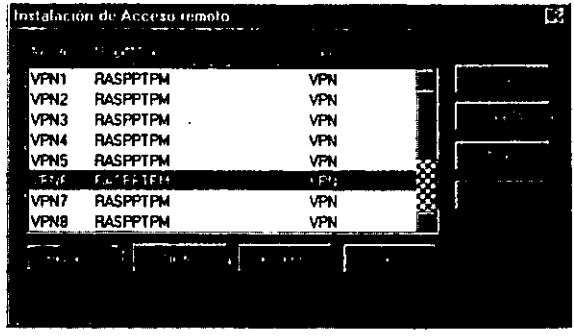
- Encriptamiento de datos enviados sobre Internet.
- Aceptación de paquetes PPTP únicamente, desde Internet.
- Acceso a Redes Privadas.
- Habilitar el traspaso de IP.

7.3.3.1. Configuración de encriptamiento en el servidor para PPTP.

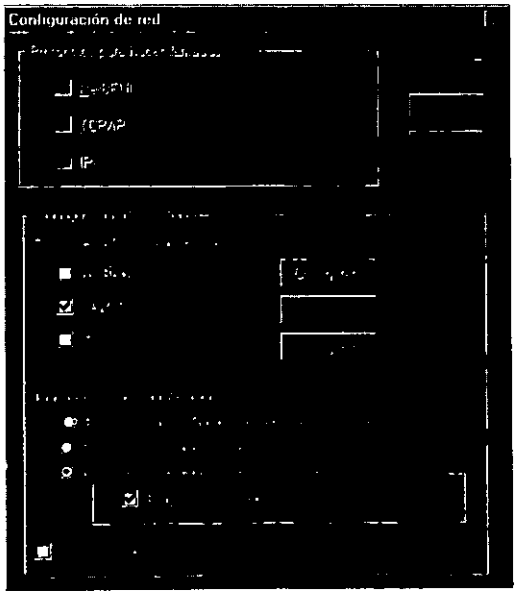
El encriptamiento de datos se instala por medio del protocolo de acceso remoto, PPP. Se puede habilitar el encriptamiento con la configuración de cada dispositivo VPN que anteriormente se haya adicionado y configurado en el RAS. Esta configuración es idéntica a la configuración de encriptamiento para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

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

1. Hacer **click** en **Inicio**, en la opción **Configuración**, seleccionar **Panel de Control.**
2. Hacer doble **click** en el icono de **Red** dentro del **Panel de Control.**
3. Hacer **click** en la opción de **Servicios** y seleccionar **Servicio de Acceso Remoto.**
4. Hacer **click** en **Propiedades** para desplegar el cuadro de dialogo de **Instalación de Acceso Remoto** (mostrada a continuación).



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



6. Seleccionar las opciones de **Autentificacion-Encriptado requeridas por Microsoft** y **Encriptamiento de Datos Requeridos**. Esta configuraciones de RAS y PPP son basadas

en Windows NT autentificación de todos los clientes remotos conectándolos al servidor PPP.
7. Hacer **click** en **Aceptar** para regresar al cuadro de dialogo de **Instalación de Acceso Remoto**.
8. Hacer **click** en **Continuar**.
9. Cerrar **Red**, salir de esta opción y reiniciar la maquina.

7.3.3.2. Configuración del filtreado en un servidor PPTP.

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

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

7.3.3.3. Configuración de enrutamiento LAN en un servidor PPTP.

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

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

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

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

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

Deberán ser establecidas los enrutamientos estáticos para la red privada.

7.3.3.4. Habilitar el traspaso de IP.

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

Para habilitar el traspaso IP

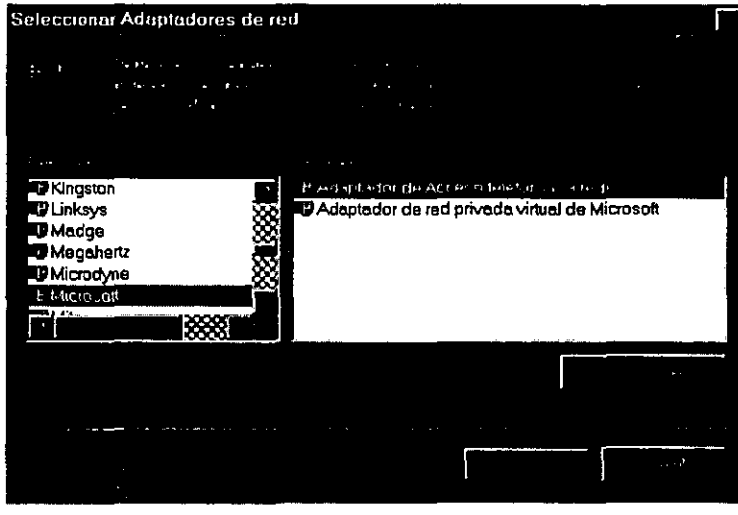
1. Hacer **click** en Inicio, en **Configuración**, y **click** en Panel de Control.
2. Doble **click** en **Red** dentro del **Panel de Control**.
3. **Click** en la opción de **Protocolos**, seleccionar TCP/IP y hacer **click** en **Propiedades**.
4. **Click** en la opción **Routing**, y hacer **click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

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

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

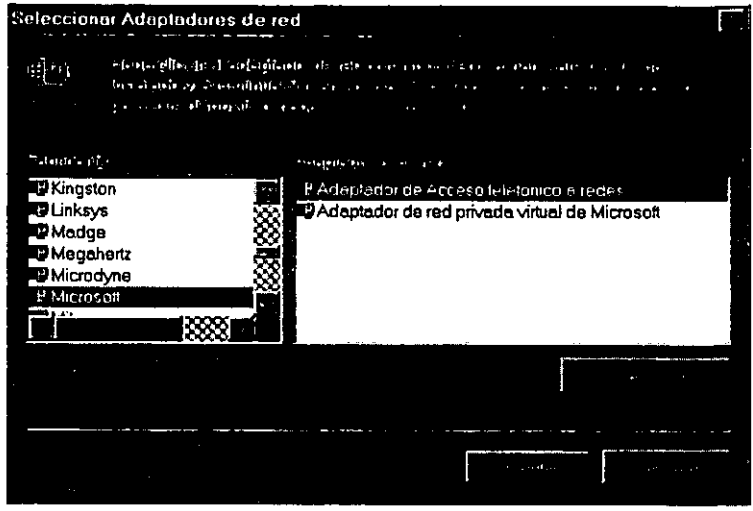
Para instalar el adaptador VPN en una computadora trabajando con Windows 98.

1. **Click Inicio**, en el punto de **Configuración**, y **click** en el **Panel de Control**.
2. Doble **click** en **Red** dentro de **Panel de Control.**
3. **Click** en la opción de **Agregar**, y **click** en **Adaptador** para desplegar la caja de dialogo. El cuadro de dialogo del **Adaptador de Red Seleccionado** se ilustra en la siguiente figura:

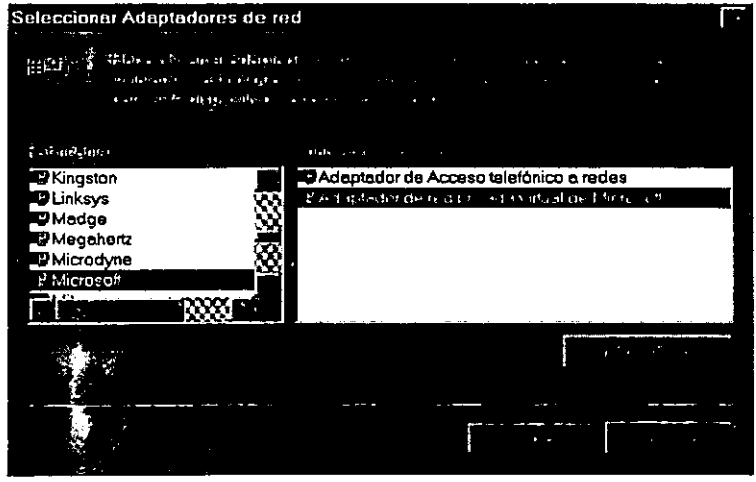


4. Seleccionar la opción de **Adaptador de Acceso telefónico a redes** y hacer **click** en **Aceptar.**

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



6. Seleccionar la opción de **Adaptador de Acceso telefónico a redes #2 (Compatibilidad con VPN) y** hacer **click** en **Aceptar.**
7. **Click** en la opción de **Agregar**, y **click** en **Adaptador** para desplegar la caja de dialogo. El cuadro de dialogo del **Adaptador de Red Seleccionado** se ilustra en la siguiente figura:



8. Seleccionar la opción de **Adaptador de red privada virtual de Microsoft** y hacer **click** en **Aceptar.**
9. **Click en Aceptar** y Reiniciamos la maquina.

7.5 Configuración de acceso telefónico a redes con Windows 98.

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

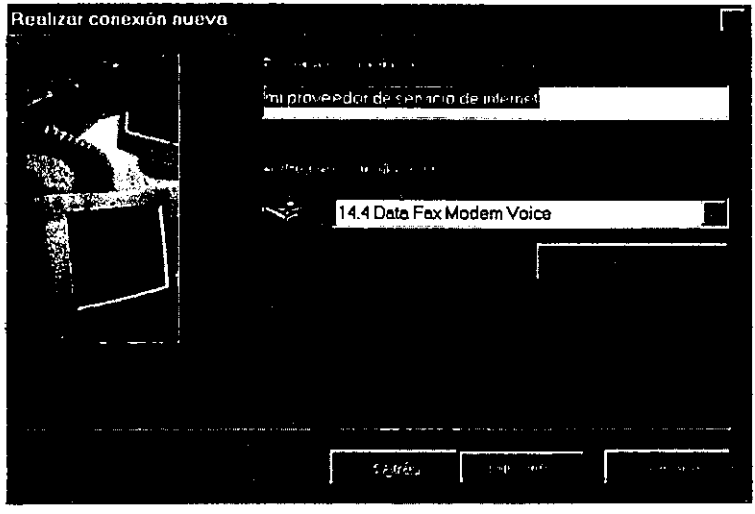
Los siguientes procedimientos describen como usar una conexión telefónica a la red para configurar una conexión ISP y una PPTP.

7.5.1. Creando la conexión para el ISP.

Si se esta usando un PPTP y una conexión telefónica a la red para conectarte al servidor PPTP con Internet, se necesita crear una conexión al ISP.

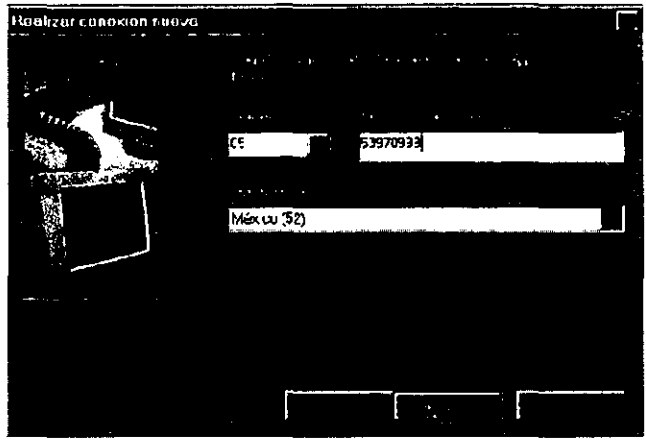
Para crear una nueva entrada ISP con el uso del asistente para hacer una nueva conexión.

1. Hacer **click** en **Inicio**, en **Programas**, en **Accesorios**, y hacer **click** en **Acceso Telefónico a Redes**. Aparecerá la ventana de **Acceso Telefónico a Redes**.
2. Hacer **click** en **Realizar Conexión**. Aparecerá el asistente para **Realizar una nueva conexión.**
3. Hacer **click** en **Siguiente**. Aparecerá la siguiente pantalla

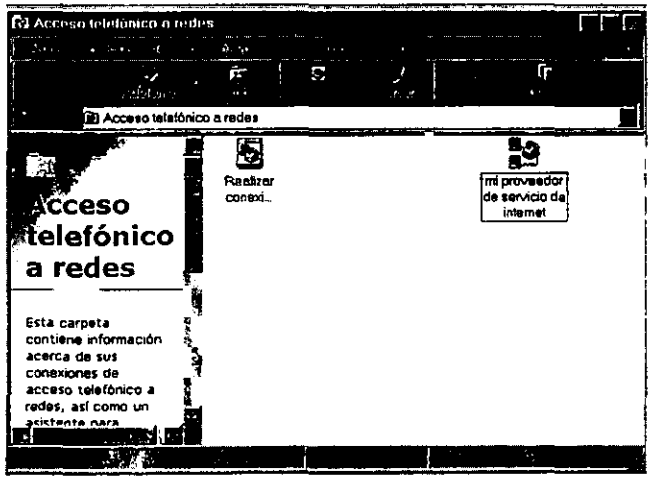


4. Se escribe el nombre para la conexión, en **Escriba un nombre para el equipo al que esta llamando.**

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



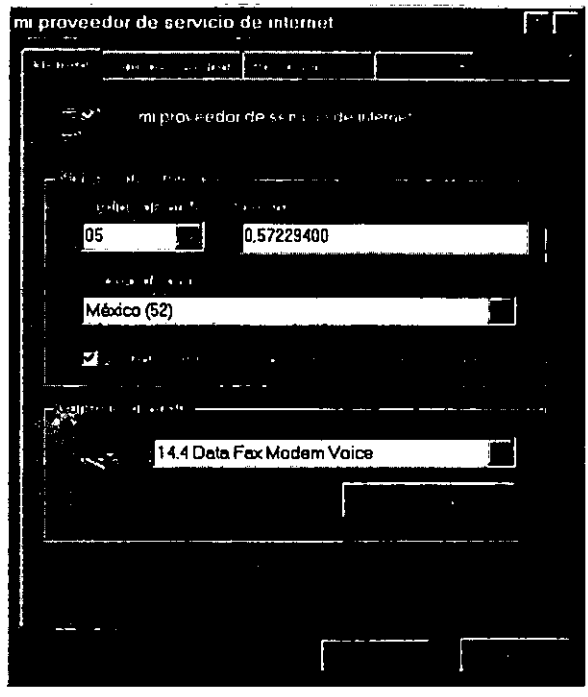
6. Escribe el numero de teléfono del ISP en **Numero de Teléfono**.
7. Hacer **click** en **Siguiente**, y después en **Finalizar**. Un icono de conexión se ha creado en la carpeta **de Acceso Telefónico a Redes**, tal como se muestra en la siguiente figura.



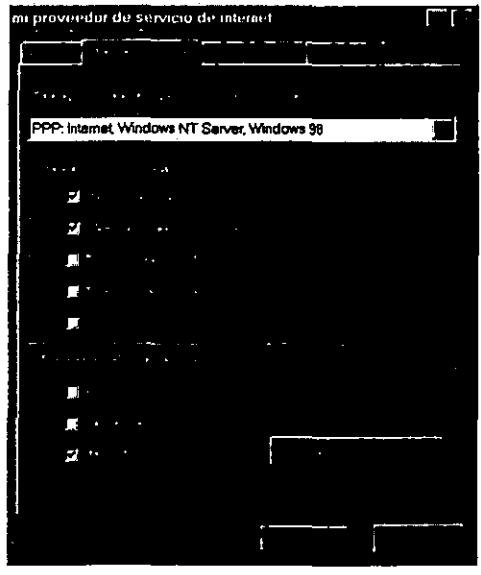
8. Verificar la conexión, usando el siguiente procedimiento.

7.5.2. Verificar o editar la conexión ISP.

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



2. Revisar la información dentro de la pestaña de **General** para asegurar de que el numero de teléfono sea el correcto y que el módem o dispositivo ISDN seleccionado también sea el correcto. De lo contrario hacer los cambios necesarios.
3. Hacer **click** en la pestaña de **Tipos de Servidor**. Esta pestaña se ilustra en la siguiente figura.



4. Revisa la información que contiene la pestaña **de Tipos de Servidor**.
5. Que el cuadro de Acceso telefónico por tipo de servidor, despliegue lo siguiente: **"PPP: Internet, Windows NT Server, windows 98"**.
6. En el cuadro de Opciones Avanzadas, borra el login de acceso a red que se encuentra en el cuadro. No es necesaria una conexión ISP para esta opción, aun borrando el login, puede realizarse la conexión mas rápidamente.

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

7. En el cuadro **de Protocolos de red Admitidos**, asegúrarse de que el TCP/IP este seleccionado y que los otros protocolos de red no estén seleccionados. Cancelando la selección de los otros protocolos de red, se habilita la conexión del ISP mas rápidamente.
8. Hacer **click** en Configuración de TCP/IP se despliega el cuadro de dialogo de Configuración de PPP y TCP/IP. Asegúrarse que la instalación del TCP/IP este conformada por las configuraciones requeridas por el proveedor de ISP.

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

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

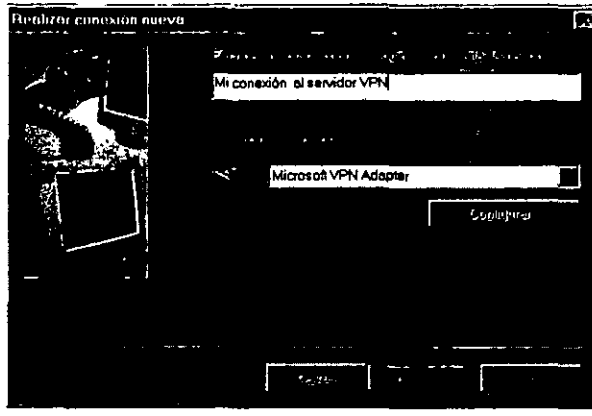
9. **Hacer click en Aceptar.**

7.6. Creando la conexión al servidor PPTP.

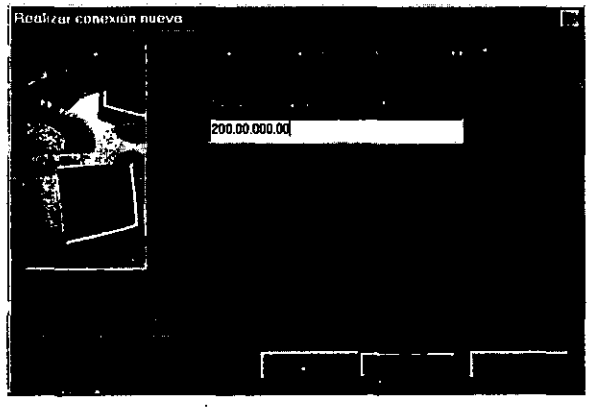
Se deberá crear la conexión al servidor PPTP usando un dispositivo VPN

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

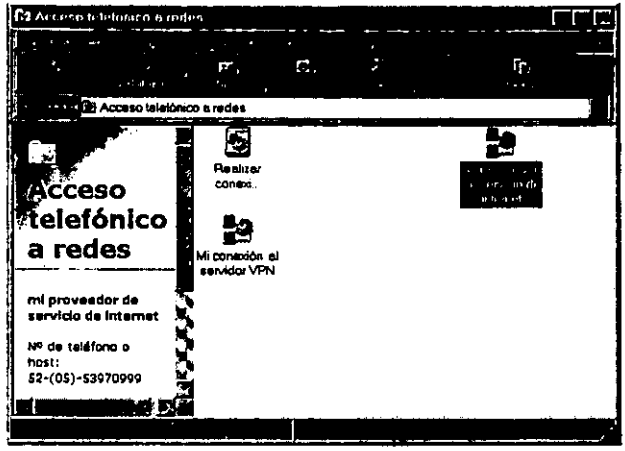
1. Hacer **click** en Inicio, en **Programas**, en **Accesorios**, y hacer **click** en **Acceso Telefónico a Redes**. Aparecerá la ventana de **Acceso Telefónico a Redes**.
2. Hacer **click** en la ventana de **Hacer una conexión nueva**. Aparecerá el asistente para Realizar una **Conexión Nueva**, tal como se ilustra en la siguiente figura.



3. Escribir el nombre de la conexión del servidor PPTP en el cuadro de Escribe un nombre para la computadora a la que deseas enlazarte.
4. Selecciona el Adaptador de Microsoft VPN en la caja de **Seleccionar un Dispositivo** y hacer **click** en **Siguiente**. Aparecerá el siguiente cuadro de dialogo.



5. Dentro del cuadro del **Nombre del Host y dirección IP**, escribe el nombre o dirección IP del servidor PPTP que este conectado a Internet.
6. Hacer **click** en **Siguiente**, y después hacer **click** en **Finalizar**. Un icono de conexión se ha creado en la carpeta **de Acceso Telefónico a Redes**, así como se ilustra en la siguiente figura:



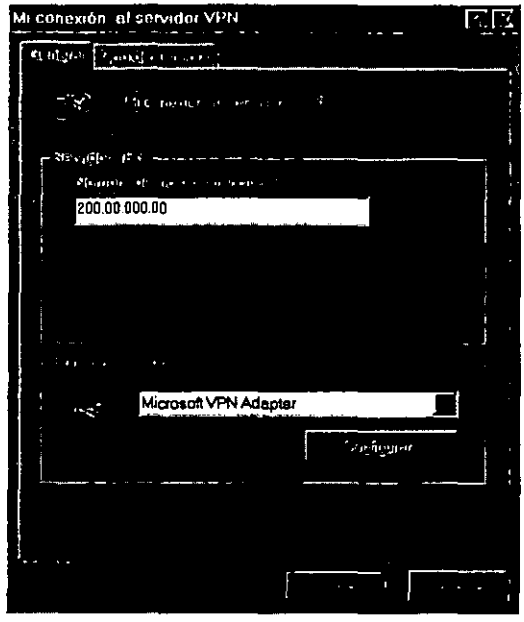
7. Verificar que la conexión del servidor PPTP este usando el siguiente procedimiento.

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

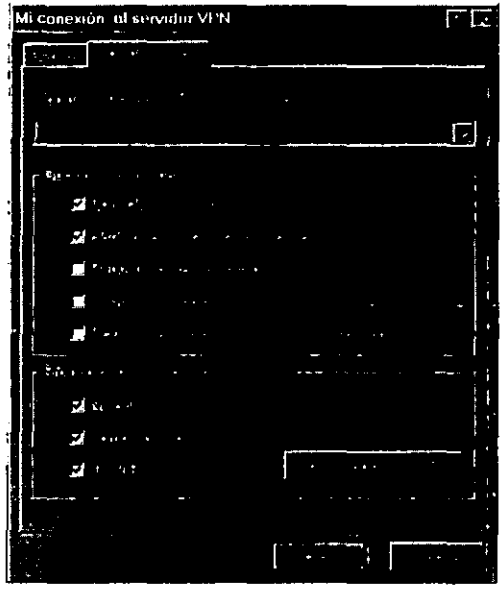
7.6.1. Para verificar o editar la conexión al servidor PPTP.

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

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



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



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

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

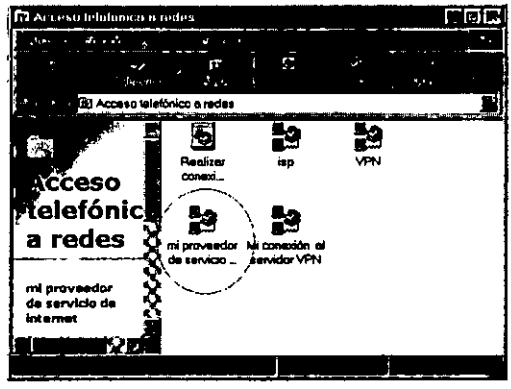
5. En el cuadro de protocolos de red admitidos, asegúrarse de que los protocolos de red usados en la la Red local estén seleccionados.

6. Si se usa el protocolo TCP/IP en la red privada, hacer **click** en Configuración de TCP/IP para que se despliegue el cuadro de Configuración de TCP/IP. Asegúrarse de que la configuración del TCP/IP este conformado por las configuraciones requeridas por un cliente.

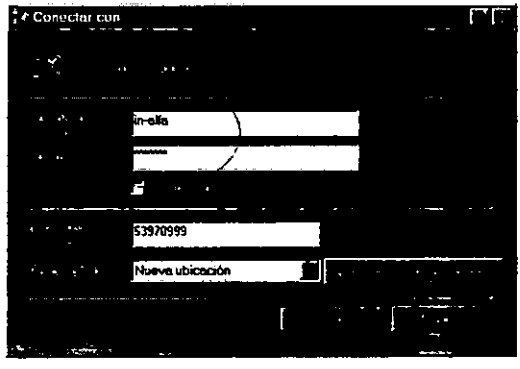
7. Hacer **click** en **Aceptar**.

7.7. Conectando al Servidor VPN.

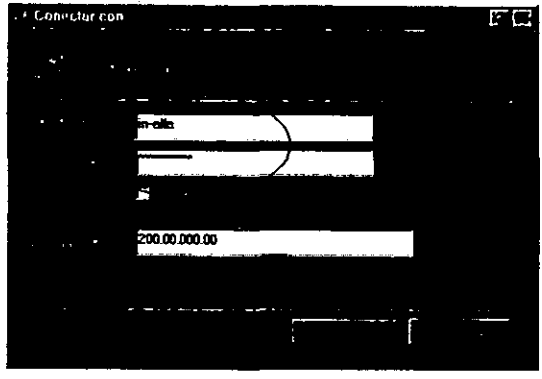
Primero , necesitamos conectarnos al ISP :



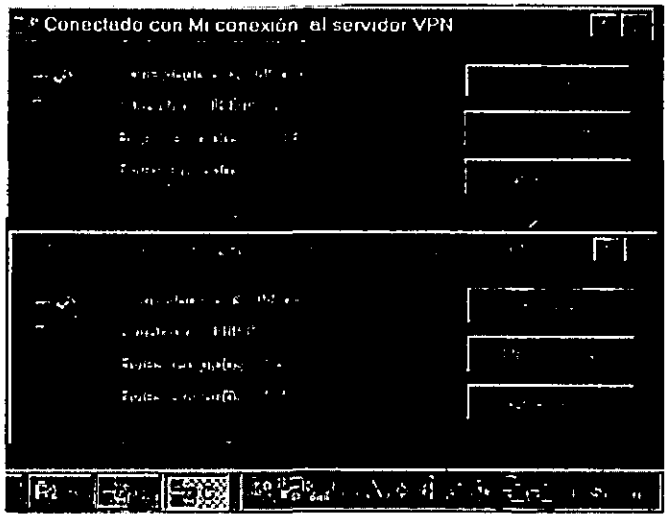
1 . Hacer **click** a **"mi proveedor de servicio de internet"** , debemos contar con una cuenta de usuario la cual la proporciona el Proveedor de Servicios de Internet.



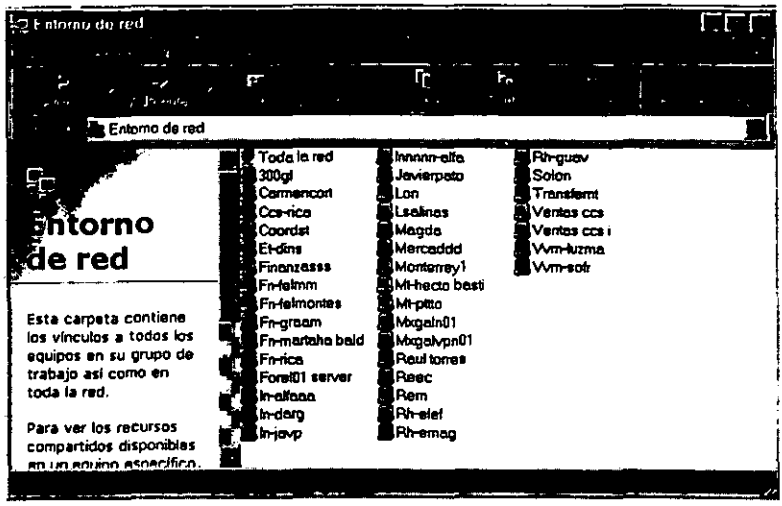
2. - Hacer **click a "mi conexión al servicio VPN"** , debemos contar con una cuenta de usuario (NT) que tenga los derechos necesarios para acceder a la red local.



3.- Tendremos ahora 2 conexiones nuevas :



4.- Para confirmar que estemos conectados a la red, hacer **click a Entorno de Red :**



5.- Listo estamos conectados.

GLOSARIO

10BASET Es una parte de la especificación IEEE802 que usa cable de par trenzado, también *llamada par trenzado ethernet*. El 10 significa que pude transmitir a 10 *Mbps*. BASE indica que trabaja en banda base y la *T* significa cableado de par trenzado.

ANCHO DE BANDA. Indica el rango de frecuencia asignadas a un canal analógico de transmisión. Corresponde a la diferencia entre las frecuencias mayor y menor que pueden ser transmitidas por dicho canal.

ARCHIVO. Conjunto de *bytes* relacionados y tratados con una unidad. Un archivo puede contener datos, programas o ambas cosas.

ASÍNCRONO. Es un tipo de comunicación que envía datos usando control de flujo sin necesidad de sincronización entre un terminal origen y un terminal destino.

AUTENTIFICACIÓN. Se llama así al proceso de validación de la conexión del usuario que determina el permiso de acceso a los recursos del servidor.

AUTENTIFICACIÓN DESAFÍO/RESPUESTA. Es un método de autentificación que utiliza algoritmos de desafío/respuesta junto con mecanismos de seguridad de *Windows Nt Server* para permitir el control de acceso a los recursos.

AUTO DIAL. Es un componente de *Microsoft Proxy Server* que habilita a los usuarios la conexión automática a redes remotas durante un tiempo predeterminado

BACKBONE. Con este nombre se indica una red de alta velocidad y alto rendimiento que se enlaza con otras redes formando una inter-red.

BANDA BASE. Es un método de transmisión de datos en una red que utiliza el ancho de bandas completo para una transmisión individual. *Ethernet* es una banda base estándar con una única transmisión posible en cada momento.

Bps (Bits por segundo) : Unidad de medida de la velocidad de transmisión del modem por una línea de telecomunicaciones.

CLIENTE. Es un *software* que trabaja en el computador local para poder hacer uso de algún servicio del computador remoto. El software del computador remoto que permite este uso recibe el nombre de servidor.

CONMUTACIÓN DE PAQUETES. La conmutación de paquetes es un sistema de comunicación de datos mediante el cual toda la información que sale un terminal para ser transmitida por la red de conmutación de paquetes es dividida en bloques de una determinada longitud (paquetes). A cada paquete se le añade la información necesaria al comienzo del mismo, de manera que cada uno se pueda mover por la red de forma independiente. Si en un momento dado una ruta o un nodo de comunicación queda fuera de servicio, los paquetes que en principio utilizaban estos medios son enviados de forma automática por otras rutas sin que quede interrumpida la comunicación.

DATAGRAMA. Es un paquete individual de datos que es enviado al computador receptor sin ninguna información que lo relacione con ningún otro posible paquete enviado. El procedimiento de datagramas se suele usar cuando los datos a transmitir son pocos.

DIALOG. Es el mayor suministrador comercial de bases de datos. Los usuarios de *Internet* pueden acceder a las bases de datos de *DIALOG* a través de *TELNET (dialog.com)*. El acceso a estas bases de datos no es gratuito, sino que su acceso está restringido exclusivamente a los clientes de DIALOG.

DIRECCION. Cada computador conectado a Internet dispone de una dirección. La dirección consta de una parte que identifica al computador, llamada nombre de dominio *(domain name)*, y otra parte que identifica al usuario, llamada identificador de usuario *(userid)*. Una parte de está separada de la otra por el carácter @ *(usuario@dominio)*. Cuando se envía un mensaje, todos los nombres de domino son convertidos a otro tipo de dirección numérica entendible por Internet. A esta dirección numérica se le llama dirección *IP (IP address)* o número *IP*.

ENCAPSULACIÓN. Es un método de transmisión del tráfico de la red que usa protocolo de red encerrándoce en otro protocolo de red.

ENCRIPTACIÓN. Es el proceso de hacer indescifrable la información para proteger su uso o su visualización no autorizada durante el proceso de transmisión o cuando se guarda en un medio magnético transportable.

ETHERNET. Es un tipo particular de red de área local. En este tipo de red las computadoras pueden utilizar el protocolo TCP/IP, por lo que muchos computadores acceden a Internet a través de la red de área local ETHERNET a la que están conectados.

FAST ETHERNET. Es una versión de Ethernet que permite transferencias de datos entre 10 y 100 Mbps y usa un protocolo CSMA/CD.

FRAME. Ver TRAMA.

FRAME RELAY. Es un servicio de transmisión de datos por conmutación de paquetes similar a X25 pero más rápido y eficiente (no realiza la misma comprobación de errores que X25, ya que asume que actualmente las telecomunicaciones están libres de errores).

GATEWAY. Ver PASARELA.

HOST. Ordenador conectado a una red, que permite a los usuarios comunicarse con otros hosts.

INTERNET Es un conjunto de redes de ámbito mundial conectadas entre sí mediante el protocolo IP (Internet Protocolo). A través de Internet se puede acceder a servicios como transferencia de archivos, acceso remoto, correo electrónico y noticias, entre otros.

INTERNIC. (Internet Network Information Center) (Centro de Información de la Red Internet). Es una organización patrocinada por NSF para proveer y coordinar los servicios de NSFNET. Ofrece servicios a toda la comunidad Internet y entre ellos se puede encontrar todo el material relativo a los trabajos generados por la sociedad Internet, como por ejemplo, la documentación completa de los RFC. También ofrece un servicio de directorio y de base de datos conocido como directorio de directorios que contienen información diversa como lista de servidores, lista de directorios, catálogos de libros, etc.

INTRANET. Es la Red propia de una organización, diseñada sigiuendo los protocolos propios de internet, pero protegida mediante identificadores, palabras clave y contrafuegos. Puede tratarse de una red aislada o bien conectada a internet.

IP. (Internet Protocol) (Protocolo Internet). Es el protocolo de nivel de red usado en Internet. Mediante el protocolo IP cualquier paquete puede viajar a través de las distintas redes de Internet hasta llegar a su destino final. Registra las direcciones de nodos, encamina los mensajes que se envían y reconoce los mensajes recibidos.

IP ADDRESS. Dirección IP que identifica un nodo de la Red internet, representada mediante notación decimal separada por puntos.

IPX (Internet Packet Exchange) (Intercambio de paquetes Internet). Es el protocolo de comunicaciones de NetWare. Se utiliza para transferir datos entre servidor y los programas de las estaciones de trabajo.

ISDN. Ver RDSI

LAN. Ver RED DE ÁREA LOCAL.

LINEA DEDICADA. Es una c9onexión permanente entre dos localidades mediante algún medio de transmisión de datos. Las líneas dedicadas se suelen utilizar para conectar redes locales con Internet.

LÍNEAS PUNTO A PUNTO. Es una línea dedicada exclusivamente a conectar dos computadores distantes. Estas líneas se alquilan a las compañías telefónicas.

LINK. (Enlace). Es una ruta de comunicación entre dos nodos de una red.

LOGIN. Es el nombre de acceso de un usuario a una red o a un computador multiusuario. Este término se le puede aplicar tanto al nombre de su cuenta como al hecho de entrar en un computador de este tipo.

MAINFRAME. Con este nombre se indica un gran computador que es capaz de soportar simultáneamente a miles de usurarios.

MAN. Ver RED DE ÁREA METROPOLITANA.

MÓDEM. Es un equipo que se conecta al computador para poder transmitir datos por una línea de transmisión. El módem suele ser utilizado en las comunicaciones de datos por línea Telefónica. Éste convierte las señales digitales propias del computador en señales analógicas, más aptas para ser trasmitidas por una línea telefónica. Los módems utilizados habitualmente en las líneas telefónicas suelen ofrecer una velocidad de transmisión de entre 9.600 y 32.400 bps.

NDIS. (Network Driver Interface Specification). Es una especificación de Microsoft para controladores de dispositivos de red que permite que distintos protocolos de comunicaciones se ejecuten en una misma tarjeta de acceso a la red de forma simultánea.

NETBEUI (NetBios Extended User Interface). Es la extensión para NetBIOS de Microsoft utilizada por LAN Manager, Microsoft Windows para Trabajo en Grupo, Microsoft Windows NT, Windows 95 y Windows 98.

NIC (Network Information Center) (Centro de Información de Red). Recibe este nombre cualquier organización responsable de facilitar información sobre una re.

NODO. Punto de una red al que se conectan varios ordenadores que reciben servicios de la red.

ODI (Open Data-link Interface). Es una interfaz estándar, desarrollada por Apple y Novell, que realiza las mismas funciones que NDIS.

OSI (Open Systems Interconnect) (Interconexión de Sistemas Abiertos). Se trata de una serie de protocolos normalizados por la Organización Internacional para la Normalización (ISO).

PAQUET. Ver PAQUETE

PAQUETE. En una red los datos transmitidos por un computador son divididos en conjunto de caracteres independientes que reciben el nombre de paquetes. Cada paquete viaja por la red independiente de los demás hasta llegar al destino. El tamaño de los paquetes puede variar de entre los 10 y los 32.000 bytes, aunque normalmente no tienen tamaños superiores a los 1.500 bytes.

PASARELA. Es un sistema informático que transfiere datos entre dos aplicaciones o redes incompatibles entre sí.

PDC. (Primery Domain Controller). Es un servidor de dominio que contiene la copia maestra de la seguridad y las cuentas de los usuarios para autentificar sus accesos.

PING (Packet Internet Groper) Es una utilidad de TCP7IP que envía paquetes de información a un computador de la red permitiendo saber si está conectado o no.

PoP (Point of Presence) (Punto de presencia). Es el lugar por donde un usuario accede a las instalaciones de su proveedor de acceso Internet. Generalmente, suele ser un banco de módems situados en una ciudad y conectados mediante un circuito de alta velocidad con la estación que proporciona acceso a Internet y que se encuentra en otra ciudad. Con este sistema, cualquier usuario sólo tiene que realizar una llamada local para acceder al PoP, mientras que el proveedor de acceso no tiene que disponer de una estación en cada cuidad.

PPP (Point to Point Protocolo) (Protocolo Punto a Punto), Es un protocolo utilizado para acceder a Internet mediante una línea telefónica y un módem de alta velocidad. Gracias a PPP ase puede acceder a Intenet con plenos derechos a través de una simple línea telefónica. Es una versión más moderna del protocolo SLIP.

PPTP(Point to Point Tunneling Protocolo). Es un protocolo de red, incorporado en Windows NT, en el cual los datos se encapsulan en paquetes PPP cifrados que se envían a través de Internet. También puede ser usado para transportar el tráfico de acceso remoto IPX y NetBEUI.

PROTOCOLO. Es un conjunto de normas que indican cómo deben actuar los computadores para comunicarse entre sí.

PUERTO. Puede tener dos significados. Por un lado, puede ser un numeró que identifica una aplicación particular de Internet. Cuando un computador envía un paquete a otro, el paquete contiene la información de qué aplicación está intentando comunicarse con el computador remoto. Esta identificación se realiza mediante un número de puerto.

Por otro lado, también se conoce como puerto al conector físico que utilizan los computadores para comunicarse con el exterior (puerto de impresora, puerto serie, etc.).

Los dos significados son completamente distintos, y no tienen nada que ver entre sí.

RDSI (Red Digital de Servicios Integrados). Con este nombre se indica la red pública conmutada completamente digital de terminal a terminal, concebida como red integradora de las actuales redes públicas de voz y datos.

RED DE ÁREA ANCHA. Es una red formada por nodos conectados en una área geográfica extensa. También se le puede denominar RED DE ÁREA EXTENSA o AMPLIA.

RED DE ÁREA LOCAL. Es una red localizada que tiene un computador central, llamado servidor, que proporciona servicios a múltiples nodos asociados llamados clientes.

RED DE ÁREA METROPOLITANA. Es una red formada por nodos conectados en una área geográfica localizada dentro de una ciudad.

ROUTER (Encaminador). Es un sistema utilizado para transferir datos entre dos redes que utilizan un mismo protocolo. Un router puede ser un dispositivo software, hardware o bien una combinación de ambos.

SEMIDÚPLEX. Indica un método de transmisión sobre un canal de comunicaciones en el que las señales pueden ir en ambas direcciones pero no simultáneamente.

SERVER. Ver SERVIDOR

SERVIDOR. Se trata de un software instalado en n computador, llamado remoto, que le permite ofrecer un servicio a otro computador llamado local. El computador local contacta con el computador remoto gracias a otro software llamado cliente. También puede recibir el nombre de servidor el propio computador en el que está instalado el software servidor.

SINCRONIA. Es un método de comunicación a través de una comunicación a través de una conexión controlada por un temporizador que requiere que cada participante esté sincronizado con el resto.

SMTP. (Simple Mail Transfer Protocol) (Protocolo simple de Transferencia de Correo). Se trata del protocolo en el que se basa el servicio de correo electrónico en Internet. Y define el formato que deben tener los mensajes y cómo deben ser transferidos. Gracias a SMTP distintos fabricantes de software pueden desarrollar programas completamente compatibles entre sí.

TCP (Transmission Control Protocol) (Protocolo de Control de Transmisión) Es un conjunto de protocolos de los niveles de red y transporte del modelo OSI que permite el intercambio de datos de computadores conectados a Internet.

TERMINAL. Pantalla teclado unidos por una red a un ordenador central que contiene el disco y la CPU, y que generalmente sopora decenas de terminales.

TOKEN RING. Es un tipo particular de red de área local (LAN). Las redes *TOKEN RING* utilizan a menudo el protocolo *TCP/IP*. Estas redes de área local pueden estar conectadas a *internet.WW*

TRAMA. Es una unidad de transmisión de red en el nivel de enlace de datos. Se refiere a la unidad que se envía fuera de la estación origen en la red física.

UDP. (*User Datagram Protocol*). Es un protocolo sobre el que funcionan ciertos servicios de *Internet*. Se utilizan cuando se necesita transmitir voz o vídeo resulta mas importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los *bytes*.

WAN. Es una red formada por nodos conectados en una área geográfica extensa. También se le puede denominar RED DE AREA EXTENSA O AMPLIA.

WINSOCK (*Windows Socket*). Es un *API* creado para permitir que los programas *WINDOWS* puedan acceder a los servicios *TCP/IP*.

BIBLIOGRAFIA

Netware 5
José Luis Raya, Elena Raya
Alfaomega ra-ma, 2000

Redes de Computadoras
Andrew S. Tanenbaum
Prentice Hall Hispanoamericana, S.A.
Tercera Edición 1997.

Todo acerca de ... Redes de computación
Kevin Stoltz
Prentice Hall Hispanoamericana, S.A., 1995

REVISTAS CONSULTADAS

Computer
Volumen 15, Número 6
Redes Vituales

Byte
Enero, 1999
Tecnología VPN

Red
Número 117
Redes Inalámbricas

Pc Semanal

Año 8 Volumen 15 #354
Redes Virtuales

Pc Semanal

Año 8 Volumen 15 #388
Protocolo PPTP

DIRECCIONES URL

http:/www.monografias.com

http://microsoft.com/ntserver/nts/downloads/recommended/dun13win95/ReleaseNotes.asp

http://www.ceenet.org/workshops99/Richard_Perlman/Part-9/sld051.htm

http://www.cantug.ab.ca/vpn/sld017.htm

http://www.freesoft.org/CIE/Topics/65.htm

http://eicon.com/support/ap/DIVACNT/ppplog.htm

http://www.abcdatos.com/tutoriales/redes.html

http://www\Consultas más frecuentes PPTP y Redes Privadas Virtuales.htm

http://www.Soporte/Windows NT 4_0.htm

http://www.freebsd.org/FAQ/ppp.html

http://www.wntmag.com/atrasados/1999/29_mar99/articulos/internet.htm