12

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN

REDES DE COMPUTADORAS. TRANSMISION DE INFORMACION A TRAVES DE UNA RED WAN CON ARQUITECTURA ETHERNET PARA LA PRODUCCION Y VENTA DE LLANTAS.

TRABAJO DE SEMINARIO

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMATICA

P R E S E N T A :

OSCAR RODRIGUEZ MENDEZ

ASESOR: ING. MIGUEL ALVAREZ PASAYE

CUAUTITLAN IZCALLI, ESTADO DE MEXICO. 2000.

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. Transmisión de información a través de una red WAN con arquitectura Ethernet para la producción y venta de llantas.

que presenta el pasante: Oscar Rodríguez Núñez

con número de cuenta: 9559507-8 para obtener el título de :

Licenciado en Informática

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en 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
II		

A mis padres:

Gracias por todo el apoyo y ayuda que me han brindado, sin ustedes no hubiera sido posible alcanzar esta meta.

A mis hermanas:

Gracias por todo el cariño que me han dado en todo este tiempo en que hemos estado juntos. Sigan adelante con mucho entusiasmo como hasta este momento

A mis amigos:

Gracias por haberme permitido conocerlos y compartir muchos momentos importantes de mi vida, especialmente el equipo INFOSOFT.

A mi nena:

Gracias por todo el apoyo y comprensión que me haz brindado.

ÍNDICE

OBETIVO GENERAL

Optimizar el servicio de comunicación de las oficinas corporativas de una empresa llantera con sus plantas, almacenes y distribuidores de toda la República Mexicana para la producción y venta de neumáticos, por medio de VPN.

OBJETIVOS PARTICULARES

- Conocer las características de las redes LAN con el estándar Ethernet
- Conocer las características de las redes WAN
- Conocer el funcionamiento de las redes privadas virtuales (VPN)
- Identificar los beneficios de utilizar las redes privadas virtuales (VPN)

INTRODUCCIÓN.

En los últimos años las telecomunicaciones han tenido un gran auge y han venido a formar parte de nuestra vida cotidiana, hoy en día es común que establezcamos videoconferencias con personas que se encuentran a miles de kilómetros, que compremos por medio de Internet o que enviemos correos electrónicos a personas de cualquier parte del mundo. Los sistemas distribuidos han venido a sustituir a los pequeños sistemas operativos monousuario.

Todos estos avances tecnológicos también nos han hecho dependientes de los sistemas de información en los cuales se ingresan datos por diversos medios y se obtiene como insumo información oportuna para facilitar la toma de decisiones.

La tendencia de las economías de la gran mayoría de los países es de una globalización de mercados en donde es esencial contar con medios de comunicación electrónicos para facilitar y agilizar las transacciones entre diferentes entidades económicas, lo que las hace más competitivas.

En la actualidad la empresa utiliza terminales tontas para accesar al sistema antes mencionado que se encuentra dentro de una plataforma AS/400 y solamente algunos usuarios cuentan con los servicios de Internet, además los distribuidores y almacenes se comunican por medio de un módem, utilizando líneas dedicadas para este propósito.

En este trabajo se verá el caso de una empresa llantera transnacional en la cual se diseñará una red para poder conectar las oficinas corporativas que se encuentran en la Ciudad de México con las plantas de Cuernavaca y del Distrito Federal, y con los almacenes y distribuidores que están situados a lo largo de la república. Esta red debe ser usada para accesar al sistema integral que utiliza la

empresa para registrar su información, así como para utilizar los servicios de Internet e impresión.

En el primer capítulo se verán las características de la empresa para determinar sus necesidades de información, en el segundo, se incluirán conceptos generales de la redes de área local (LAN), redes de área amplia (WAN), redes privadas virtuales (VPN) y finalmente, en el tercer capítulo se desarrollará el caso práctico.

CAPITULO 1. CARACTERISTICAS DE LA EMPRESA.

Para diseñar una red o para hacer modificaciones sobre la misma se tiene que hacer un análisis de las necesidades de información que tiene la empresa y de la distribución física de los dispositivos que se desean conectar a la misma, para así poder determinar todos los recursos y equipo que serán necesarios para poder implantar el nuevo modelo en la red. A continuación se describirán las características de la empresa en la cual se desarrollará el proyecto.

1.1 Principios organizacionales de la empresa

A continuación enunciaré brevemente los lineamentos y valores que existen dentro de la empresa:

1.1.1 Visión de la empresa.

- Ser el número 1 en producción/manufactura en México.
- Ser el número 1 en ventas en México.
- Ser el número 1 en utilidades en México.
- Ser el número 1 en calidad de vida en el trabajo.

1.1.2 Misión

Fabricar y comercializar llantas para el desplazamiento de vehículos automotores con el fin de facilitar el traslado propio de la gente y movimiento de la economía.

1.1.3 Filosofía

Valores humanos

Valores fundamentales	Valores primario
• Servicio	Enfoque al cliente
	Comunicación
	Responsabilidad
	Compromiso
• Disciplina	Participación
	Reconocimiento
	Autodesarrollo
	Trabajo en equipo
• Optimismo	Orientación al cambio
	Velocidad de respuesta
• Honestidad	Lenguaje "Onto-ni"

Figura 1.1 Filosofía de la empresa

1.1.4 Política de calidad total

"Nuestra compañía está dedicada a proveer productos y servicios a la sociedad, con un nivel de calidad superior que exceda las expectativas de nuestros clientes. Nuestro trabajo deberá será desarrollado con entusiasmo, aplicando continuamente los conceptos y las metodologías de calidad total cuidadosamente establecidos."

1.2 Infraestructura tecnológica

En este apartado daré un panorama general de la situación actual de la empresa en el ámbito tecnológico.

1.2.1 Plataforma utilizada

La plataforma informática Aplication System/400© de IBM (AS/400) es, sistema informático de rango medio que ha permanecido en el mercado por más de 30 años.

El AS/400 está definido por cinco principios arquitectónicos fundamentales:

- **Independencia tecnológica**

El primer y quizá más importante principio es la independencia tecnológica, A diferencia de otros sistemas computacionales, el AS/400 no está definido por el hardware. Esto quiere decir que un programa no "habla" directamente del hardware; "habla" a una máquina de interface tecnológicamente independiente (MITI o simplemente máquina de interface). Entre su interface y el hardware real existen

alrededor de cinco millones de líneas de software del sistema operativo llamado System Licensed Internal Code (SLIC).

Este diseñador de software aísla los programas de aplicación de las características relevantes del hardware. Un programa AS/400 no tiene conocimiento del diseño de hardware; este conocimiento permanece completamente dentro del SLIC. Esto significa que cuando el procesador cambia de tecnología, IBM puede sobreescribir los componentes SLIC que están pendientes de estos cambios tecnológicos y así perservar la integridad de la interface de máquina. Debido a este diseño de tecnología independiente, los programas de aplicación de los clientes son también inconscientes de los cambios tecnológicos y pueden explotar nuevas tecnologías sin ser interrumpidos por ellos. La importancia de este principio arquitectónico fue dramáticamente ilustrada cuando el procesador de la tecnología AS/400 cambió de 48 bits CISC a 64 bits RISC. Muchos clientes simplemente necesitaron salvar sus programas fuera de sus máquinas CISC y restaurarlos en sus nuevas máquinas RISC para correrlos como programas de 64 bits. Ningún otro sistema puede hacer esto; las arquitecturas convencionales requieren por lo menos la recompilación de los programas de herencia y usualmente algo de sobreescritura antes de que usted pueda correrlos en un sistema con una arquitectura diferente. Pero el AS/400 permite a los usuarios correr sus aplicaciones originales de 48 bits como aplicaciones de 64 bits – en un sistema operativo de 64 bits que contiene una base de datos relacional de 64 bits.

- **Diseño con base de objetos**

El AS/400 está completamente diseñado con base de objetos. Esto quiere decir que todo dentro del sistema – programas, bases de datos, colas de mensajes- es un objeto. Cada objeto tiene dos partes inseparables: una parte descriptiva, que define

las maneras válidas de usar esa información; y una parte de información, que sirve como el aspecto funcional del objeto.

Si un objeto es definido por un programa, su parte descriptiva establece que la parte de información será tratada como ejecutable, código compilable de sólo lectura. Las únicas operaciones permitidas en este código son aquellas que tienen sentido para el programa. Por ejemplo, usted puede escribir a la mitad de un archivo de datos, pero no puede escribir a la mitad de un código compilado; el sistema no permitirá que esto suceda. Así, las dos partes de los objetos AS/400 diseñan seguros de integridad de información para todos los objetos del sistema.

El diseño basado en objetos tiene importantes implicaciones de seguridad. Por ejemplo, un mecanismo por el que los virus computacionales entran a los sistemas disfrazados como si fueran información. Una vez dentro, el virus trata de convertirse en un código ejecutable y devastar con destrucción. Tal cambio de características es imposible en el AS/400 – si el sistema permite que un paquete ingrese al mismo como información, retendrá por siempre las características de la información. No puede cambiar de forma y volverse un código ejecutable. Como una parte clave del diseño fundamental de AS/400, los objetos son una de las muchas razones por las que el AS/400 goza de una casi legendaria reputación de ser roca sólida de la seguridad y la integridad.

- **Integración de Hardware**

Mientras que el ambiente ingeniero - científico de la computación es computacionalmente intensivo (lo que significa que los usuarios ejecutan operaciones complejas con una relativa pequeña cantidad de información), el ambiente general de la computación de negocios es informáticamente intensivo (es decir, que los usuarios ejecutan operaciones simples en una gran cantidad de

información). Debido a que el AS/400 está optimizado para el ambiente general de negocios, contiene características de diseño de hardware que le permiten ofrecer un desempeño exagerado en un ambiente informacionalmente intensivo.

En una transacción típica de negocios, un programa de aplicación es cargado dentro del almacén principal, y, entonces, el procesador principal comienza a ejecutarlo. Cuando el procesador principal llega a través de una petición de información para, por ejemplo, ser leída del disco, delega la petición al procesador de entrada/salida (IOP) que está dedicado al dispositivo del disco. Entonces el procesador principal desvía su atención a otras aplicaciones del programa – la tarea que está dedicado a hacer- y regresa al programa original solamente cuando la petición de información anterior está disponible en el almacén principal.

En un AS/400 grande usted puede tener más de 200 IOPs conectados a buses de alta velocidad, creando un servidor extremadamente poderoso. Tal diseño de servidor es excelente para aplicaciones informacionalmente intensas.

- **Integración de software**

Algunas características del software son fundamentales para todos los negocios. Adicionalmente a los tradicionales drivers básicos del sistema operativo que manejan los numerosos dispositivos de E/S, los negocios siempre necesitan software para funciones estándar de cómputo, tales como la seguridad, las comunicaciones, servidor de Red, respaldo y recuperación. Con un sistema tradicional, los clientes con frecuencia deben comprar componentes adicionales de software para agregarlos a su base de sistema operativo. Estos clientes deben también asegurarse de que los niveles de liberación de módulos adicionales son compatibles con los niveles de liberación de todos los otros ítems que planean integrar.

Con el AS/400, sin embargo, todos los componentes necesarios del software del negocio están completamente integrados en el sistema operativo estándar. IBM prueba todos los componentes en el contexto de otros componentes, así la totalidad del sistema operativo trabaja en una entidad. Más aún, si IBM hace cambios en el OS/400, da a los clientes una nueva entrega del sistema operativo; así, nunca hay conflictos de liberación entre componentes individuales del OS/400 porque IBM embarca un sistema operativo completo y totalmente probado a sus clientes en cada entrega.

Dos beneficios de este sistema operativo completamente integrado aparecen de inmediato para los clientes: un rápido despliegue de nuevas soluciones de negocios y un costo sobresalientemente bajo de su adquisición.

- **Almacenamiento de un solo nivel**

El espacio de almacenamiento masivo de 64 bits del AS/400 puede guardar ¡18 quintillones de bytes de información! Arquitectónicamente, el AS/400 está diseñado para tener aún más capacidad – arriba de 128 bits de almacenamiento.

Mapeado dentro de este espacio de 64 bits es un almacén "real: drives de disco y memoria principal. Pero los clientes no tienen que estar conscientes de ninguna de tales tecnologías de almacenamiento que subyacen al enorme espacio de direccionamiento porque el AS/400 las administra automáticamente. Tanto como los clientes se preocupan, todos los programas y la información simplemente residen en este espacio masivo. Los usuarios no necesitan preocuparse acerca de dónde reside un programa; ellos sólo necesitan referirlo por su nombre.

De manera similar, los clientes no necesitan preocuparse de hacer extensiones para archivos que están llenos. El AS/400 maneja esto de manera automática

también. Y cuando los clientes agregan más dispositivos de almacenamiento a su máquina, no necesitan redistribuir la información a través de ellos; el sistema reconoce el nuevo almacenamiento disponible y lo utiliza. La mayoría de las instalaciones AS/400 incluso no tienen un administrador tradicional de la base de datos porque no lo necesitan. El sistema hace mucho de este tipo de trabajo por sí mismo. Los procesos de aplicaciones de negocios en un ambiente de multiaplicaciones y multiservidores con frecuencia implican la conexión entre tareas diferentes. Gracias a su almacenamiento de un solo nivel, el AS/400 completa esta función con mucho más eficacia que los sistemas convencionales. Conectar una nueva tarea en el AS/400 es tan simple como ejecutar una instrucción branch en la locación donde la nueva tarea reside. No es necesario (como en los sistemas UNIX y Windows) crear un espacio de direcciónamiento separado antes de que la ejecución de una nueva tarea pueda comenzar.

Diseñado para la conexión frecuente de tareas que caracteriza los ambientes de negocios, el almacenamiento de un solo nivel del AS/400 no solamente simplifica la administración del almacenamiento, sino que también brinda un excelente desempeño.

- **Poniendo todo junto**

La arquitectura del AS/400 está diseñada para ser extremadamente flexible para adecuarse a las nuevas tecnologías de hardware y software del nuevo milenio. Al preparar a los usuarios para el futuro, mientras los equipa con las aplicaciones de negocios que necesitan, para tener éxito en la actualidad, el AS/400 puede ser descrito con verdad como "más allá de la tecnología".

1.2.2 Software de aplicación

La compañía utiliza un sistema integral llamado J. D. Edwards, el cual contiene programas, formularios, archivos de datos y reportes que están diseñados para registrar y consultar información en las bases de datos distribuidas del servidor AS/400. Generalmente a este tipo de sistemas se les denomina como ERPs (Enterprise Resource Planning) o planeación de recursos empresariales.

Actualmente, la compañía cuenta con los siguientes módulos:

- Compras
- Cuentas por cobrar
- Administración de ordenes de ventas
- Contabilidad
- Administración de inventarios
- Cuentas por pagar

Además existen otras aplicaciones desarrolladas en RPG III [1] (Report Program Generator) para la nómina, descuentos de ventas e incentivos a vendedores.

1.2.3 Necesidades de información

Actualmente la compañía cuenta con 2 plantas de producción, (una ubicada en la ciudad de México y otra en la ciudad de Cuernavaca), un almacén de producto terminado en Cuernavaca, tres en el área Cuautitlán, uno en Culiacán, uno en Hermosillo y otro en Nuevo Laredo, Texas.

(1) RPG III es el lenguaje de programación nativo del AS/400

Existe una red local (LAN) principal con estándar Ethernet, en la cual se encuentran conectados 225 nodos para proporcionar los servicios de correo electrónico, Internet, impresión y acceso al sistema AS/400 a todos los usuarios de las oficinas corporativas ubicadas en la calle de Darwin # 74, colonia Anzures, México D. F. Cabe mencionar que la red funciona adecuadamente ya que es segura (tiene un firewall instalado) y actualmente no existe mucho tráfico en ella, lo que proporciona respuesta una respuesta rápida. También existe una conexión con Frame Relay hacia la red local de Cuernavaca donde se encuentran la planta y almacenes más importantes para la compañía, es importante subrayar que esta conexión no se desea modificar por la importancia de la misma.

Por otra parte, los demás almacenes que se encuentran a lo largo de todo el país se conectan mediante líneas telefónicas dedicadas. Esto provoca que se gasten fuertes sumas de dinero mensualmente por el alquiler de dicho servicio telefónico más el pago de larga distancia.

Por lo anterior, podemos decir que el servicio que se proporciona por medio de la red es eficiente, pero es necesario implementar un sistema de comunicación remoto con el cuál se minimicen los costos de telefonía y que además sea totalmente transparente para el usuario.

CAPITULO 2. CONCEPTOS GENERALES

2.1 Redes LAN y el estándar Ethernet

Una red LAN (red de área local por sus siglas en inglés) es un conjunto de nodos que están distribuidos en un región relativamente pequeña (hasta 1 Km de distancia entre uno y otro) para compartir recursos. Este es el modelo de red típica que se implanta en las empresas para poder tener acceso a servicios como impresión compartida de documentos y correo electrónico.

Ethernet es una tecnología de red de área local (LAN) que transmite información entre computadoras a velocidades de entre 10 y 100 millones de bits por segundo (Mbps). Actualmente la versión que más se usa de Ethernet es la de 10-Mbps de par trenzado.

Las versiones de 10-Mbps de Ethernet incluyen la original de cable coaxial grueso, así como la de cable coaxial fino, par trenzado, y fibra óptica. El más reciente estándar de Ethernet define el nuevo Sistema de 100-Mbps Fast Ethernet que opera sobre par trenzado y fibra óptica.

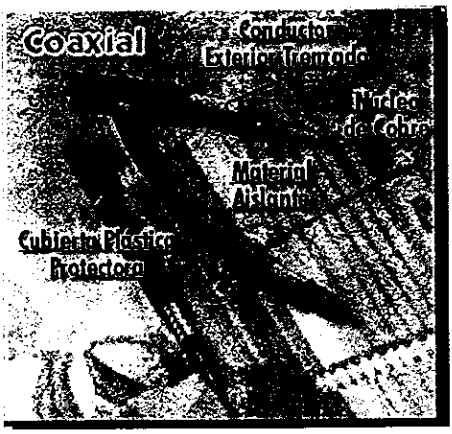

Figura 2.1 Cable coaxial

Figura 2.2 Cable par trenzado apantallado

Figura 2.3 Cable par trenzado no apantallado

Figura 2.4 Cable par trenzado con pantalla global

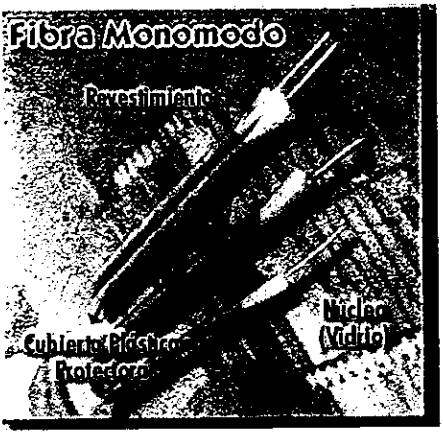

Figura 2.5 Fibra monomodo

Figura 2.6 Fibra multimodo

2.1.1 Difusión de Ethernet

Actualmente se usan distintos tipos de redes LAN, pero Ethernet es con mucho la más popular. Se estima que en 1994, se instalaron más de 40 millones de nodos Ethernet en todo el mundo. La amplia popularidad de Ethernet asegura que habrá un gran mercado para el equipamiento Ethernet, lo que conlleva una reducción en los precios del equipo.

Desde los tiempos del primer estándar de Ethernet, las especificaciones y derechos para construir tecnología Ethernet se han hecho fácilmente accesibles a cualquiera. Esta apertura, combinada con la facilidad de uso y la robustez del sistema Ethernet, a dado como resultado el gran mercado de Ethernet y es una de las razones por las que Ethernet está tan ampliamente implantado en la industria de los computadoras.

La gran mayoría de fabricantes de computadoras equipan actualmente sus productos con conectores Ethernet de 10-Mbps, haciendo posible conectar todo tipo de computadoras con una LAN Ethernet. Hasta que el estándar de 100-Mbps sea adoptado más ampliamente, los computadoras están siendo equipados con un interface Ethernet que opera tanto a 10-Mbps como a 100-Mbps. La capacidad de conectar una amplia gama de computadoras usando una tecnología de red estándar vendor-neutral network technology es un rasgo esencial para los gestores de LANs actuales.

Más LANs deberían soportar una amplia variedad de computadoras ofrecidos por los diferentes fabricantes, lo que requiere un alto grado de interoperatividad de red, del tipo que proporciona Ethernet.

2.1.2 Elementos del sistema Ethernet

El sistema Ethernet consta de tres elementos básicos:

1. El medio físico usado para transportar las señales Ethernet entre computadoras,

2. Una serie de reglas de control de acceso al medio incluidas en el interface que permite a múltiples computadoras regular su acceso al medio de forma equitativa

3. Una trama Ethernet que consiste en una serie estandarizada de bits usados para transportar los datos en el sistema.

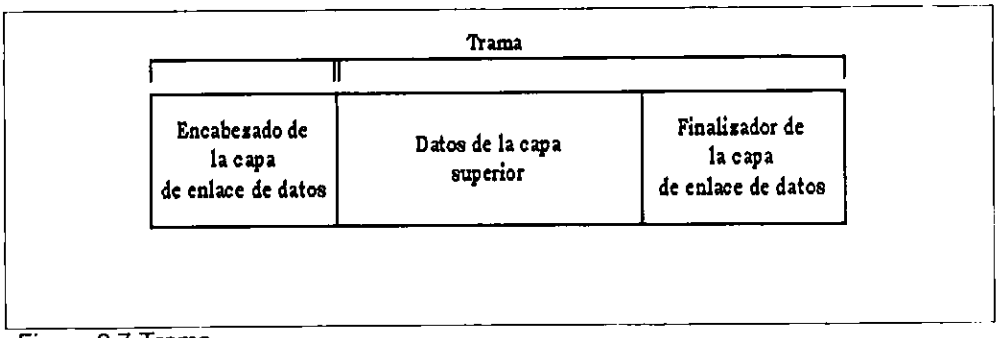

Figura 2.7 Trama

2.1.3 Funcionamiento de Ethernet

Cada terminal equipado con Ethernet, también llamado estación, opera independientemente de todas las otras estaciones de la red: no hay un controlador central. Todas las estaciones conectadas a una red Ethernet están conectadas a un

medio compartido. En Ethernet las señales se transmiten en serie, un bit cada instante, por el canal compartido, a todas las estaciones conectadas. Para mandar datos una estación lo primero que hace es escuchar el canal, y cuando el canal esta vacío, la estación transmite sus datos en forma de trama Ethernet, o paquete.

Después de cada transmisión, todas las estaciones de la red tienen las mismas posibilidades de ser las siguientes en transmitir. Esto asegura que el acceso al medio sea fácil, y que ninguna estación pueda bloquear a las demás. El acceso al medio es determinado por el control de acceso al medio (MAC), que es un mecanismo contenido en el interface Ethernet de cada estación. El mecanismo del MAC se basa en un sistema llamado Acceso Múltiple Sin Portadora con Detección de Colisiones (CSMA/CD).

El protocolo CSMA/CD funciona de algún modo como una conversación en una habitación oscura. Todo el mundo escucha hasta que se produce un periodo de silencio, antes de hablar (Sin Portadora). Una vez que hay silencio, todo el mundo tiene las mismas oportunidades de decir algo (Acceso Múltiple). Si dos personas empiezan a hablar al mismo tiempo, se dan cuenta de ello y dejan de hablar(Detección de Colisiones.)

En términos de Ethernet, cada interface debe esperar hasta que no haya ninguna señal en el canal, entonces puede empezar a transmitir. Si algún otro interface esta transmitiendo habrá una señal en el canal, a la cual se llama portadora. Todos los otros interfaces deben esperar hasta que la portadora cese antes de intentar transmitir, este proceso es llamado Sin Portadora.

Todos las interfaces Ethernet tienen las mismas posibilidades de mandar tramas a la red. Ninguno tiene una prioridad mayor que los demás, y reina la democracia. Esto es lo que significa Acceso Múltiple. Como la señal tarda un tiempo finito en viajar de un extremo al otro de un segmento Ethernet, los primeros bits de

una trama no llegan simultáneamente a todas las partes de la red. Asi pues, es posible que dos interfaces escuchen que el canal esta vacío y comiencen a transmitir sus tramas simultáneamente. Cuando esto ocurre, El sistema Ethernet tiene un modo de detectar la "colisión" de las señales e interrumpir la transmisión y reenviar las tramas. A esto se le llama Detección de Colisiones.

El protocolo CSMA/CD esta diseñado para permitir un fácil acceso al medio compartido, con lo que todas las estaciones tienen oportunidad de usar la red. Después de cada transmisión todas las estaciones usan el protocolo CSMA/CD para determinar cual es la siguiente en usar el canal.

Si mas de una estación comienza a transmitir en el canal Ethernet al mismo tiempo las señales colisionan. Esto es notificado a las estaciones, que inmediatamente reestructuran sus transmisiones usando un algoritmo especialmente diseñado. Como parte de este algoritmo, cada una de las estaciones involucradas elige un intervalo de tiempo aleatorio para volver a intentar retransmitir la trama, lo que impide que todas vuelvan a intentarlo al mismo tiempo.

La palabra colisión no debe interpretarse como algo malo, no es un fallo de la red, se trata de algo absolutamente normal y esperado en una red Ethernet, e indica simplemente que el protocolo CSMA/CD funciona como es debido. Cuantas mas estaciones se añaden a una red Ethernet, y cuanto mas se incrementa el trafico en la red, ocurrirán mas colisiones como parte del funcionamiento normal de Ethernet.

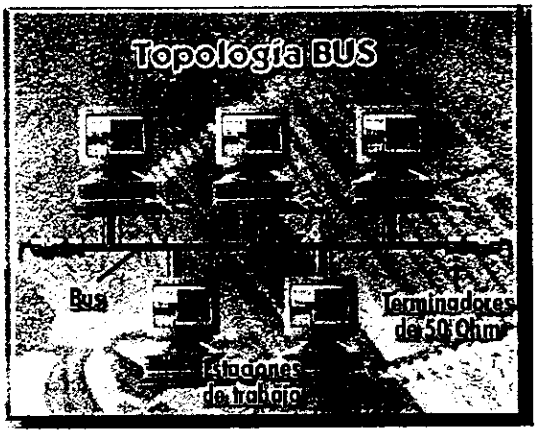

Figura 2.8 Ejemplo de red Ethernet

El diseño del sistema asegura que la mayoría de colisiones en una red Ethernet que no este sobrecargada, serán resueltas en microsegundos, (millonésima de segundo). Una colisión normal no supone perdida de datos. En caso de colisión el interface Ethernet espera durante un numero de microsegundos, y después retransmite los datos.

En redes con trafico denso pueden darse múltiples colisiones para los intentos de transmisión de una trama dada. Esto también es normal. Si se da esta situación, las estaciones involucradas eligen aleatoriamente tiempos cada vez mayores para intentar la retransmisión.

Solo tras 16 colisiones consecutivas para los intentos de transmisión de una misma trama, esta será descartada por el interface. Esto solo puede ocurrir si el canal esta sobrecargado por un periodo muy largo, o si esta dañado en alguna parte.

El corazón del sistema Ethernet es la trama Ethernet, que es usada para transmitir datos entre las estaciones. La trama consiste en una serie de bits organizados en distintos campos. Estos campos incluyen campos de direcciones, un campo de datos de tamaño variable que contiene entre 46 y 1.500 bytes de datos, y un campo de control de errores que se usa para comprobar si la trama ha llegado intacta.

Los primeros dos campos contienen direcciones de 48 bits, llamadas dirección destino y fuente. El IEEE controla la asignación de esas direcciones administrando una parte de cada campo de dirección. El IEEE hace esto proporcionando identificadores de 24 bits llamados "Identificadores Unicos Organizados" (OUIs), de modo que se asigna un identificador de 24 bits único a cada organización que desea fabricar interfaces Ethernet. Después la organización, crea direcciones de 48 bits usando el OUI asignado como los primeros 24 bits de cada dirección. Esta dirección de 48 bits es conocida como dirección física, dirección hardware, o dirección MAC.

A cada interface Ethernet fabricado, se le preasigna una dirección de 48 bits única, lo que simplifica enormemente la conexión y funcionamiento de la red.

Cuando una trama Ethernet es enviada al medio, cada interface Ethernet comprueba el primer campo de 48 bits de la trama, que contiene la dirección de destino. El interface compara esta dirección con la suya. Si es igual, el interface leerá toda la trama. Los demás interfaces dejaran de leer la trama cuando vean que la dirección de destino no es la suya.

Una dirección multicast permite que una trama Ethernet sea recibida por un grupo de estaciones. El software de red puede hacer que el interface de una estación reconozca una dirección multicast concreta. Esto hace posible que un grupo de estaciones tengan asignada una misma dirección multicast. Una trama enviada a la

dirección multicast asignada al grupo, será recibida por todas la estaciones del mismo.

También hay un caso especial de dirección multicast conocida como dirección broadcast, que tiene los 48 bits a unos. Todos los interfaces Ethernet que vean una trama con esta dirección de destino leerán la trama.

2.1.4 Fast Ethernet

Comparado con las especificaciones de 10-Mbps, los resultados del sistema de 100 Mbps son mucho mejores, produciéndose una reducción del "tiempo de bit"*(bit-time)*que es el tiempo empleado en transmitir un bit por el canal Ethernet. Esto produce un incremento en la velocidad de los paquetes que viajan a través del sistema. Sin embargo, el otro aspecto importante del sistema Ethernet es que el formato, la cantidad de datos que una trama transporta y el mecanismo de control de acceso al medio, siguen todos igual que antes, sin cambios.

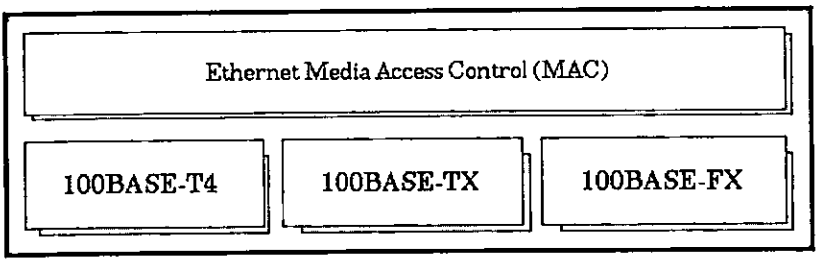

Figura 2.9 Tipos de Fast Ethernet

Los 3 tipos están con sus nombres abreviados propuestos por el IEEE. Estas abreviaturas o identificadores incluyen 3 partes de información. La primera, "100" hace referencia a la velocidad de comunicación ."Base" se refiere a *banda base* que

es el tipo de señalización. La tercera parte del identificador indica el tipo de segmento.

2.2 Redes WAN

2.2.1 Características de las redes WAN

Son redes de comunicación de datos que tiene una cobertura geográfica relativamente grande (un país o continente) que suelen utilizar las instalaciones de transmisión que ofrecen compañías portadoras de servicios como las telefónicas.

Las tecnologías WAN operan en las tres capas inferiores del modelo de referencia OSI:

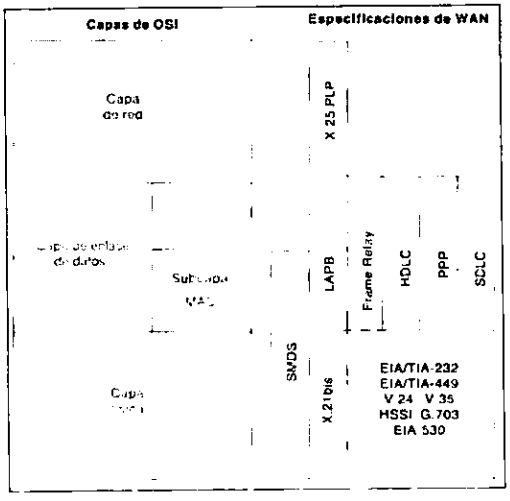

Figura 2.10 Tecnologías WAN

2.2.2 Enlace punto a punto

Una solución simple para una red es el circuito real permanente constituido por lo que se conoce como líneas dedicadas o líneas alquiladas (leased lines); está formado por un enlace punto a punto abierto de forma permanente entre los nodos que se desean unir. Una línea dedicada es únicamente un medio de transmisión de datos a nivel físico, todos los protocolos de niveles superiores han de ser suministrados por el usuario.

Normalmente no es posible contratar una línea dedicada de una velocidad arbitraria, existen unas velocidades prefijadas que son las que suelen ofrecer las compañías telefónicas y que tienen su origen en la propia naturaleza del sistema telefónico. El precio de una línea dedicada es una cuota fija mensual que depende de la velocidad y de la distancia entre los dos puntos que se unen.

En las líneas dedicadas la capacidad contratada está reservada de forma permanente en todo el trayecto. Su costo es elevado y por tanto su instalación generalmente sólo se justifica cuando el uso es elevado (al menos tres o cuatro horas al día). Por este motivo las líneas dedicadas no suelen utilizarse en casos en que se necesita una conexión de forma esporádica, por ejemplo una oficina que requiere conectarse unos minutos al final del día para transferir unos archivos, o un usuario doméstico que se conecta a Internet en los ratos de ocio.

Para mostrar el elevado consumo de recursos que representan las líneas dedicadas pondremos un ejemplo: supongamos que la empresa X con sede central en Valencia ha abierto treinta sucursales en distintos puntos de España, y necesita que las computadoras de las sucursales se comuniquen con la sede central todos los días durante treinta minutos cada uno para transferir 2 MBytes de información. Para esto la empresa solicita 30 líneas dedicadas de 64 Kbps a la compañía telefónica, y constituye una red con topología de estrella. Aunque cada línea se utiliza únicamente

el 2% del tiempo con una eficiencia del 14% el ancho de banda está reservado en su totalidad de forma permanente. Además, se requieren treinta interfaces físicas en el servidor, lo cual lo encarece y complica bastante.

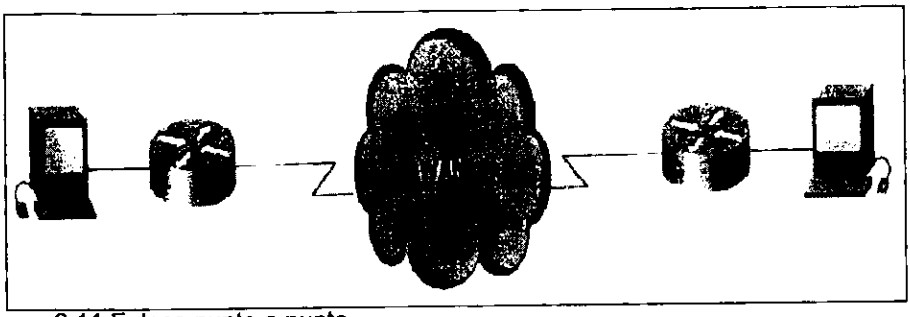

Figura 2.11 Enlace punto a punto

2.2.3 Conmutación de circuitos

La conmutación de circuitos supone una utilización más óptima de los recursos que las líneas dedicadas, ya que la conexión extremo a extremo sólo se establece durante el tiempo necesario. Para la transmisión de datos mediante conmutación de circuitos se utiliza la misma red que para la transmisión de la voz, mediante módems o adaptadores apropiados. Genéricamente se la denomina Red Telefónica Conmutada (RTC) o PSTN (Public Switched Telephone Network) y comprende en realidad tres redes diferentes:

- La Red de Telefonía Básica (RTB) también llamada POTS (Plain Old Telephone Service); Está formada por las líneas analógicas tradicionales y por tanto requiere el uso de módems; la máxima velocidad que puede obtenerse en este tipo de enlaces es de 33.6 Kbps (recientemente han aparecido en el mercado módems capaces de comunicar a 56 Kbps por líneas analógicas si se dan ciertas condiciones).

- La Red Digital de Servicios Integrados (RDSI) también llamada ISDN (Integrated Services Digital Network). Está formada por enlaces digitales hasta el bucle de abonado, por lo que el circuito se constituye de forma digital extremo a extremo. La velocidad por circuito es de 64 Kbps, pudiendo con relativa facilidad agregarse varios circuitos (llamados canales) en una misma comunicación para obtener mayor ancho de banda.

- La Red GSM (Global System for Mobile communications). Se trata de conexiones digitales, como en el caso de la RDSI, pero por radioenlaces. La capacidad máxima de un circuito GSM cuando se transmiten datos es de 9.6 Kbps.

Para evitar confusiones conviene usar sólo el término RTB al referirse a la red telefónica analógica, y reservar el término RTC para referirnos al conjunto de todas las redes conmutadas existentes, ahora o en el futuro.

En el caso de la RTC los equipos se conectan a la red pública y en principio cualquier equipo puede comunicar con cualquier otro, siempre que conozca su dirección (número de teléfono). Podemos ver la RTC como una gran nube a la que se conectan multitud de usuarios. Una vez establecido un circuito en RTC la función que éste desempeña para los protocolos de nivel superior es equivalente a la de una línea dedicada.

Es posible la interconexión entre computadoras de redes diferentes (RDSI, RTB o GSM); en cuyo caso la velocidad de transmisión será igual a la mas lenta de las conexiones implicadas; en algunos casos puede ser necesario disponer de equipos o contratar servicios especiales.

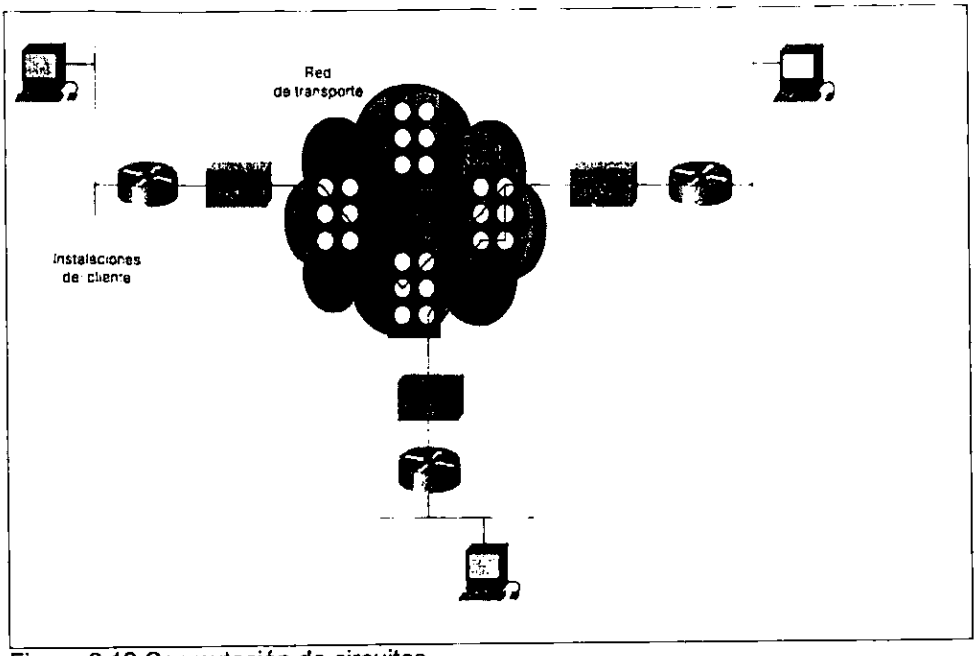

Figura 2.12 Conmutación de circuitos.

2.2.4 Conmutación de paquetes

La conmutación de circuitos aprovecha más la infraestructura de comunicaciones en comparación con las líneas dedicadas, sin embargo aún existen tres inconvenientes:

- En ocasiones no podremos establecer la conexión por no haber circuitos libres, salvo que contratemos un número de circuitos igual al máximo número posible de conexiones simultáneas, lo cual sería muy costoso.

- Que un circuito se esté utilizando no garantiza que se esté aprovechando el ancho de banda que tiene asignado; en nuestro ejemplo cada sucursal está conectada 30 minutos para enviar 2 MBytes de información, que cual supone un aprovechamiento del 14% suponiendo que se trata de conexiones de 64 Kbps.

- El servidor ha de tener una conexión física por cada circuito, aun cuando la ocupación media sea reducida.

Para evitar estos inconvenientes se crearon redes en las que el usuario puede mantener una única conexión física a la red, y sobre ella varios circuitos virtuales con equipos remotos. De esta forma podemos dotar a nuestro ordenador central de treinta circuitos virtuales, con lo que las sucursales siempre van a encontrar un circuito libre sobre el cual establecer la conexión. Al mantener un solo enlace físico el costo de las interfaces, módems, etc., es fijo e independiente del número de circuitos virtuales utilizados. Lógicamente al tener el ordenador central que atender a todas las conexiones por el mismo enlace físico sería conveniente (aunque no necesario) incrementar la velocidad de este; en nuestro ejemplo con conexiones el 2% del tiempo y con un tráfico medio del 14%; para las 30 oficinas agregadas nos daría una ocupación media del 8,4% (0.02x0.14x30) suponiendo un reparto homogéneo (cosa poco probable); como previsiblemente muchas oficinas querrán conectar mas o menos a la misma hora sería conveniente ampliar el enlace del servidor a 128 o 256 Kbps para evitar congestión en horas punta.

Para poder definir circuitos virtuales es preciso disponer de equipos inteligentes en la red que puedan hacer la distribución de los paquetes en función de su destino. Por esto a las redes que permiten crear circuitos virtuales se las denomina redes de conmutación de paquetes, y en cierto sentido podemos considerarlas como la evolución lógica de las redes de conmutación de circuitos. En realidad existen dos tipos de redes de conmutación de paquetes, según ofrezcan

servicios orientados a conexión o no orientados a conexión (envío de datagramas). La primera red de conmutación de paquetes que existió fue como ya hemos visto ARPAnet, pero como no era orientada a conexión no se adaptaba bien a un servicio de compañía telefónica. Para facilitar la facturación las redes públicas de conmutación de paquetes suelen ofrecer servicios orientados a conexión en el nivel de red. Actualmente hay tres tipos de redes públicas de conmutación de paquetes: X.25, Frame Relay y ATM, y todos ofrecen servicios orientados a conexión. Las tres representan implementaciones bastante completas de los tres primeros niveles del Modelo de Referencia OSI, y tienen muchos puntos en común, según veremos a continuación.

La subred de una red de conmutación de paquetes se constituye mediante conmutadores unidos entre sí por líneas dedicadas. La distribución de los conmutadores y la forma como éstos se unen entre sí (es decir la topología de la red) es algo que decide el proveedor del servicio y que fija la carga máxima que la red podrá soportar en lo que se refiere a tráfico entre conmutadores; la topología fija también la fiabilidad de la red, es decir cuan resistente será a fallos de los enlaces (por ejemplo una red muy mallada será muy resistente). Cuando un usuario desea conectar un equipo a la red el acceso se hace normalmente mediante una línea dedicada entre el equipo a conectar y el conmutador mas próximo del proveedor de servicio (normalmente la Compañía Telefónica). La velocidad de la conexión entre el equipo y el conmutador establece de entrada un máximo a las prestaciones que ese usuario podrá obtener de la red. Puede haber además otras limitaciones impuestas por la capacidad de la red, por saturación o porque se hayan impuesto limitaciones de acuerdo con lo contratado por el usuario con el proveedor del servicio.

Aunque se está considerando el caso en que la red de conmutación de paquetes la gestiona una compañía Telefónica (con lo que tenemos una red pública de conmutación de paquetes), también es posible que una organización o conjunto de organizaciones (por ejemplo una gran empresa, una administración o un conjunto

de universidades) establezcan una red privada basada en X.25, Frame Relay o ATM. En este caso normalmente la gestión de la red se asigna a algún grupo especializado (por ejemplo el departamento de comunicaciones en el caso de la empresa) que se ocupa de diseñar topología, solicitar los enlaces correspondientes, instalar los conmutadores, etc. Si se desea que la red privada esté interconectada con la red pública es preciso prever que al menos uno de los conmutadores de la red privada esté conectado con la red pública. Desde el punto de vista técnico ambas redes son equivalentes en su funcionamiento, salvo que normalmente en una red privada o no se tarifica la utilización, por lo que el control no es tan crítico.

En X.25, Frame Relay y ATM existe el concepto de circuito virtual (VC), que puede ser de dos tipos: conmutado o SVC (Switched Virtual Circuit) y permanente o PVC (Permanent Virtual Circuit). El conmutado se establece y termina a petición del usuario, mientras que el permanente tiene que ser definido por el proveedor del servicio, mediante configuración en los conmutadores a los que se conectan los equipos implicados, normalmente mediante modificación contractual con el cliente. En cierto modo es como si los PVCs fueran 'líneas dedicadas virtuales' mientras que los SVCs son como conexiones RTC 'virtuales'.

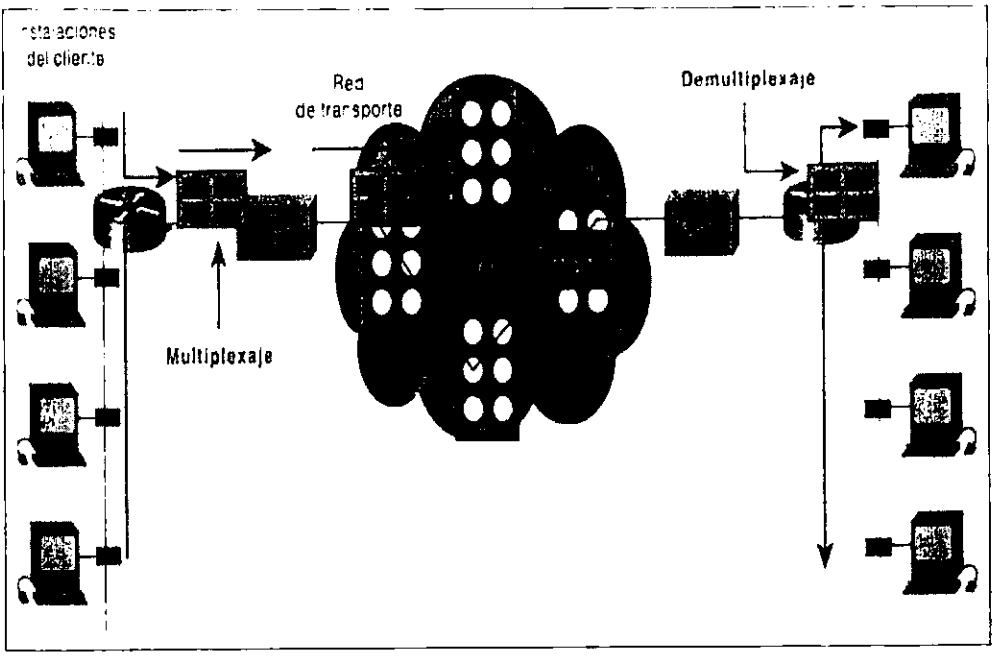

Figura 2.13 Conmutación de paquetes

2.2.4.1. Protocolo X.25

X.25 fue el primer protocolo estándar de red de datos pública. Se definió por primera vez en 1976 por la CCITT (Comité Consultatif International Télégraphique and Téléphonique). Aunque el protocolo ha sido revisado múltiples veces (la última en 1993) ya se ha quedado algo anticuado y no es en la actualidad un servicio interesante, salvo en algunos casos, debido a su baja eficiencia y velocidad; normalmente no supera los 64 Kbps, aunque se pueden contratar conexiones de hasta 2.048 Kbps. A pesar de estas desventajas conviene conocer los aspectos básicos de X.25 pues aun existe una gran cantidad de usuarios de este tipo de

redes. Además, en el protocolo X.25 se definieron por primera vez muchos de los conceptos en que se basa frame relay y ATM, que podemos considerar en cierto sentido como sus descendientes. El conjunto de estándares que definen X.25 ha sido adoptado como parte del modelo OSI para los tres primeros niveles. A nivel físico se definen en X.25 dos interfaces, la X.21 cuando se usa señalización digital (cosa poco habitual) y la X.21bis (un subconjunto de la EIA-232D/V.24) cuando es analógica.

A nivel de enlace se utiliza un protocolo llamado LAP-B (Link Access Procedure-Balanced) que es una versión modificada del estándar ISO HDLC (High-level Data Link Control), que veremos en detalle al estudiar la capa de enlace.

El protocolo utilizado a nivel de red se conoce como X.25 PLP (Packet Layer Protocol). En este nivel se realizan todas las funciones de control de flujo, confirmación y direccionamiento. Cada NSAP (Network Services Access Point) en una red X.25 viene representado por una interfaz de un conmutador X.25, y tiene una dirección única. Las direcciones son numéricas y típicamente pueden tener entre nueve y quince dígitos. Las redes X.25 públicas de muchos países están interconectadas, como ocurre con las redes telefónicas. Para facilitar su direccionamiento la CCITT ha establecido un sistema jerárquico análogo al sistema telefónico en la recomendación X.121; así es posible por ejemplo llamar desde Iberpac (la red X.25 pública española) a una dirección de Transpac (la red pública X.25 francesa), sin más que añadir el prefijo correspondiente a dicha red en la dirección de destino.

X.25 es un servicio fiable orientado a conexión; los paquetes llegan en el mismo orden con que han salido. Una vez establecido un circuito entre dos NSAPs la información se transfiere en paquetes que pueden ser de hasta 128 bytes (aunque en muchas redes se permiten tamaños de hasta 4 KB). En la red los paquetes son transferidos de cada conmutador al siguiente (almacenamiento y reenvío), y solo

borrados cuando se recibe la notificación de recepción. Un mismo NSAP puede tener establecidos varios VCs (PVCs y/o SVCs) hacia el mismo o diferentes destinos.

Los computadoras que se conectan a un conmutador X.25 necesitan tener la capacidad suficiente para procesar los complejos protocolos X.25. Cuando se definió el estándar X.25 los computadoras personales eran caros y poco potentes; muchos usuarios que tenían necesidad de conectarse a redes X.25 no disponían de un ordenador adecuado. Para estos casos se diseñó un equipo capaz de conectar un terminal asíncrono, que trabaja en modo carácter (es decir, un paquete por carácter) a una red X.25. A dicho equipo se le denominó PAD (Packet Assembler Disassembler) ya que se ocupaba de ensamblar y desensamblar los paquetes X.25 que recibía. A través de un PAD un usuario de un PC, o incluso de un terminal 'tonto', podía conectarse a un host en una red X.25 y trabajar como un terminal remoto de aquel. La CCITT publicó tres documentos para especificar todo lo relacionado con el funcionamiento de un PAD: el X.3 describe las funciones propias del PAD, el X.28 define el protocolo de comunicación entre el PAD y el terminal asíncrono, y el X.29 define el protocolo entre el PAD y la red X.25. El uso conjunto de estos tres protocolos permite iniciar una sesión interactiva desde un terminal conectado a un PAD con un ordenador remoto, por lo que se le conoce como el logon remoto XXX. Cuando un usuario en un ordenador conectado a X.25 desea establecer una conexión como terminal remoto de otro ordenador a través de una red X.25 lo hace mediante un programa en su ordenador que emula el comportamiento de un PAD (PAD Emulation). El logon remoto XXX ofrece en redes X.25 un servicio equivalente al de Telnet en TCP/IP. Para el caso de usuarios que no dispongan de un PAD propio muchas compañías telefónicas ponen a su disposición un servicio de acceso a PADs por RTC (normalmente RTB). Este servicio se denomina normalmente X.28, por ser este estándar el que define el protocolo de comunicaciones entre el terminal de usuario y el PAD.

El rendimiento que se obtiene de un VC X.25 depende de muchos factores: velocidad de los accesos físicos implicados, número de VC simultáneos, tráfico en cada uno de ellos, carga de la red, infraestructura, etc.

En España Telefónica inició un servicio de red pública de conmutación de paquetes en 1971 con la red RSAN, basada en unos protocolos propios, no estándar. Esta red hoy desaparecida fue la segunda red de conmutación de paquetes del mundo (después de ARPAnet que empezó en 1969), y la primera establecida por un operador de telefonía. En 1984 Telefónica inició la red Iberpac, que ya obedecía a los estándares X.25. A través de Iberpac es posible acceder a mas de 200 redes similares en todo el mundo. Las velocidades de acceso a Iberpac pueden ser de 2,4 a 2.048 Kbps. Es posible contratar PVCs, aunque lo normal es utilizar SVCs. La tarificación se hace por tres conceptos: en primer lugar una cuota fija mensual según la velocidad de la línea de acceso, en segundo por el tiempo que dura cada llamada (o lo que es lo mismo, el tiempo que esta establecido cada SVC), y en tercer lugar por el número de paquetes transferidos por llamada. Para los dos últimos conceptos existen tres ámbitos de tarificación: nacional, europeo e internacional (en X.25 cuesta lo mismo transferir datos entre dos oficinas vecinas que entre Valencia y La Coruña). Telefónica dispone también de un servicio de acceso X.28 a su red Iberpac, conocido como Datex28.

Los protocolos X.25 se diseñaron pensando en los medios de transmisión de los años setenta, líneas de baja velocidad con tasa de errores elevada. El objetivo era aprovechar lo mejor posible las lentas líneas de transmisión existentes, aun a costa de hacer un protocolo de proceso pesado. Por si esto fuera poco, las redes X.25 casi siempre se utilizan para encapsular tráfico correspondiente a otros protocolos, por ejemplo TCP/IP, SNA o DECNET (podríamos decir que los paquetes de estos protocolos viajan 'disfrazados' en paquetes X.25); cuando se encapsula un protocolo como TCP/IP en X.25 se realizan de forma redundante las tareas de la capa de red,

con lo que el resultado es aún mas ineficiente. Para resolver este tipo de problemas a partir de 1990 se empezaron a crear redes basadas en frame relay.

2.2.4.2 Frame Relay

Frame Relay (que significa retransmisión de tramas) nació a partir de los trabajos de estandarización del servicio RDSI, como un intento de crear una versión 'light' de X.25, que permitiera aprovechar las ventajas de poder definir circuitos virtuales pero sin la baja eficiencia que tenían los protocolos excesivamente 'desconfiados' de X.25. Mientras que en X.25 la capa de enlace y la capa de red eran sumamente complejas en frame relay ambas se intentaron reducir a su mínima expresión, dejando en manos de los equipos finales toda la labor de acuse de recibo, retransmisión de tramas erróneas y control de flujo; de esta forma frame relay se convertía en el complemento perfecto a otros protocolos, tales como TCP/IP. En muchos casos se considera que frame relay no es un protocolo a nivel de red sino a nivel de enlace (de ahí su nombre), y aun visto como nivel de enlace resulta bastante ligero. El servicio que suministra frame relay consiste básicamente en identificar el principio y final de cada trama, y detectar errores de transmisión. Si se recibe una trama errónea simplemente se descarta, confiando en que el protocolo de nivel superior de los equipos finales averigüe por sí mismo que se ha perdido una trama y decida si quiere recuperarla, y como. A diferencia de X.25, frame relay no tiene control de flujo ni genera acuse de recibo de los paquetes (estas tareas también se dejan a los niveles superiores en los equipos finales). El tamaño máximo de los paquetes varía según las implementaciones entre 1 KB y 8 KB. La velocidad de acceso a la red típicamente esta entre 64 y 2.048 Kbps, aunque ya se baraja la estandarización de velocidades del orden de 34 Mbps.

Una novedad importante de Frame Relay estriba en que se define un ancho de banda 'asegurado' para cada circuito virtual mediante un parámetro conocido como

CIR (Committed Information Rate). Un segundo parámetro, conocido como EIR (Excess Information Rate) define el margen de tolerancia que se dará al usuario, es decir, cuanto se le va a dejar 'pasarse' del CIR contratado. Por ejemplo, supongamos que un ordenador se conecta a una red frame relay mediante una línea de acceso al conmutador de 1.984 Kbps, y tiene dos circuitos establecidos con otros dos computadoras, cada uno de ellos con un CIR de 256 Kbps y un EIR de 256 Kbps; en este caso cada circuito tendrá asegurado un ancho de banda de 256 Kbps como mínimo, y si la red no está saturada podrá llegar a 512 Kbps; si un circuito intenta utilizar mas de 512 Kbps el conmutador frame relay empezará a descartar tramas. Obsérvese que en este caso la línea de acceso nunca llegaría a saturarse, ya que como mucho podrían enviarse 512 Kbps por cada circuito. La especificación del CIR para un circuito virtual se hace de forma independiente para cada sentido de la transmisión, y puede hacerse asimétrica, es decir dar un valor distinto del CIR para cada sentido.

Cuando un usuario hace uso del EIR (es decir, genera un tráfico superior al CIR contratado en un circuito virtual) el conmutador frame relay pone a 1 en las tramas excedentes un bit especial denominado DE (Discard Elegibility). Si se produce congestión en algún punto de la red el conmutador en apuros descartará en primera instancia las tramas con el bit DE marcado, intentando resolver así el problema. Este mecanismo permite a un usuario aprovechar la capacidad sobrante en la red en horas valle sin perjudicar la calidad de servicio a otros usuarios en horas punta, ya que entonces se verá limitado a su CIR. En realidad el CIR tampoco está garantizado, ya que si la congestión no se resuelve descartando las tramas DE el conmutador empezará a descartar tramas normales (no marcadas como DE) que pertenecen a usuarios que no han superado su CIR. Afortunadamente las redes frame relay se suelen dimensionar de forma que el CIR de cada usuario esté prácticamente garantizado en cada momento. En cierto modo podemos imaginar el bit DE como un sistema de 'reserva de asiento' en un billete de tren (el bit a 0 significaría en este caso tener hecha reserva).

Una red Frame Relay podría utilizarse en vez de líneas dedicadas para interconectar conmutadores X.25; a la inversa sería mucho más difícil ya que al ser X.25 una red mas lenta los retardos introducidos serían apreciados por los usuarios de Frame Relay.

En ocasiones se utilizan redes Frame Relay para transmitir voz digitalizada; esto no es posible con X.25 debido a la lentitud del protocolo, que introduciría unos retardos excesivos; el envío de voz por una red tiene unos requerimientos especialmente severos en cuanto a retardos para que la transmisión se efectúe correctamente.

La red pública Frame Relay de Telefónica se denomina Red Uno, y esta operativa desde 1992. Aunque Telefónica anunció la disponibilidad de SVCs en Frame Relay para 1997, parece que estos aun no estan disponibles y el único servicio contratable es el de PVCs. La tarificación se realiza por dos conceptos: el primero es una cuota fija mensual en función de la velocidad de acceso a la red; el segundo es una cuota fija al mes por cada circuito según el valor de CIR que se tenga contratado; en ambos casos la tarifa depende de la distancia. El EIR no se especifica en el contrato, y por tanto no se paga, pero tampoco se compromete su valor por parte de Telefónica; habitualmente Telefónica pone un EIR que es 256 Kbps superior al CIR contratado. La velocidad del acceso físico puede tener valores comprendidos entre 64 y 1.984 Kbps. El CIR puede ser de 0 a 1.984 Kbps. Al no existir circuitos conmutados la Red Uno no es una red abierta como lo son Iberpac o la RTC. Es posible la conexión internacional con muchas otras redes frame relay gracias a acuerdos suscritos con diversos operadores.

2.2.4.3 ATM y B-ISDN

Casi todos los servicios de comunicación que hemos visto hasta ahora fueron diseñados para la transmisión de voz o datos, pero no ambos. La RTB y la red GSM, pensadas para la voz, pueden transmitir datos, pero sólo a muy bajas velocidades. Las líneas dedicadas y redes Frame Relay, pensadas para datos, pueden transmitir voz si se utilizan los equipos apropiados y se respetan ciertas restricciones.

El único servicio de los que hemos visto hasta ahora que se diseñó pensando en voz y datos es la RDSI (de ahí el nombre de Servicios Integrados). Pero la RDSI tiene dos inconvenientes importantes:

Al ser una red de conmutación de circuitos reales la reserva del ancho de banda se realiza durante todo el tiempo que esta establecida la comunicación, independientemente de que se estén transfiriendo datos o no (o en el caso de transmitir voz independientemente de que se este hablando o se este callado). Como el teléfono.

El estándar RDSI se empezó a definir en 1984. En aquel entonces las líneas dedicadas eran de 9.6 Kbps en el mejor de los casos y hablar de enlaces a 64 Kbps parecía algo realmente avanzado; sin embargo el proceso de estandarización tardó mas de lo previsto (cosa que ocurre a menudo) y cuando aparecieron los primeros servicios RDSI diez años más tarde la red 'avanzada' resultaba interesante sólo en entornos domésticos y de pequeñas oficinas; se había quedado corta para nuevas aplicaciones.

Hasta aquí sólo hemos hablado de la transmisión de voz o datos, pero las redes de comunicaciones permiten transmitir también otros tipos de información como imágenes en movimiento (videoconferencia o vídeo), que tienen unos requerimientos

distintos. De una forma muy concisa resumimos en la siguiente tabla las características esenciales de cada tipo de tráfico:

Cuando una red está preparada para transmitir tanto audio y vídeo como datos informáticos decimos que es una red multimedia. Generalmente el tráfico multimedia tiene unas necesidades muy variables de ancho de banda, se dice que es un tráfico a ráfagas ('bursty traffic').

Cuando se tiene tráfico a ráfagas resulta especialmente útil disponer de una red de conmutación de paquetes con circuitos virtuales, ya que así unos usuarios pueden aprovechar en un determinado instante el ancho de banda sobrante de otros. Sin embargo las redes de este tipo que hemos visto hasta ahora (X.25 y frame relay) no son apropiadas para tráfico multimedia porque el retardo y el jitter son impredecibles cuando la red esta cargada, y en general son demasiado lentas (especialmente X.25).

Las compañías telefónicas vienen trabajando desde hace bastante tiempo en el diseño de una red adecuada al tráfico multimedia que permita aprovechar las ventajas de la conmutación de paquetes, para así utilizar de forma mas eficiente las infraestructuras y ofrecer servicios nuevos, tales como la videoconferencia o el vídeo bajo demanda. La tecnología que permite todo esto se denomina ATM (Asynchronous Transfer Mode) y sus orígenes se remontan nada menos que a 1968, cuando se concibió en los laboratorios Bell el primer sistema de transmisión de celdas.. En esencia lo que se intenta con esta nueva tecnología es integrar todos los servicios en una única red digital, lo mismo que pretendía la RDSI (aunque como hemos visto llegó demasiado tarde). Por este motivo ATM también se denomina a veces RDSI de banda ancha o RDSI-BA (B-ISDN, Broadband-ISDN); por contraste a la 'antigua' RDSI se la denomina en ocasiones RDSI de banda estrecha o RDSI-BE (N-ISDN, Narrowband-ISDN). Podríamos decir que la RDSI de banda ancha es lo más parecido a las 'autopistas de la información'.

En 1986 la CCITT definió el concepto de RDSI-BA y eligió ATM como la tecnología sobre la que se basarían los futuros estándares. En aquel entonces ATM era una tecnología que interesaba exclusivamente a las compañías telefónicas. Gradualmente los fabricantes de computadoras se fueron percatando de las posibilidades y futuro de dicha tecnología; para acelerar el proceso de estandarización se creó en 1991 el ATM forum, en el que participaban compañías telefónicas y fabricantes de computadoras. A partir de ese momento se ha producido un avance impresionante en las normas y equipos ATM, especialmente en lo que se refiere a redes de datos. El primer conmutador ATM comercial apareció en 1991.

En cierto sentido ATM puede verse como una evolución de frame relay. La principal diferencia es que los paquetes ATM tienen una longitud fija de 53 bytes (5 de cabecera y 48 de datos) frente al tamaño variable y mucho mayor de las tramas frame relay. Debido a su tamaño pequeño y constante los paquetes ATM se denominan celdas, y por esto en ocasiones a ATM se le denomina cell relay (retransmisión de celdas). Manejar celdas de un tamaño tan reducido tiene la ventaja de que permite responder con mucha rapidez a tráfico de alta prioridad que pueda llegar inesperadamente mientras se están transmitiendo otro menos urgente, algo muy importante en tráfico multimedia. El hecho de que todas las celdas sean del mismo tamaño simplifica el proceso en los nodos intermedios, cuestión esencial cuando se quiere que dicho proceso sea lo más rápido posible. En el lado negativo está el hecho de que la eficiencia de una conexión ATM nunca puede superar el 90% (48/53) debido a la información de cabecera que viaja en cada celda.

Al igual que en X.25 o frame relay, una red ATM se constituye mediante conmutadores ATM normalmente interconectados por líneas dedicadas, y equipos de usuario conectados a los conmutadores. Mientras que en X.25 o frame relay se utilizan velocidades de 64 Kbps a 2 Mbps, en ATM las velocidades pueden llegar a 155,52, 622,08 o incluso superiores. La elección de precisamente estos valores se debe a que son los que se utilizan en el nuevo sistema de transmisión sobre fibra

óptica en redes WAN denominado SONET/SDH (Synchronous Optical NETwork/Synchronous Digital Hierarchy), que es el que están utilizando las compañías telefónicas actualmente en las infraestructuras. ATM también puede utilizarse a velocidades inferiores, 34 Mbps e incluso 2 Mbps.

Dos equipos conectados a una red ATM pueden establecer entre si un circuito virtual, permanente o conmutado, y transmitir por él información digital de cualquier tipo. ATM da al usuario muchas mas facilidades que X.25 o frame relay para controlar las características de su circuito virtual: se puede fijar un ancho de banda máximo permitido, un margen de tolerancia sobre dicho máximo, un ancho de banda mínimo garantizado, un ancho de banda asimétrico, un perfil horario de forma que el ancho de banda fluctúe con la hora del día de una forma preestablecida, etc. Además es posible definir prioridades y distintos tipos de tráfico, de forma que se prefiera fiabilidad o rapidez, tráfico constante o a ráfagas, etc.

2.3 VPN (Redes Privadas Virtuales)

Hasta hace poco, siempre había existido una clara división entre las redes públicas y las privadas. Una red pública, como el sistema público telefónico y el Internet, es una gran colección de pares de nodos que intercambian información más o menos libremente. Una red privada está compuesta por computadoras que pertenecen a una sola organización y que comparten información especifica entre ellas. Ellos se han asegurado que serán los únicos en usar la red y que la información que sea transferida solamente podrá ser visualizada por algunos integrantes de la misma. Las típicas redes corporativas LAN o WAN son un ejemplo de las redes privadas. La línea entre una red privada y una pública siempre se ha dibujado en el router (ruteador), donde una compañía levantará un firewall para mantener a los intrusos fuera de la red privada o para eliminar el acceso de sus propios usuarios a las redes públicas.

VPN es un concepto que borra la línea existente entre las redes públicas y privadas, ya que permite crear una red privada segura sobre una red pública como Internet.

2.3.1 ¿Qué es VPN?

Una Red Privada Virtual (VPN) es una forma de simular una red privada sobre una red pública como el Internet. Es llamada "virtual" porque depende de conexiones virtuales que son conexiones temporales que no tienen presencia física pero que consisten de paquetes enviados a través de varias máquinas sobre Internet.

Las VPNs permiten establecer conexiones remotas seguras como en el caso de empleados de ventas o almacenes hacia una red local (LAN) corporativa utilizando la infraestructura de ruteo proporcionada por las redes públicas como Internet. Desde la perspectiva del usuario, la VPN es una conexión punto a punto entre la computadora del usuario y el servidor corporativo. Las conexiones intermedias son irrelevantes porque los datos son transmitidos como si fueran enviados a través de un enlace dedicado.

Como se mencionaba, la tecnología de las VPNs también permiten a una empresa corporativa conectarse con sus oficinas regionales o incluso con otras compañías (Extranets) utilizando una red pública, manteniendo la seguridad en las comunicaciones. Las conexiones por medio de VPN a través de Internet funcionan como una liga de una red WAN entre dos puntos.

En ambos casos, la seguridad que existe al mandar información a través Internet es similar a la que se tiene en una red privada – a pesar del hecho de que la

comunicación ocurra sobre una red pública- de ahí el nombre de "Red Privada Virtual".

La tecnología VPN está diseñada para manejar operaciones distribuidas y operaciones altamente dependientes de otras compañías donde los empleados deben ser capaces de utilizar los recursos centrales, comunicarse entre ellos y las empresas necesitan manejar los inventarios eficientemente para la producción justo a tiempo ("just in time").

Para proveer a los empleados con los medios para poder utilizar recursos corporativos sin importar en donde se encuentren, la corporación debe desarrollar una solución viable y escalable para el acceso remoto. Generalmente las compañías deciden:

1. Formar un departamento para sistemas de información, el cuál es encargado de comprar, instalar y darle mantenimiento a módems compartidos y a la infraestructura de la red privada.
2. Soluciones de valor agregado (Value – Added Networks), donde se paga a una compañía para comprar, instalar y darle mantenimiento a módems compartidos y a la infraestructura de telecomunicaciones.

Ninguna de esas soluciones provee la óptima rentabilidad o escalabilidad en términos de costos, rentabilidad, flexibilidad de administración y demanda para las conexiones. Por eso se necesita buscar un medio donde las organizaciones complementen o reemplacen sus inversiones actuales en módems compartidos y en su infraestructura de redes privadas con una solución más económica basada en la tecnología de Internet. De esta manera las empresas se pueden enfocar en sus negocios con la seguridad de que la accesibilidad nunca estará comprometida y de que la solución más económica esta implementada. El uso de Internet para accesos remotos permite ahorrar grandes cantidades de dinero porque se pueden hacer

llamadas al proveedor de servicios de Internet (ISP) a cualquier lugar en que éste tenga un punto de presencia (POP). Si se contrata un ISP con cobertura nacional es muy probable que la red Local a la que nos queramos conectar esté tan solo a una llamada local de distancia.

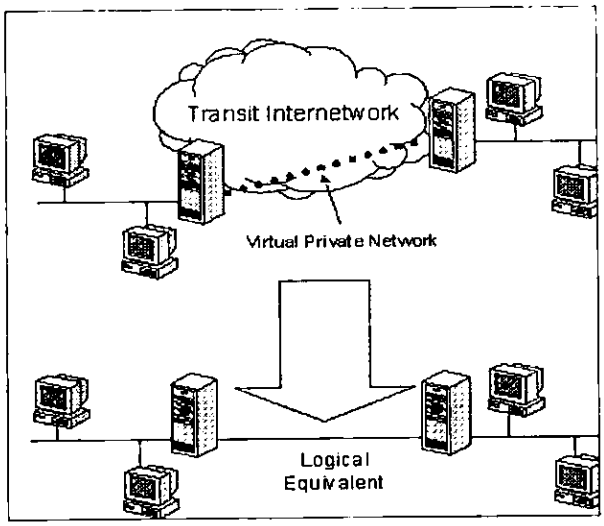

Figura 2.14 Red Virtual Privada (VPN)

En la figura anterior se puede ver la conexión utilizando VPN , en la parte superior donde la nube representa Internet y en la parte inferior se esquematiza una conexión mediante una línea dedicada.

2.3.2 Creación de túneles lógicos.

La creación de túneles lógicos es un método para utilizar una infraestructura de Internet para transmitir datos de una red sobre otra. La información que es transferida puede ser un paquete (o frame) de otro protocolo. En lugar de mandar un paquete como se produce en el nodo origen, el protocolo del túnel lo encapsula en

un encabezado adicional. El encabezado adicional provee la información de la ruta para que el paquete encapsulado pueda atravesar la red intermedia.

Entonces, los paquetes encapsulados son enrutados entre los puntos finales del túnel sobre el Internet. La ruta lógica a través de la cual los paquetes encapsulados viajan sobre el Internet es llamada túnel. Una vez que los paquetes encapsulados alcanzan su destino a través del Internet, son desencapsulados y reenviados a su destino final. Nótese que la creación del túnel lógico incluye el proceso completo (encapsulación, transmisión y desencapsulación de paquetes).

La tecnología de túneles ha existido desde hace algún tiempo. Algunos ejemplos de estas tecnologías son:

- **SNA sobre redes IP.** Cuando el tráfico de SNA (Sistema de Arquitectura de Red) o (System Network Architecture) es enviado a través de las redes IP, el paquete de SNA es encapsulado en un UDP (Protocolo de Unidad de Datos) y un encabezado IP.

- **IPX para Novell Netware sobre redes IP.** Cuando un paquete IPX es enviado a un servidor NetWare o un ruteador IPX, el servidor o el ruteador envuelven el paquete IPX en un UDP (Protocolo de Unidad de Datos) y un encabezado IP, entonces lo envían a través de la red IP. El ruteador destino remueve el UDP y el encabezado IP, enviando el paquete al destino IPX.

Adicionalmente, nuevas tecnologías de túneles han sido introducidas recientemente. Esas nuevas tecnologías incluyen:

- **Protocolo punto a punto para túneles (PPTP).** PPTP permite que el tráfico de IP, IPX o NetBEUI sea encriptado y entonces encapsulado en un encabezado IP

para ser enviado a través de la red IP corporativa o una red IP pública como Internet.

- **Protocolo de la capa 2 para túneles (L2TP).** L2TP permite que el tráfico de IP, IPX o NetBEUI sea encriptado y enviado sobre algún medio que soporte la entrega de datagramas de punto a punto como IP, X.25, Frame Relay o ATM.

- **Seguridad IP (IPSec Tunnel Mode).** IPSec permite encapsular las transferencias de IP utilizando un encabezado adicional para ser enviado a través de la red IP corporativa o la red IP pública como el Internet.

A continuación se mostrará una figura donde se esquematiza un túnel lógico creado a través del Internet:

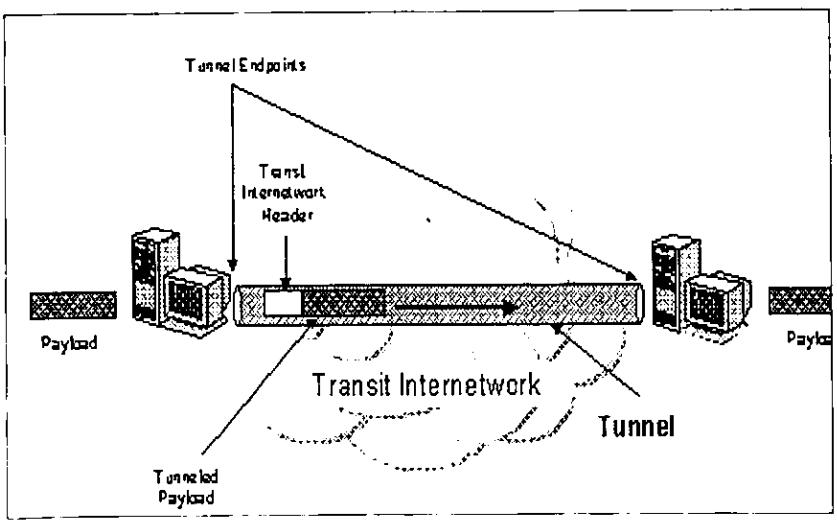

Figura 2.15 Túnel lógico

Observe que la nube representa cualquier red – el Internet es una red pública y es la red mundial más conocida, Hay muchos ejemplos de túneles que son creados Sobre redes corporativas (Intranet). Y aunque Internet representa la red más costeable, se puede utilizar cualquier otra red pública o privada para construir el túnel.

Para que un túnel sea establecido, tanto el cliente como el servidor deben estar utilizando el mismo protocolo.

La tecnología de túneles puede estar basada en los protocolos de túneles de la capa 2 o 3. Esas capas corresponden al modelo de referencia de los Sistemas Abiertos de Interconexión (OSI). Los protocolos de la capa 2 corresponden a la capa den Enlace de Datos y utilizan las tramas como su unidad de intercambio. PPTP, L2TP y L2F (Reenvío de capa 2) son protocolos de túneles que trabajan en la capa 2; ellos encapsulan la información enviada en una trama del protocolo punto a punto (PPP) para ser enviado a través de la red. Los protocolos de la capa 3 corresponden a la capa de Red y utilizan paquetes. IP sobre IP e IPSec son ejemplos de los protocolos de túneles que actúan sobre la capa 3. Esos protocolos encapsulan los paquetes IP en un encabezado adicional de IP antes de enviarlos a través de las redes IP.

Los túneles pueden ser creados de diferentes formas:

- **Túneles voluntarios.** Una computadora de un cliente puede mandar una solicitud a la VPN para configurar y crear túneles voluntarios. En este caso, la computadora del cliente es uno de los extremos del túnel y actúa como el cliente del túnel. Actualmente estos tienden a ser los más utilizados.

  Un túnel voluntario ocurre cuando una estación de trabajo o un ruteador usa un software de túnel cliente para crear una conexión virtual hacia el servidor del

túnel. Para llevar a cabo esto, se debe instalar el protocolo adecuado en la PC del cliente (sin importar si se conecta por medio de una LAN o por marcación telefónica).

En el caso de la marcación telefónica, el cliente debe establecer la conexión hacia la red antes de que el se configure el túnel. El mejor ejemplo para esto es el usuario de Internet que debe llamar a un IPS (proveedor de servicios de Internet) para obtener una conexión a Internet antes de que el túnel pueda ser creado.

Para una PC conectada a una LAN, el cliente cuenta con la conexión hacia red mundial que puede proveer la ruta de las transmisiones hacia el servidor LAN del túnel. Un ejemplo sería el caso de un cliente en una LAN corporativa que inicia un túnel para alcanzar una red privada o una subred oculta en la misma LAN.

Comúnmente existe una falsa concepción de que las VPNs necesitan una conexión de marcado telefónico. Ellas solamente requieren una red IP. Algunos clientes (como las PCs de las casas) utilizan las conexiones de marcado telefónico para establecer el transporte IP. Esto sólo es un paso preliminar en la creación de un túnel y no es parte del protocolo del túnel.

- **Túneles obligatorios.** Un servidor VPN de acceso configura y crea un túnel obligatorio. En un túnel obligatorio, la computadora del usuario no es un extremo del túnel. Otro dispositivo, el servidor remoto de acceso entre la computadora del usuario y el servidor del túnel es el final del mismo y actúa como el cliente del túnel.

Algunos proveedores que venden servidores e acceso por marcado telefónico han implementado la capacidad de poder crear un túnel a partir del cliente que está marcando. La computadora o el dispositivo de red que provee el túnel para el cliente es conocido variablemente como procesador de aplicación (FEP) en PPTP, concentrador de acceso L2TP (LAC) o Acceso de seguridad en IPSec.

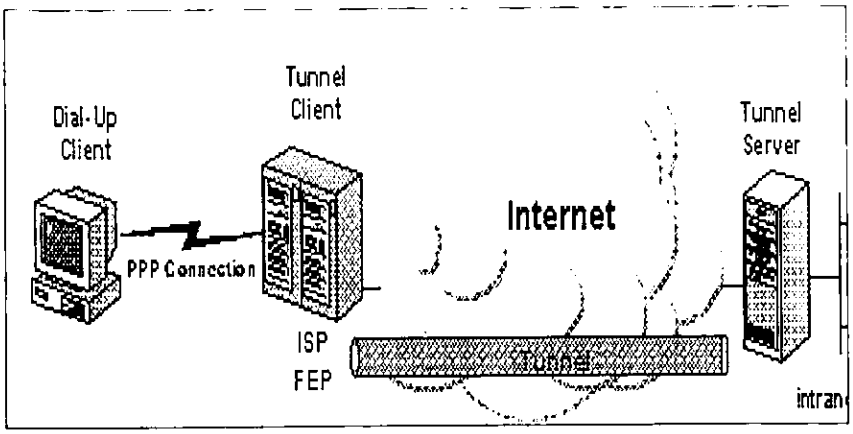

Figura 2.16 Túnel obligatorio

Esta configuración es conocida como túnel "obligatorio" porque el cliente obligado a utilizar el túnel creado por el FEP (procesador de aplicación). Una vez que la conexión inicial es establecida, todo el tráfico de la red desde y hacia el cliente es enviado automáticamente a través del túnel. Con los túneles obligatorios la computadora del cliente realiza una conexión punto a punto y cuando el cliente marca hacia el NAS (servidor de acceso) se crea un túnel y todo el tráfico es enviado a través de él. Un FEP puede ser configurado para que todas las llamadas de un cliente sean canalizadas hacia un servidor de túnel específico.

A diferencia de los túneles voluntarios creados por cada cliente, un túnel entre el FEP y el servidor del túnel puede ser compartido por múltiples clientes. Cuando un segundo cliente marca hacia el servidor de acceso para alcanzar un destino para el cuál ya existe un túnel, no es necesario crear una nueva instancia del túnel entre el FEP y el servidor del túnel. Desde que puede

haber múltiples clientes en un túnel, el túnel no puede ser cerrado hasta que el último usuario se desconecte.

2.3.3 Requerimientos básicos de una VPN

Generalmente cuando se desarrolla una solución de red, una empresa desea facilitar el "acceso controlado" a los recursos de información corporativos. La solución debe permitir que los clientes remotos, que estén debidamente autorizados, se puedan conectar fácilmente a los recursos de la LAN (red de área local) corporativa y también debe permitir que las oficinas remotas se conecten con cualquier otra para compartir recursos e información (conexiones LAN a LAN). Finalmente, se debe asegurar la privacidad y la integridad de la información que viaja a través de las redes públicas. Lo mismo se aplica para la información confidencial que viaja a través de una red corporativa (Intranet). Por esto, una solución por medio de VPN debe proveer lo siguiente:

- **Autenticación de usuarios.** Se debe verificar la identidad de los usuarios y restringir el acceso de la VPN a usuarios autorizados. Además se debe contar con registros de auditoría para mostrar qué información es accesada y por quién.

- **Administración de direcciones.** Se debe asignar una dirección a cada cliente sobre la red privada, asegurándose de que esas direcciones permanezcan privadas.

- **Encriptación.** La información transmitida sobre la red pública debe ser enviada de tal forma que los usuarios no autorizados sean incapaces de
- interpretarla.

- **Administración de llaves.** Se deben generar y actualizar las llaves de encriptación para el cliente y el servidor.

- **Soporte multiprotocolo.** La solución debe se capaz de manejas protocolos utilizados comúnmente en la re pública. Eso incluye al protocolo de Internet (IP) y al de intercambio de paquetes de Internet (IPX) entre otros.

Una solución de VPN basada en el protocolo PPTP (protocolo punto a punto para túneles) o en el protocolo L2TP (protocolo de la capa 2 para túneles) cumplen con todos esos requerimientos básicos y toman ventaja de la amplia disponibilidad mundial del Internet. Otras soluciones, incluyendo el reciente protocolo IPSec (Protocolo de Seguridad IP), cumplen con algunos de estos requerimientos, pero son útiles para algunas situaciones específicas.

2.3.4 Usos comunes de VPN

- **Acceso remoto de usuarios mediante Internet.**

Las VPNs proveen acceso remoto a servicios corporativos sobre la red pública (Internet) manteniendo la privacidad de la información. La figura siguiente muestra una VPN utilizada para conectar a un usuario remoto con una Intranet corporativa.

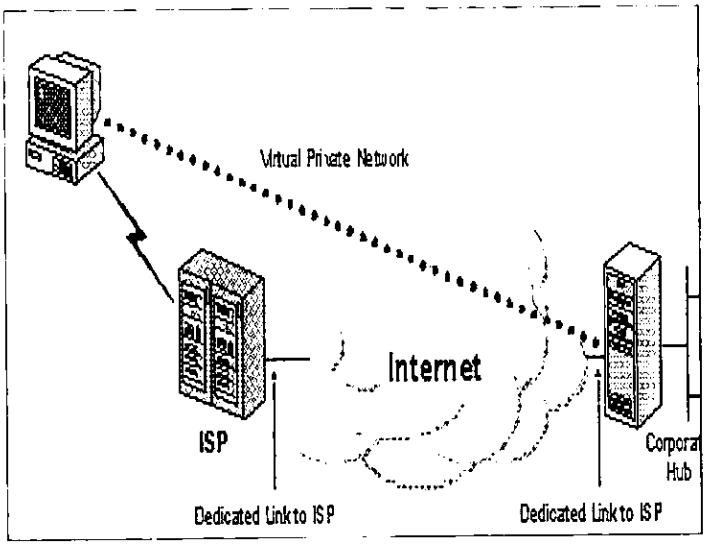

Figura 2.17 Conexión mediante una VPN de un usuario remoto a una LAN privada

En lugar de utilizar una línea dedicada, o una llamada de larga distancia (o 1-800) hacia el servidor de acceso a la red "NAS" (Network Acces Server) de la corporación, el usuario primero hace una llamada al NAS del proveedor local de Internet (ISP). Utilizando la conexión local hacia el ISP, el software de la VPN crea una red virtual privada entre el usuario que hace la llamada y el servidor corporativo de la VPN a través del Internet.

- **Conexión de redes sobre Internet.**
  Existen dos métodos para conectar redes LAN a sitios remotos:

a) **Usando líneas dedicadas para conectar una oficina regional con una LAN corporativa.** En lugar de utilizar un circuito dedicado de larga distancia entre la

oficina regional y el concentrador (hub) corporativo, que resulta ser muy costoso, ambas partes pueden usar un circuito dedicado y un ISP local para conectarse al Internet. El software de la VPN utiliza las conexiones locales del ISP y el Internet para crear una red virtual privada entre el ruteador (router) de la oficina regional y el de la red LAN corporativa.

b) **Utilizando una línea telefónica para conectar una oficina regional con una LAN corporativa.** En lugar de tener un ruteador (router) en la oficina regional haciendo una línea dedicada, una llamada de larga distancia (o 1 –800) hacia el NAS corporativo, el ruteador de la oficina regional puede llamar al ISP local. El software de la VPN utiliza las conexiones locales del ISP y el Internet para crear una red virtual privada entre el ruteador (router) de la oficina regional y el concentrador (hub) de la red LAN corporativa.

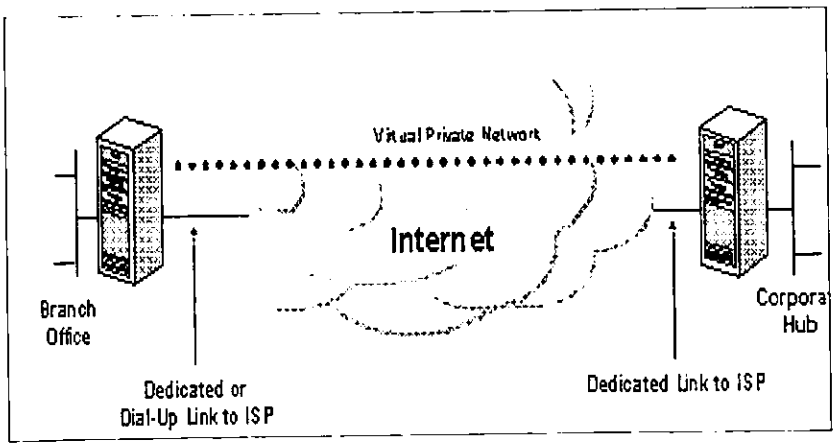

Figura 2.18 Conexión de dos sitios remotos utilizando VPN

Nótese que en ambos casos, la conexión que se hace entre la oficina regional y la corporativa es local. Los costos por la conexión del servidor del cliente y el servidor central son ampliamente reducidos por el uso de un número telefónico local.

Es recomendable que el concentrador (hub) corporativo que actúa como el servidor VPN sea conectado al ISP local mediante una linea dedicada. Este servidor VPN debe estar recibiendo las 24 horas del día el tráfico de la VPN.

- **Conexión de computadoras sobre una intranet.**

En algunas redes corporativas, la información es tan importante que algunos departamentos están físicamente desconectados de la intranet formando una LAN independiente. Mientras esto protege la información confidencial crea problemas de accesibilidad para aquellos usuarios que no están conectados físicamente a la LAN.

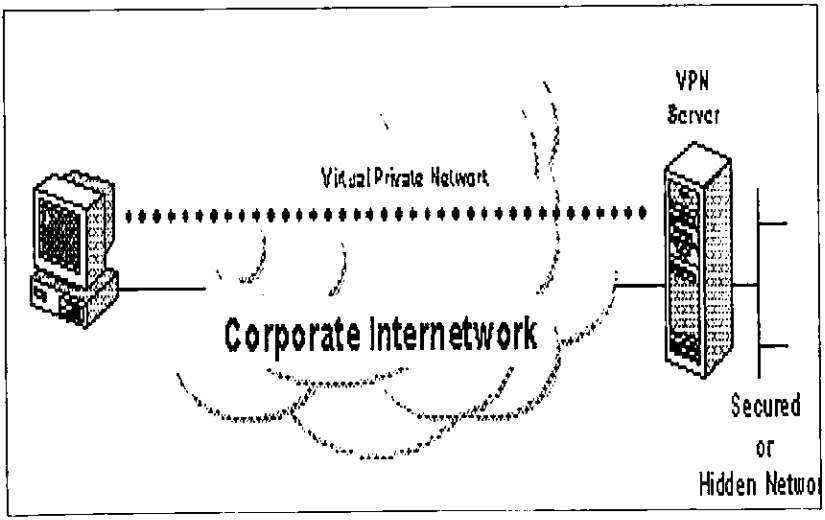

Figura 2.19 Conexión de dos computadoras en una intranet mediante VPN

VPN permite que la LAN departamental esté físicamente conectada a la intranet pero separada por un servidor VPN. Nótese que el servidor VPN no está actuando como un ruteador entre la intranet corporativa y la LAN departamental. Un ruteador conectaría ambas redes, permitiendo que todos accesaran a la red LAN

departamental. Usando VPN, el administrador puede asegurarse que sólo aquellos usuarios de la intranet que tengan la autorización necesaria podrá establecer una conexión con el servidor de la VPN para obtener el acceso a los recursos protegidos de los departamentos. Adicionalmente, todas las comunicaciones a través de la VPN pueden ser encriptadas para obtener confidencialidad de información. Aquellos usuarios que no tengan el permiso necesario no podrán accesar a la LAN departamental.

CAPITULO 3. CASO PRACTICO

Como ya hemos visto, el servicio de la red con el que cuenta la empresa está funcionando adecuadamente, ya que los usuarios de sistema pueden hacer uso de los servicios de Internet y además pueden accesar al servidor AS/400 sin ningún problema, pero es necesario reducir los costos de telefonía que producen las conexiones remotas a los diferentes almacenes. Para darnos una idea de estos costos a continuación se darán algunos ejemplos reales de los mismos:

Concepto	Contratación	Renta Mensual	Renta Anual
Ladaenlace local de 64 Kbps Darwin – Cautitlán (18 de septiembre de 2000)	$ 25,816.00	$ 1,814.00	$ 21,768
Ladaenlace internacional de 64 kbps Darwin - Nuevo Laredo Tramo Nacional Tramo Internacional (USD) (5 de enero de 1999)	 $ 31,334 $ 2,252	 $ 15,667 $ 1,160	 $ 188,0004 $ 13,920
Ladaenlace nacional de 64 kbps Darwin – Sonora (28 de diciembre de 1998)	$ 24,258	$ 7,101.19	$ 85,214.28

Figura 3.1 Costos de enlaces dedicados

Las características de estos enlaces son las siguientes:

- Los precios no incluyen I. V. A.
- Ancho de banda garantizado de 64 Kbps.
- Cuentan con alto índice de confiabilidad
- Para transmisión de voz y/o datos se requiere equipo adicional por parte del cliente.

Como pudimos ver en la tabla anterior el costo por tener este tipo de enlaces es sumamente alta aún sin tomar en cuneta la compra del equipo necesario para hacer uso de los mismos. En contraste, para poder instalar una VPN se necesita lo siguiente:

- Un módem con Microsoft TCP/IP, FTP OnNet versión 2.0.

- El usuario remoto debe de contar con el servicio de Internet. El costo de este servicio depende del proveedor que se elija, pero se pueden encontrar servicios de este tipo desde $200 mensuales.

- Debe instalarse un software del lado del cliente para que lleve a cabo la emulación de la red privada sobre Internet. Para este fin, el usuario debe tener un sistema operativo Windows 95 , Windows 98 o Windows NT 4.0 Service Pack 3 corriendo en una PC con un CPU 486/33 y 1 MB disponible en el disco duro.

- En el lado del proveedor de los servicios se debe instalar y configurar las VSU (VPN Service Unit) o Unidad de Servicio de VPN. VSU es un elemento de la red que utiliza los protocolos y algoritmos estándares de seguridad para proveer el servicio de la VPN (compresión, encriptación, autenticación, y administración).

El costo de los elementos para armar la VPN que necesitamos no sobrepasa los $150,000, y el pago mensual por la conexión, aún cuando la empresa pagara los servicios de conexión a Internet, no costaría mas de $5000.

Existen diferentes proveedores en el mercado que ofrecen los elementos para instalar una VPN, la decisión de qué software se empleará quedará en manos del responsable del proyecto, el cuál deberá evaluar los beneficios y desventajas del mismo. A continuación se muestra un ejemplo de la instalación utilizando un software llamado VPNet:

En el servidor (VSU)

Se tienen que dar de alta las cuentas de los clientes que accesarán a la red, por medio del panel de configuración.

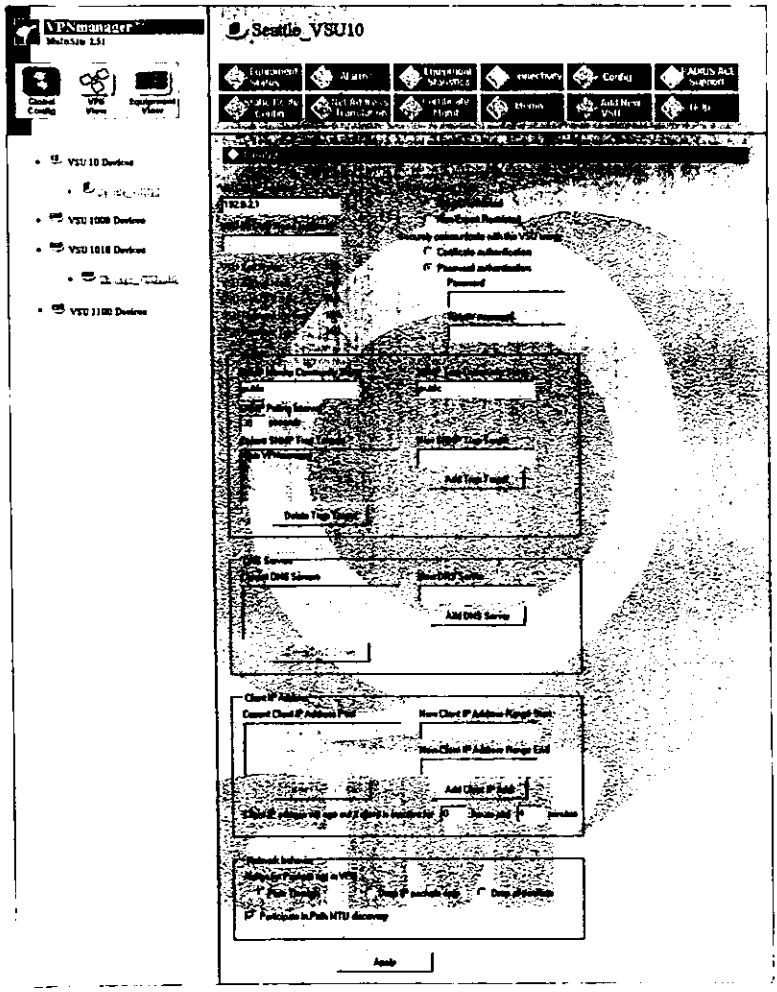

Figura 3.2 Panel de configuración de la VSU

En el cliente.

Este es un cliente remoto que se conectará por medio de un módem a un ISP para poder accesar al servidor de red remoto.

1. Se tiene que modificar el archivo lmhosts.sam que se encuentra en el directorio de Windows, utilizando el bloc de notas para agregar la dirección del servidor al que nos conectaremos.

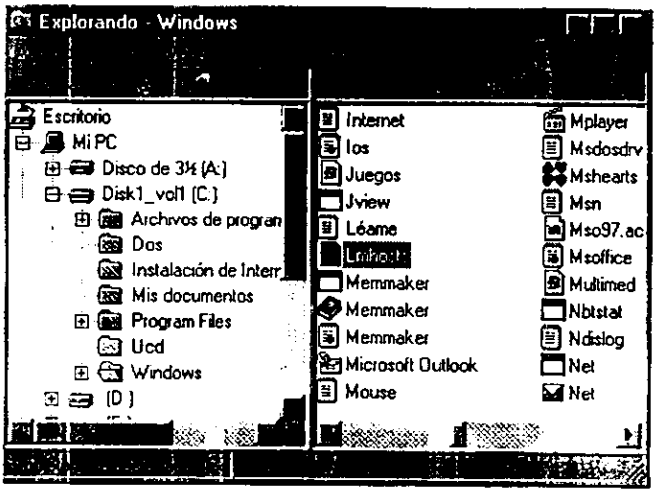

Figura 3.3 Localización del archivo lmhosts.sam

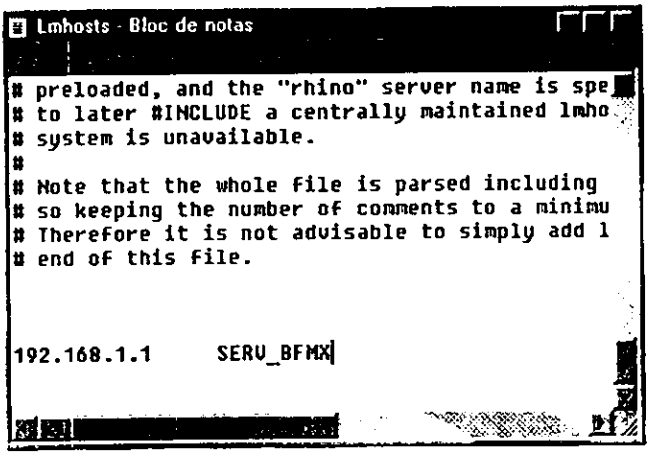

Figura 3.4 Edición del archivo lmhosts

2. Después de que se editó el archivo, hay que renombrarlo como lmhosts (sin extensión). Esto se puede hacer desde una sesión de MSDOS o desde la opción ejecutar que se encuentra en el botón de inicio de la barra de tareas

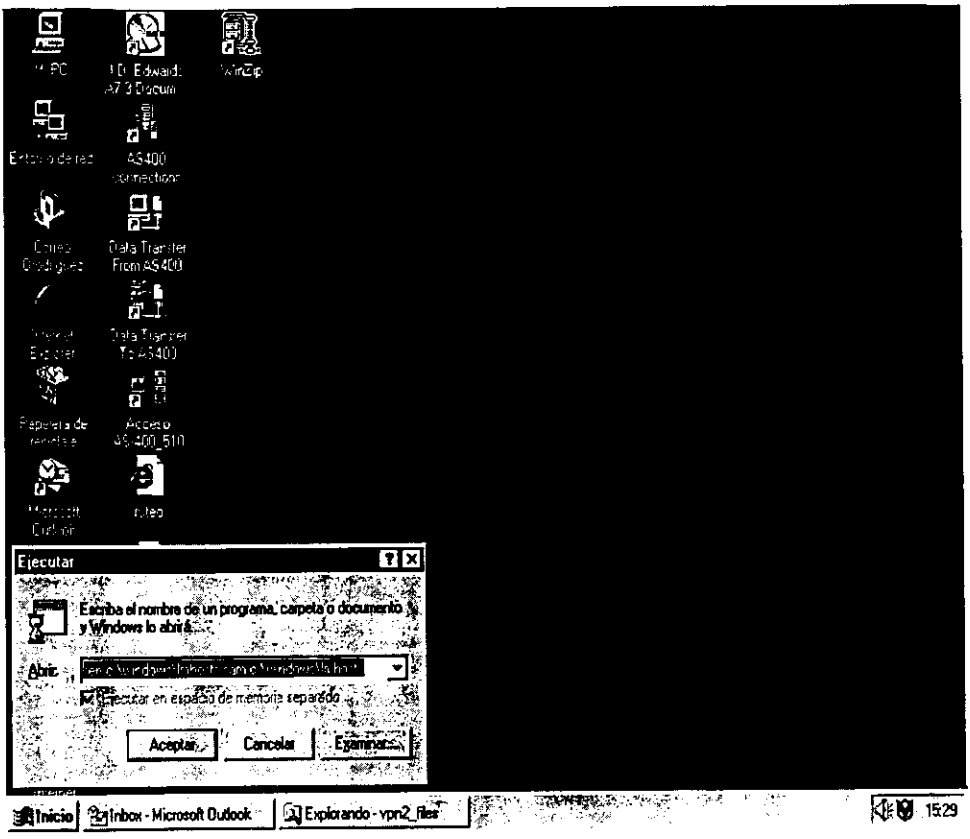

Figura 3.5 Renombrar archivo lmhosts

3. Si la computadora cuenta con una tarjeta de red instalada, ésta deberá ser inhabilitada. Para hacer esto, hay que selecccionar Mi PC y hacer un click con el boton derecho, posteriormente hay que seleccionar la pestaña de Administrador de dispositivos. Una vez localizada la tarjeta de red hay que seleccionarla y presionar el botón de propiedades, entonces aparecerá una ventana donde habilitará la opción para especificar que sea desabilitada.

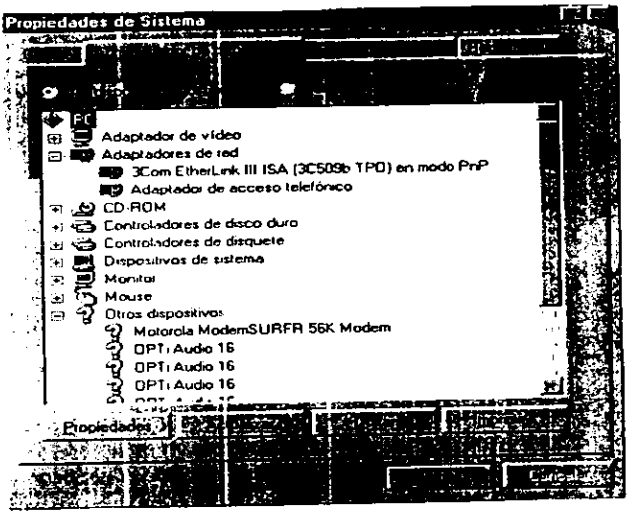

Figura 3.6 Administrador de dispositivos

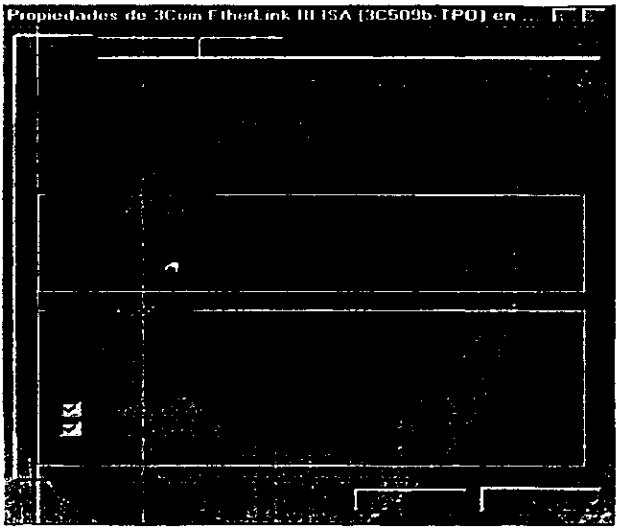

Figura 3.7 Propiedades de la tarjeta de red

4. Una vez concluido lo anterior, hay que correr el programa ejecutable que instalará el software en la PC, donde en la sección del adaptador utilizado para la VPN se seleccionará el adaptador de acceso telefónico (módem). Finalmente, al terminar el programa de instalación, se reiniciará la PC.

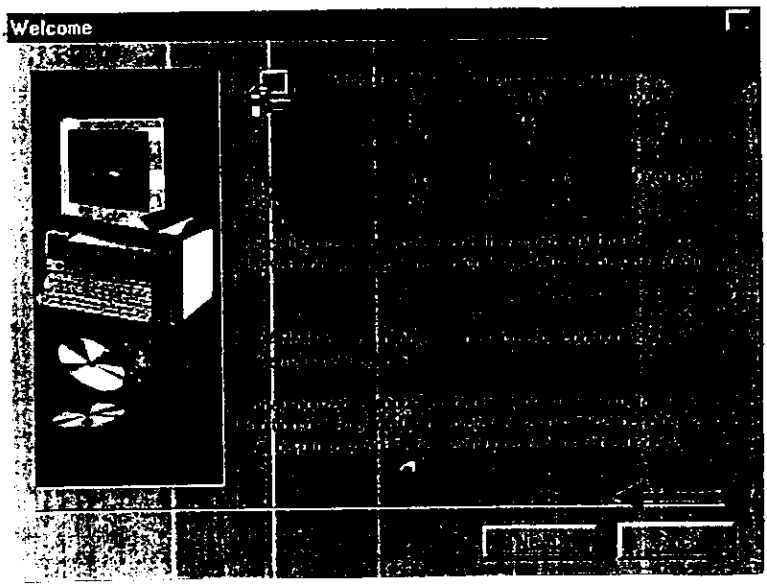

Figura 3.8 Pantallas de instalación

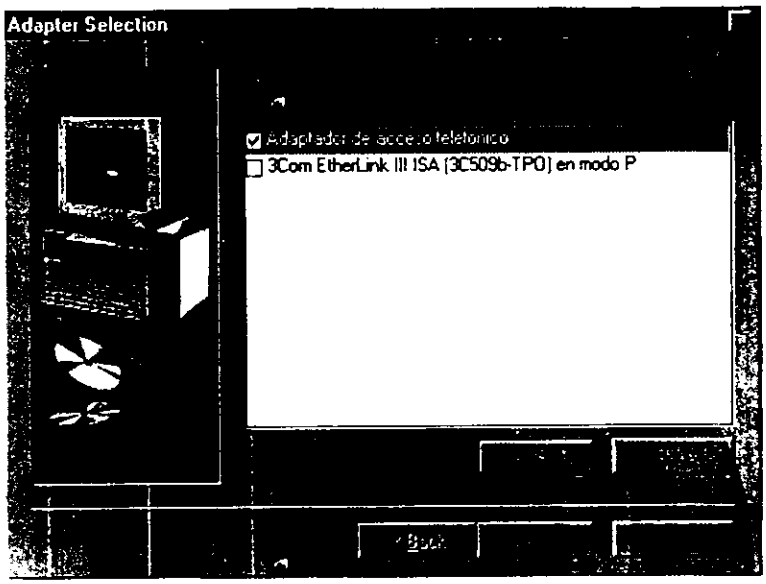

Figura 3.9 Selección de adaptador.

5. Cuando la máquina sea reinicializada, hay que ejecutar el programa "VPNremote for Windows 9x" que se encuentra en el menú "Programas" del botón de "Inicio" de Windows.

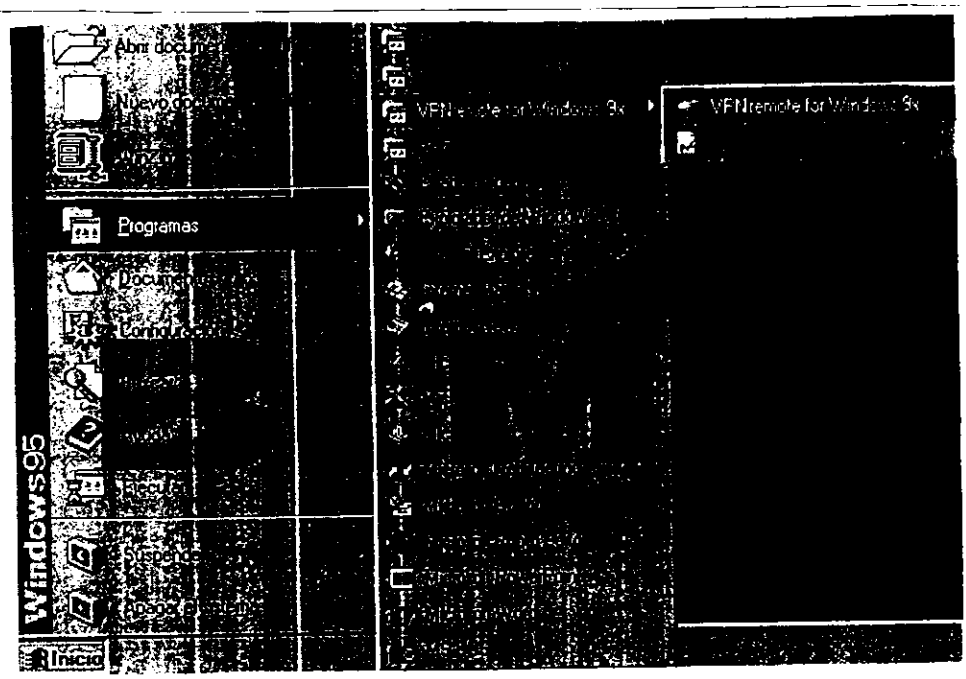

Figura 3.10 Selección del software

Aparecerá una pantalla donde se indica que el software no está configurado, hay que activar el botón que permite cargar la configuración desde el mismo servidor (Download Configuration).

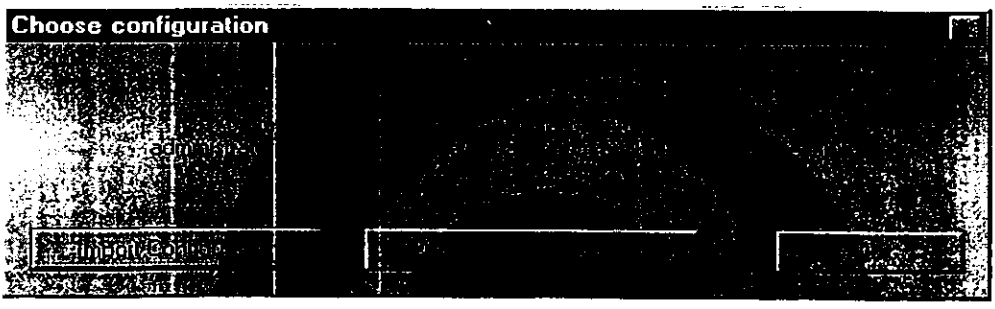

Figura 3.11 Configurar aplicación

Aparecerá otra pantalla donde hay que escribir la dirección IP del servidor de VPN (VSU) y el número de certificado del mismo.

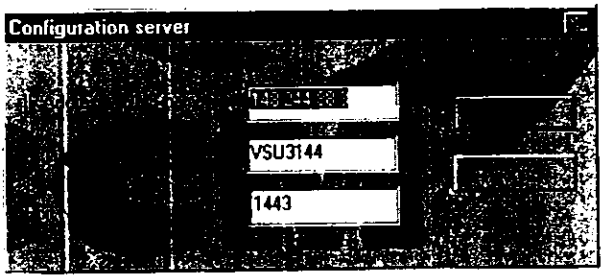

Figura 3.12 Configurar servidor

Finalmente aparecerá la pantalla de la aplicación, la cuál se activará en las siguientes ocasiones en que se ejecute la aplicación.

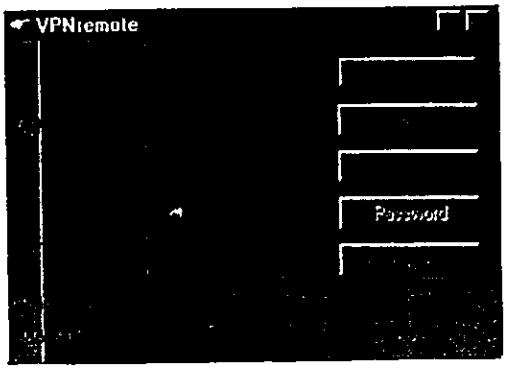

Figura 3.13 Aplicación

CONCLUSIONES

De acuerdo con la información que se ha mostrado aquí, podemos ver que con la utilización de una red VPN se decrementan considerablemente los costos por conexiones remotas, además de que no necesitamos de una gran infraestructura para poder darle un servicio a un cliente remoto.

Otra de las ventajas que ofrece el utilizar este tipo de enlaces es que el usuario no necesita de una gran capacitación, esto debido a que el software que se instala en el cliente es fácil de utilizar, ya que prácticamente se tiene que activar un switch después de conectarse a Internet.

Por otra parte, las VPNs son tan seguras como las redes privadas porque se valen de las mismos mecanismos de defensa para poder evitar la entrada de personas ajenas y así proteger la información crítica de las empresas.

El único inconveniente que existe hasta ahora con este tipo de redes, es el tráfico que se genera y la calidad del servicio dependen en gran parte del ISP (Proveedor de servicios de Internet).

Finalmente a pesar de los inconvenientes que pueden presentarse con estos enlaces, son mayores los beneficios que se tienen especialmente en el aspecto económico, por lo que hace de estos enlaces una buena opción para aquellas empresas que necesiten conectarse a diferentes partes de todo el mundo.

BIBLIOGRAFÍA

Andrew Hopper, Steven Temple, Robin Williamson.
Local area network design.
Editorial Adison-Wesley, 1986

Charlie Scott, Paul Wolfe, Mike Erwin.
Virtual Private Networks
O'Relly and Associates, 1991

Comer, Douglas
Internetworking with TCP/IP
Prentice Hall International, 1991

Gilbert Held.
Network management: techniques, tools and systems.
Editorial Artech, 1989

Schartz, Mischa
Telecomunication Networks – Protocols, Modeling and Analysis.
Adison-Wesley, 1987

Tanembaum, Andrew S.
Redes de Ordenadores
Prentice Hall Hispanoamericana, 1991

Uyless Black.
Redes de computadoras: protocolos, normas e interfaces.
Editorial Macrobit, Ra-ma. 1990

REVISTAS CONSULTADAS

EMPRESAS/400, No. 17
LOS ORÍGENES DE LA PLATAFORMA

EMPRESAS/400, No. 18
Una solución ERP para industrias

EMPRESAS/400, No. 18
J.D Edwards crece y consolida su liderazgo en el mercado de soluciones empresariales

DIRECCIONES URL

http://enete.us.es/indice.html

http://wwwhost.ots.utexas.edu

http://cs.wpi.edu

ÍNDICE DE FIGURAS