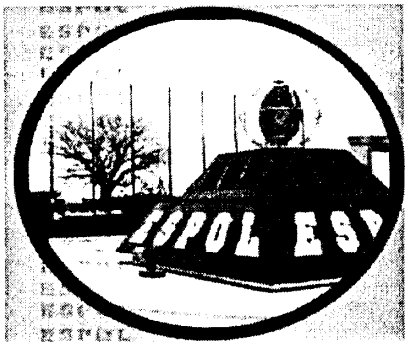


ESCUELA SUPERIOR POLITECNICA DEL LITORAL

FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACION

PROYECTO DE TÓPICO DE GRADUACIÓN
previo a la obtención del título de:
Ingenieros en electricidad
especialización: electrónica

TEMA:

"Diseño de una intranet usando tecnología VPN (Virtual Private Network), que comunique la matriz de SECOHI con sus oficinas sucursales y que además permita el acceso remoto de usuarios móviles"

Presentado por:

Kena Karol Tejada Zúñiga
Silvia Karina León Guerrero
Christian Rafael Astudillo Avila

Guayaquil - Ecuador

2001

AGRADECIMIENTO

A LA ESCUELA SUPERIOR POLITECNICA
Por acogernos durante estos años.

ANUESTROSPADRES
Por su paciencia y apoyo.

A MI HERMANO
Por su apoyo incondicional.

A NUESTROS HIJOS
Por su comprensión, inocencia y ternura.

A TODOS LOS PROFESORES
Por las enseñanzas que aportaron para formar estos nuevos profesionales.

AL ING BORIS RAMOS
Director de Tesis.
AL ING WASHINGTON MEDINA
Profesor del Tópico de Graduación.
Por su ayuda y colaboración.

DEDICATORIA

A DIOS.

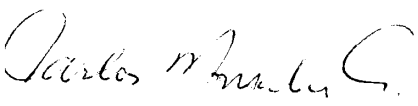
A NUESTROS PADRES.

A MI HERMANO ANDRES.

A MI PEQUEÑA DIANITA.

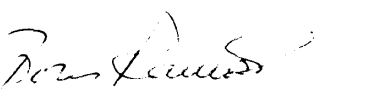
A MI PEQUEÑO JOSUE.

TRIBUNAL DE GRADO



Ing. Carlos Monsalve.

Presidente del Tribunal.

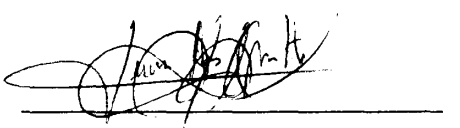


Ing. Boris Ramos.

Director del Tópico.

Ing. Guido Caicedo.

Miembro del Tribunal.



Ing. Juan Carlos Avilés.

Miembro del Tribunal.

“La responsabilidad por los hechos, ideas y doctrinas expuestos en esta tesis, nos corresponden exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral”. (Reglamento de Exámenes y Títulos profesionales de la ESPOL)

Kena Karol Tejada Zúñiga

Silvia Karina León Guerrero

CIB - ESPOL

Christian Rafael Astudillo Avila

CIB - ESPOL

RESUMEN

Desde un principio, el tema de las VPN nos atrajo debido a que constituye en sí una solución no muy difundida en nuestro país con enormes ventajas para aquellas empresas y corporaciones que tienen sucursales en distintas partes de un país o del mundo y que buscan una alternativa más económica al momento de interconectar sus redes. La característica principal de esta tecnología es usar los enlaces de una infraestructura desarrollada como lo es el Internet.

De esta forma redes locales independientes pueden compartir recursos e interactuar entre sí. El nombre virtual se debe a que no se utilizan enlaces privados, sino públicos, garantizando una alta confidencialidad gracias a las nuevas técnicas de seguridad existentes.

Esto, sin duda, trae el atractivo beneficio de reducir el costo derivado de la infraestructura que requiere una red privada convencional por enlaces dedicados a más de un 50%. Además de permitir que un usuario móvil pueda accesar a la intranet desde cualquier lugar donde exista un punto de acceso a Internet.

Nuestro trabajo ha consistido en la recopilación, análisis y organización de toda la información referente a las VPN, que nos permita tener una visión amplia del funcionamiento de las mismas, así como de sus beneficios y aplicaciones. Todo esto con el objeto de demostrar cuán funcional, prácticas, fiables y económicas son las VPN comparadas con las redes privadas convencionales que además son afectadas por el factor ubicación de sus oficinas sucursales.

INDICE DE CAPÍTULOS

INDICE GENERAL

Capítulo 4.

Capítulo 5.

INDICE DE FIGURAS

LISTA DE TABLAS

Capítulo 1.

1. Descripción general de una red.

1.1. ¿Qué es una red?

A través del tiempo las organizaciones han tenido la necesidad de que su información fluya, en el menor tiempo posible, para mejorar sus procesos e incrementar sus ventas. Por tal razón, las empresas adquirieron sistemas de comunicación que enlazaron sus medios de almacenamiento de información. La interconexión de estos medios recibió el nombre de redes.

Una red es un conjunto de computadoras y dispositivos de transmisión que se acoplan mediante líneas de comunicación y protocolos de software que permiten intercambiar datos en forma rápida y confiable, a la vez que comparten sus recursos.

Para describir como funciona una red se puede pensar, por un momento, en el servicio de correos.

Cuando alguien desea mandar una carta a otra persona primero la escribe, la guarda en un sobre con el formato respectivo impuesto por el correo, la sella e introduce en un buzón. La carta será recogida, y clasificada posteriormente por el personal de correos, según su destino y enviada a través de los medios de transporte correspondientes hacia la ciudad del destinatario. Allí la recogerán y llevarán al domicilio indicado en el sobre. Si la dirección no existe, la carta será devuelta a su origen por los mismos cauces que hicieron llegara ésta a su supuesto destino.

La carta escrita es la información a transmitir; el sobre y sello constituyen el formato del paquete impuesto por el protocolo de transporte que se utiliza en el proceso; el lugar del destinatario es la dirección del nodo destino y el domicilio del remitente, la ruta del nodo origen; los medios de transporte que llevan la carta cerca del destino constituyen los sistemas de transmisión que pueden ser cable coaxial, fibra óptica, enlaces de microondas o enlaces satelitales; la norma del servicio de correos, los carteros y demás personal representan al conjunto de los protocolos de comunicaciones establecidos.

Si se supone que se utiliza el modelo OSI de la ISO, que tiene siete niveles, se interpreta como que la carta pasa a través de siete filtros (trabajadores con diferentes cargos) desde que es introducida al buzón hasta que llega a su destino. Cada nivel de esta torre realiza funciones diferentes e importantes para transmitir información. Cada nivel por el que pasa la carta añade información de control que le permitirá llegar a su destino, en donde le será retirada. Cada nivel realiza funciones distintas que van desde el control de errores hasta la reorganización de la información transmitida cuando esta se ha fragmentado en tramas.

Si el mensaje va dirigido a una red diferente (otra ciudad en el caso de la carta), la trama debe llegar a un dispositivo de interconexión de redes (router, gateway, bridges), el cual decidirá, dependiendo de su capacidad, el camino que debe seguir la trama para arribar a su destino.

Es imprescindible, entonces, que el paquete lleve la dirección destino y que ésta contenga, además del domicilio que identifica al nodo, el derrotero que reconoce la red a la que pertenece el nodo.

1.2. ¿Por qué son tan necesarias las redes en el mundo actual?

Hace algunos años era impredecible la evolución que las comunicaciones, en el mundo de la informática, iban a tener; no podía preverse que fuese tan necesaria la interconexión ya no sólo de varios ordenadores sino de cientos de ellos. Hoy no basta con tener los ordenadores en una sala conectados, es necesario integrarlos a su vez con los ordenadores del resto de las salas y de sucursales de una empresa situadas en distintos puntos geográficos.

La interconexión de redes permite, si se puede decir así, ampliar el tamaño de una intranet. Sin embargo, el término ínterconexión se utiliza para unir redes independientes, no para ampliar el tamaño de una.

El número de ordenadores que componen una íntranet es limitado, depende de la topología elegida. Recuérdese que en la topología se define el cable a utilizar. Si lo único que se quiere es sobrepasar el número de ordenadores conectados se puede pensar, simplemente, en segmentar la intranet. No obstante, existen otros factores a tener en cuenta.

Cuando se elige la topología que va a tener una intranet se tienen en cuenta algunos agentes como son la densidad de tráfico que ésta debe soportar de manera habitual, el tipo de aplicaciones a instalarse sobre ella, la forma de trabajo que debe gestionar, entre otros. Esto hace pensar en diferentes topologías por el uso que se le va a dar a la intranet. De aquí se puede deducir que, en una misma empresa, puede ser necesaria no solo la instalación de una única intranet, aunque sea segmentada, sino la implantación de redes independientes, con topologías distintas e incluso con arquitecturas diferentes e interconectadas.

Diferentes razones hacen necesario segmentar o interconectar de intranets. Ambos conceptos, a pesar de llevar a un punto en común, parten de necesidades distintas.

La tabla 1.1 refleja, de forma escueta, diferentes casos en los que se plantea la necesidad de segmentar y/o interconectar intranets, y da la opción más idónea para cada uno de los casos planteados.

Tabla 1.1. Cuando se requiere segmentar o interconectar intranets.

NECESIDAD	SOLUCION
La necesidad de manejo de aplicaciones que producen un traslado importante de información aumenta el tráfico en la red. Esto lleva a que baje el rendimiento de la misma.	Dividir la red actual en varios segmentos: segmentar la red.
Se tiene que ampliar el número de puestos que forman la intranet, pero se necesita mantener el rendimiento de la red.	Crear un nuevo segmento de red en el que se pondrán los nuevos puestos e incluso al que se pueden mover puestos, lo que por disposición física puede ser conveniente.
Se tiene la necesidad de unir dos intranets exactamente iguales en la empresa.	Se puede optar por definir una de ellas como un segmento de la otra y unirlas de esta forma; o bien, interconectarlas con un dispositivo de nivel bajo.
Se tiene la necesidad de unir dos o más redes con diferentes topologías, pero trabajando con los mismos protocolos de comunicaciones.	Es necesario la interconexión de ambas redes a través de dispositivos interconectantes de nivel medio.
Se tiene la necesidad de unir dos o más redes totalmente distintas, es decir, de arquitecturas diferentes.	Es necesario la ínterconexión de ambas redes a través de dispositivos interconectantes de nivel alto.

Los diagramas que siguen ilustran la cuestión.

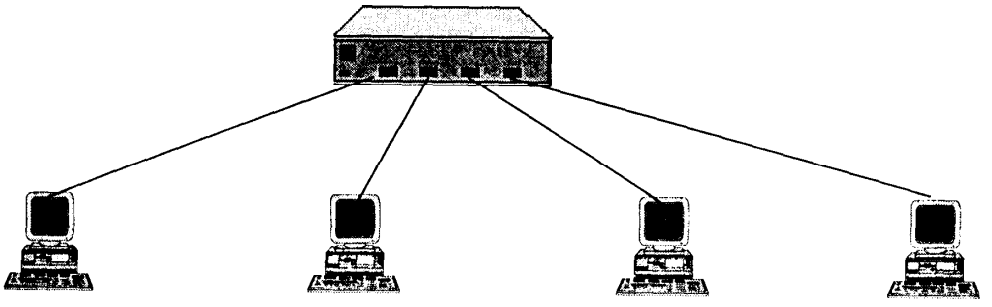


Figura 1.1. Red inicial con topología lógica en bus y física en estrella conectada a través de un Hub.

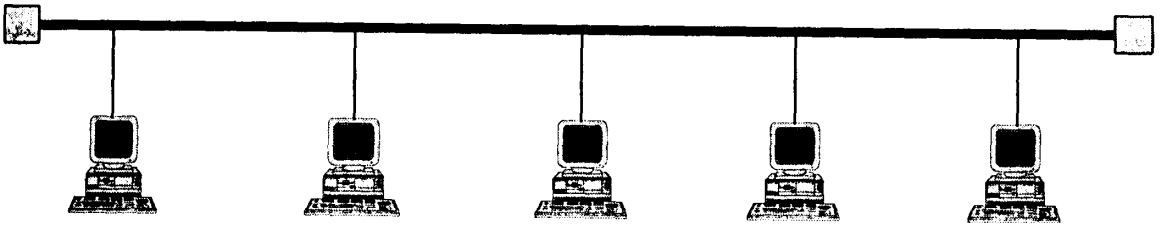


Figura 1.2. Solución que permite ampliar la red. Note que no mejora el rendimiento de la misma: se sigue presentando como una única red.

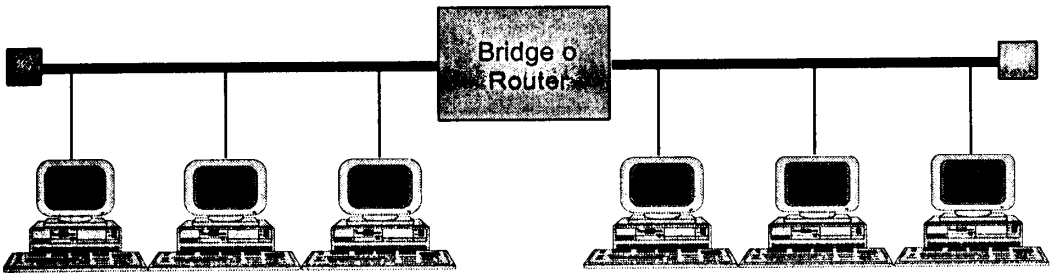


Figura 1.3. Solución que permite ampliar la red y mejorar su rendimiento.

1.3. Tipos de redes.

1.3.1. De acuerdo al espacio físico.

De acuerdo con el área geográfica que abarcan las redes, éstas se agrupan en tres grandes categorías que son:

- Redes de área amplia WANs (Wide Area Network), que cubren áreas geográficasn extensas. Normalmente, operan a velocidades relativamente lentas debido al espacio que abarcan.

- Redes de área metropolitana MAN (Metropolitan Area Network), que envuelven ciudades y, operan a velocidades comprendidas entre 56Kbps y 100 Mbps.

- Redes de área Local LANs (Local Area Network), que copan pequeñas áreas geográficas constituidas por edificios o campus. Su velocidad de operación oscila entre 4Mbps y 2Gbps.

Definitivamente, el tipo de red más común en corporaciones es la red LAN. Su conexión es sencilla debido a que cada computadora posee una interfase de red con que se conecta directamente.

La ventaja más importante de una red de área local LAN constituye la facilidad que proporciona para compartir recursos entre sus usuarios. Esto supone:

- Compartir ficheros, fundamental al disponerse de directorios en la red a los que tienen acceso un grupo de usuarios y en los que pueden guardar la información que comparten.
- Compartir impresoras.
- Utilizar aplicaciones específicas de red.
- Aprovechar las prestaciones cliente/servidor.
- Acceder a sistemas de comunicación global.

También debe tenerse en cuenta que una red de área local puede poseer distintas configuraciones que se verán más adelante, pero básicamente podemos hablar de dos tipos:

- Red con un servidor, en la cual existe un servidor central que es el "motor" de la red. El servidor puede ser activo o pasivo, dependiendo del uso que se le dé a la red.

- Red peer to peer o red de igual a igual, en la cual todos los puestos de la red pueden ejercer la función de servidor y de cliente.

En una intranet interesa tener un servidor web que será la parte más importante de la red.

1.3.2. De acuerdo al modo de transferencia de la información.

Dependiendo de su arquitectura y de los procedimientos empleados para transferir información, las redes de comunicación se clasifican en dos categorías que son:

- Redes conmutadas.

- Redes de difusión.

1.3.2.1. Redes conmutadas.

Las redes conmutadas consisten en un conjunto de nodos interconectados entre sí a través de medios de transmisión (cables por ejemplo), que forman así una topología mallada, que traslada información se transfiere del nodo de origen al nodo destino por conmutación entre los nodos intermedios.

De hecho, una transmisión de este tipo tiene 3 fases que son:

- Establecimiento de la conexión.
- Transferencia de la información.
- Liberación de la conexión.

Se entiende por conmutación en un nodo a la conexión física o lógica que establece un camino de entrada y salida del nodo para transferir información desde la entrada al nodo hacia su salida. Un ejemplo de redes conmutadas son las redes de área extensa.

A su vez, las redes conmutadas se subdividen en otros dos grupos:

- Redes de conmutación de paquetes.

- Redes de conmutación de circuitos.

Conmutación de paquetes es el procedimiento para enviar información de un nodo a otro dividida en paquetes. Cada paquete contiene información adicional y se envía por el canal de comunicación. Importante es resaltar que cada nodo intermedio, por el que pasa el paquete, lo procesa y determina hacia donde tiene que viajar para conseguir su objetivo. Otras características importantes de su funcionamiento son las que se detallan a continuación:

- En cada nodo intermedio se apunta una relación de la forma: “todo paquete con origen en el nodo A y destino en el nodo B tiene que salir por la salida 5 de mi nodo”.

- Los paquetes se numeran para poder saber sí se ha perdido alguno en el camino.

- Todos los paquetes de una misma transmisión viajan por el mismo camino.

- El camino establecido para una comunicación puede ser utilizado de forma simultánea.

Conmutación de circuitos es un procedimiento por el que dos nodos se conectan, lo que permite utilizar de forma exclusiva el circuito físico durante la transmisión. En cada nodo intermedio de la red se cierra un circuito físico entre un cable de entrada y una salida de la red. A manera de ejemplo tenemos la red telefónica.

1.3.2.2. Redes de difusión.

Estas redes se caracterizan por no establecer nodos intermedios de conmutación. Por el contrario, los nodos comparten el medio de transmisión motivo por el cual la información transferida por un nodo es conocida por los demás. Ejemplo de redes de difusión son:

- Comunicación por radio.
- Comunicación por satélite.
- Comunicación en una red local.

1.4. Topología.

La topología de una red la define únicamente la distribución del cable que interconecta los diferentes ordenadores; es el mapa de distribución del cable que forma la intranet. La topología define cómo se organiza el cable de las estaciones de trabajo, lo cual es muy importante a la hora de instalar una red porque ésta se escoge en relación con las necesidades existentes. Hay un conjunto de factores a tomar en consideración al seleccionar una topología de red concreta, entre ellos podemos mencionar los siguientes:

- La distribución de los equipos a interconectar.
- El tipo de aplicaciones a ejecutar.
- El monto de la inversión que se quiere hacer.
- El coste que es posible dedicar al mantenimiento y actualización de la red local.
- El tráfico que soportará la red local.
- La capacidad de expansión. Se debe diseñar una intranet teniendo en cuenta la escalabilidad.

No se debe confundir el término topología con el de arquitectura. La arquitectura de una red engloba:

- La topología.
- El método de acceso al cable.
- Protocolos de comunicaciones.

Actualmente la topología está directamente relacionada con el método de acceso al cable, puesto que éste se encuentra ligado casi directamente a la tarjeta de red y ésta depende de la topología elegida.

1.4.1. Topología física.

Es la forma en que el cableado se estructura a una red. Existen tres clases de topologías físicas puras que son:

- Topología en anillo.
- Topología en bus.
- Topología en estrella.

Se pueden mezclar las topologías físicas para crear redes compuestas por más de un tipo de estas topologías.

1.4.1.1. Topología en bus.

Consta de un único cable que se extiende desde un ordenador al siguiente, al modo de una serie. Los extremos del cable se terminan con una resistencia denominada **terminador** que, además de indicar que no existen más ordenadores en el extremo, cierran el bus.

Sus principales ventajas son las siguientes:

- Fácil de instalar y mantener.
- No existen elementos centrales, de los cuales dependa toda la red, y cuyo fallo afectara el funcionamiento del resto de las estaciones.

Entre sus principales inconvenientes podemos encontrar el siguiente:

- Por la forma de su estructura, si se rompe el cable en algún punto, la red queda inoperativa por completo.

Cuando se decide instalar una red de este tipo, en un edificio con varias plantas, se instala una red por planta y se las une a través de un bus troncal.

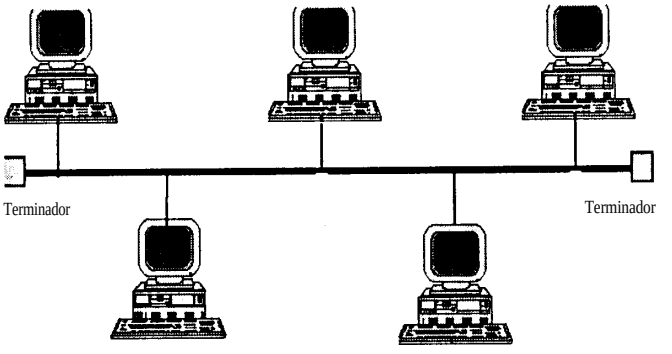


Figura 1.4. Topología en forma de bus.

1.4.1.2. Topología en anillo.

Sus principales características son:

- El cable forma un bucle cerrado a manera de un anillo.
- Todos los ordenadores, que forman parte de la red, se conectan a ese anillo.
- Habitualmente las redes en anillo utilizan para accesar al medio el modelo “esperar el turno”.

Los principales inconvenientes de este modelo son:

- Si se rompe el cable que forma el anillo se inhabilita la red.
- Difícil de instalar.

- Requiere mantenimiento.

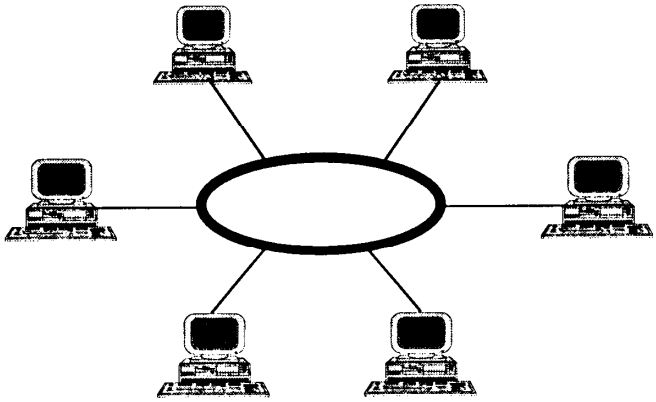


Figura 1.5. Topología en anillo.

1.4.1.3. Topología en estrella.

Sus principales características son:

- Todas las estaciones de trabajo están conectadas a un punto central (concentrador), formando una estrella física.

- Habitualmente sobre este tipo de topología se utiliza, como método de acceso al medio, el polling y es el nodo central el que se encarga de implementarlo.

- Cada vez que se quiere establecer comunicación entre dos ordenadores, la información transferida, de uno hacia el otro, debe pasar por el punto central.

- Existen algunas redes con esta topología que emplean, como punto central, una estación de trabajo que gobierna la red.

- La velocidad suele ser alta para comunicaciones entre el nodo central y los nodos extremos y es baja cuando se establece entre nodos extremos.

- Este tipo de topología se usa al intercambiar información preferentemente entre el nodo central y el resto de los nodos y no entre nodos extremos.

- Al romperse un cable se pierde la conexión del nodo que interconectaba.

- Resulta sencillo detectar y localizar un problema en la red.

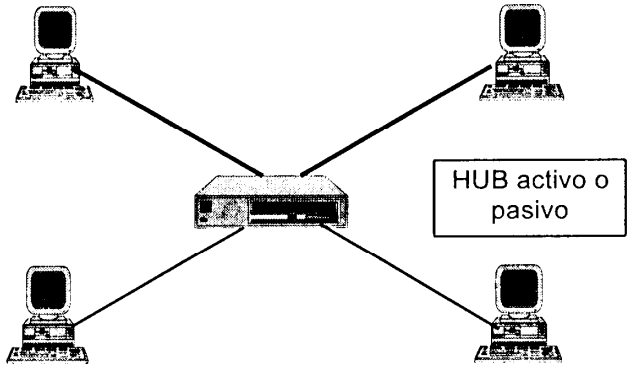


Figura 1.6. Topología en estrella.

1.4.1.3.1. Topología en estrella pasiva.

Es una estrella en la que su punto central, al que se conectan todos los nodos, está constituido por un concentrador pasivo (hub), un dispositivo con muchos puertos de entrada.

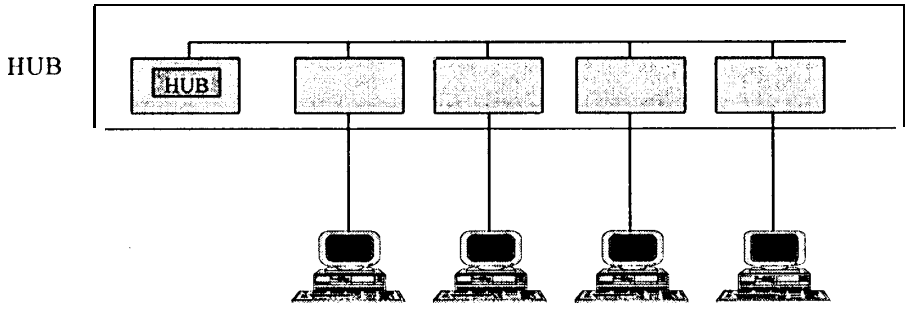


Figura 1.7. Topología en estrella pasiva.

1.4.1.3.2. Topología en estrella activa.

Utiliza como punto central un hub activo o un ordenador que hace las veces de servidor de red. El hub activo se encarga de repetir y regenerar la señal transferida e, incluso, puede él realizar estadísticas del rendimiento de la red. El ordenador empleado como nodo central, se encarga de gestionar la red y de ser el servidor de ficheros.

1.4.2. Topología lógica.

Se refiere a la manera de conseguir el funcionamiento de una topología física cableando la red de una forma más eficiente. Existen topologías lógicas definidas que son:

- Topología anillo-estrella, la cual implementa un anillo mediante una estrella física.

- Topología bus-estrella que implementa una topología en bus mediante una estrella física.

1.4.2.1. Topología anillo estrella.

Uno de los inconvenientes de la topología en anillo es que la ruptura del cable hace inoperable la red; con la topología mixta anillo estrella, éste y otros problemas quedan resueltos. Aquí un resumen de las principales características de este tipo de topología:

- Cuando se instala una configuración en anillo, éste se establece de forma lógica únicamente, ya que la forma física utiliza una configuración en estrella.

- Se recurre a un concentrador, o incluso un servidor de red, como dispositivo central, de esta forma, si se rompe algún cable sólo queda inoperativo el nodo que conectaba, y los demás seguirán funcionando.

- El concentrador que utiliza esta topología se denomina MAU (Unidad de Acceso Multiestacíón). Consiste en un dispositivo que proporciona el punto de conexión para múltiples nodos. Contiene un anillo interno que se extiende a un anillo externo.

- A simple vista la red parece una estrella aunque internamente funciona como un anillo.

- Cuando el MAU detecta que un nodo se ha desconectado (por ruptura del cable, por ejemplo), puentea su entrada y salida para cerrar el anillo.

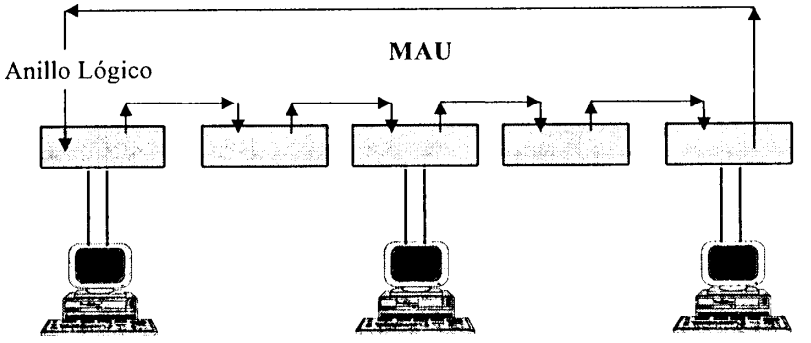


Figura 1.8. Topología anillo estrella.

1.4.2.2. Topología bus estrella.

Es en realidad una estrella que funciona como si fuese en bus. Tiene un concentrador pasivo (hub) que implementa internamente el bus y al que están conectados todos los ordenadores. La única diferencia que existe entre esta topología mixta y la topología en estrella con hub pasivo es el método de acceso al medio utilizado.

1.5. Características sobresalientes de una red.

1.51. Elementos de una red.

Entre los principales componentes requeridos para instalar una red tenemos:

- Tarjetas de interfaz de red.
- Cable.
- Protocolos de comunicaciones.
- Sistema operativo de red.
- Aplicaciones capaces de funcionar en red.

Las tarjetas de interfaz de red NICs (Network Interface Cards) son adaptadores instalados en un dispositivo que permite interconectar dos computadoras en una red. Son el pilar que sustenta toda red local, y el único elemento imprescindible que enlaza dos ordenadores a buena velocidad (excepción hecha del cable y el software). Existen tarjetas para distintos tipos de redes y sus principales características son:

- Operan en el nivel físico del modelo OSI. Las normas que rigen a estas tarjetas determinan sus características y su circuítería gestiona muchas de las funciones de la comunicación en red como son las especificaciones mecánicas, que incluyen los tipos de conector para el cable por ejemplo; las especificaciones eléctricas que definen los métodos de transmisión de la información y las señales de control para dicha transferencia; el método de acceso al medio, el cual es el tipo de algoritmo que se utiliza para acceder al canal de comunicación que sostiene la red. Estos métodos están definidos por las normas 802.x de la IEEE.

- La círcuitería de la tarjeta de red determina, antes del inicio de la transmisión de datos, elementos como la velocidad de comunicación, el tamaño del paquete, time-out, o el tamaño de los buffers. Resulta importante mencionar que para hacer posible la transmisión, todos estos elementos tienen que haberse establecido, dándose a continuación la conversión de los datos a transmitir a dos niveles.

- En primer lugar se genera el flujo de bits mutando, los datos paralelos en datos en serie. Seguidamente se codifican y hasta se comprimen para un mejor rendimiento en la transmisión.

- En segundo lugar, la dirección física es un concepto asociado a la tarjeta de red. Esto se debe a que cada nodo de una red tiene una dirección asignada que depende de los protocolos de comunicaciones que esté utilizando. La dirección física, habitualmente, al venir definida desde la fábrica es inmodificable. Sobre esta dirección física se definen otros derroteros tales como la dirección IP para redes que estén funcionando con TCP/IP.

1.5.2. Determinación de la velocidad de transmisión de una red.

Varios factores especifican la velocidad de transmisión de una red, entre ellos podemos destacar:

- El cable utilizado para la conexión. Dentro de esta característica existen elementos como el ancho de banda permitido y su longitud.

Otros agentes que delimitan el rendimiento de la red son:

- Las tarjetas de red.
- El tamaño del bus de datos de las máquinas.
- La cantidad de retransmisiones que se pueden hacer.

1.6. Aplicaciones de las redes.

Un gran número de aplicaciones aprovechan las redes locales para que el trabajo sea más provechoso. El tipo de aplicación más importante son los programas de correo electrónico que permiten el intercambio de mensajes entre los usuarios. Los mensajes pueden consistir, principalmente, en texto, sonido e imágenes y llevar asociados cualquier tipo de ficheros binarios. El correo electrónico llega a sustituir ciertas reuniones y permite el análisis más detallado del material que los usuarios remiten.

1.6.1. Aplicaciones cliente/servidor.

Es un concepto muy importante en las redes locales para aplicaciones que manejan grandes volúmenes de información. Son programas que dividen su trabajo en dos partes, una parte cliente que se realiza en el ordenador del usuario y otra parte servidor que se ejecuta en un servidor con dos fines:

- Aliviar la carga de trabajo del ordenador cliente.
- Reducir el tráfico de la red.

Si, por ejemplo, disponemos de un ordenador que actúa como servidor de base de datos, con un enfoque tradicional, el servidor solamente lo es de ficheros. Si en algún momento el usuario quiere hacer una selección de personas mayores de 30 años, por ejemplo, se deben leer todos los registros de la base de datos para comprobar cuáles cumplen la condición. Esto supone un elevado tráfico en la red.

Con las aplicaciones cliente/servidor una consulta sobre una base de datos se envía al servidor quien realiza la selección de registros y envía solo los campos que le interesan al usuario. Se reduce así, considerablemente, el tráfico en la red y el ordenador cliente se encuentra con el trabajo hecho. El sistema en sí resulta bastante más rápido aunque, a cambio, requiere servidores con mejores prestaciones.

1.6.2. Acceso a Internet.

Es una de las prestaciones que, con el tiempo, está ganando peso. Consiste en la posibilidad de configurar un ordenador con una conexión permanente a servicios en línea externos, de forma que los usuarios de una intranet no necesiten utilizar un módem personal para acceder a ellos.

Mediante un servidor de comunicaciones se puede mantener una línea permanente de alta velocidad que enlace la intranet con Internet. El servidor puede estar equipado con un módem o una tarjeta de comunicación a RDSI, que activa la conexión cuando algún usuario de la red lo necesita. Cuando la conexión está activa, cualquier otro usuario puede compartirla, aunque en este caso las prestaciones para cada usuario serán menores que si tuvieran una conexión individual.

1.7. La red más grande del mundo: el Internet.

El Internet es un conglomerado de ordenadores de diferente tipo, marca y sistema operativo, distribuidos por todo el mundo y unidos a través de enlaces de comunicaciones muy diversos. La gran variedad de ordenadores y sistemas de comunicaciones plantea numerosos problemas de entendimiento, que se resuelven con el empleo de sofisticados protocolos de comunicaciones.

En primer lugar debemos estudiar su interconexión física. Dos ordenadores de Internet se pueden conectar de maneras muy diversas, ya sea por:

- Enlaces nacionales, con líneas de uso exclusivo o compartidas (de una compañía telefónica).

- Enlaces internacionales, proporcionados por compañías de comunicaciones con implantación internacional. Pueden utilizar cableado convencional, fibra óptica, satélites, enlaces por microondas.

- Mediante módems, la opción más empleada, sobre todo por usuarios particulares. Estos se conectan a través de una llamada telefónica común a un proveedor de comunicaciones que da, a su vez, acceso a Internet.

El uso de líneas RDSI (Red Digital de Servicios Integrados) es cada vez más frecuente como solución para interconexión de usuarios particulares a las redes de información de alta velocidad.

En lo que respecta al hardware: ordenadores con distintos sistemas operativos conectados a redes diferentes enlazadas a Internet, deben correr un programa de gestión de comunicaciones que permita el entendimiento entre las máquinas, mediante el protocolo adecuado.

1.7.1. Servicios.

Internet ofrece una serie de servicios para cubrir los requerimientos de sus usuarios los que han evolucionado para adaptarse a las nuevas necesidades. Las posibilidades básicas que tenemos en Internet son:

- World Wide Web.
- Correo electrónico.
- FTP.
- Grupos de discusión. News.
- Acceso remoto. Telnet.
- IRC.
- Chat.

1.7.1. Servicios.

Internet ofrece una serie de servicios para cubrir los requerimientos de sus usuarios los que han evolucionado para adaptarse a las nuevas necesidades. Las posibilidades básicas que tenemos en Internet son:

- World Wide Web.
- Correo electrónico.
- **FTP.**
- Grupos de discusión. News.
- **Acceso** remoto. Telnet.
- IRC.
- **C**hat.

Capítulo 2.

2. Redes Privadas Virtuales.

2.1. Introducción.

El Internet ha cambiado la manera de realizar negocios. Hoy es vital la presencia en Internet para actualizarse y captar la atención de nuevos clientes potenciales. Las Redes Privadas Virtuales al transformar la metodología de hacer negocios lo hacen más rápidamente que cualquier otra tecnología.

Un servicio de Redes Privadas Virtuales, al igual que una red privada, se basa en una infraestructura (backbone), que en este caso es el Internet, para establecer conexiones seguras con usuarios remotos y mantener comunicadas las regiones y oficinas, con reducción significativa de costos de las comunicaciones debido al incremento del trabajo móvil.

Los efectos que una VPN logre tener sobre una organización son dramáticos. Las ventas pueden incrementarse al igual que el desarrollo de productos. Muchas estrategias de negocios son fortalecidas en una forma nunca antes

posible. Antes de la aparición de las soluciones basadas en VPN, la opción para crear este tipo de comunicaciones fueron costosas líneas dedicadas o circuitos Frame-Relay. Al utilizar VPN´s el acceso a Internet es, por lo general, local y mucho menos caro que las conexiones dedicadas a Servidores de Acceso Remoto (Remote Access Ser-ver).

2.2. Generalidades de Redes Privadas Virtuales.

2.2.1. Antecedentes.

El enfoque de los negocios en la actualidad tienen como objetivo dar soporte a una gran variedad de comunicaciones con el fin de llegar a lugares distantes y siempre con miras a reducir costos de su infraestructura de comunicaciones. Los empleados necesitan disponer de acceso a los recursos de sus redes corporativas de una forma remota. Existen muchas sociedades de negocios trabajando juntas en extranets para compartir información de negocios, sea para un proyecto de pocos meses de duración o bien, como ventaja estratégica a largo plazo.

De la misma manera, los negocios demuestran que las soluciones anteriores de redes de área amplia, entre la red corporativa principal y las oficinas sucursales, no proveen la flexibilidad requerida para crear nuevos enlaces a socios o dar soporte a equipos de proyectos en sus campos de acción. Como el número de

telecommutadores crece cada vez más y el área de ventas necesita ser cada vez más móvil, se produce una mayor demanda de recursos de la red corporativa, por lo que es necesario invertir más dinero en los bancos de modems, los servidores de acceso remoto y los costos de las tarifas de telefónicas.

Según estimaciones de Forrest Research', más del 80% de la fuerza de trabajo corporativa tenía, al menos una computadora portátil en 1999. Los estudios indican que la tendencia hacia la conectividad móvil no muestra ninguna señal de disminuir.

Las VPN's permiten a los administradores de redes conectar de forma remota oficinas, sucursales y equipos de proyectos ubicados a distancia a la red corporativa principal, de manera económica, proveen acceso remoto a empleados mientras reducen los requerimientos internos tanto para equipos y soporte. Con los accesos remotos seguros, que ofrecen las VPN's, las conexiones vía modem telefónico pueden transmitir datos de forma garantizada, vía un proveedor de Servicios de Internet hacia una red Corporativa. Los datos se encriptan en el cliente antes de ser transmitidos y se desencriptan en la

[1] Forrest Research es una firma de investigación independiente que analiza el futuro de los cambios en la tecnología y su impacto en los negocios, en el sector consumidor y en la sociedad.

puerta del firewall. El software proporcionado, habilita a los usuarios remotos a conectarse a la red Corporativa como si ellos estuvieran detrás del firewall. La tecnología VPN proporciona un medio para utilizar el canal público de Internet como vehículo apropiado para comunicar datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privado a través del Internet. De esta manera se consigue reducir las responsabilidades de administración de una red local.

En lugar de depender de líneas dedicadas o circuitos virtuales permanentes (PVCs) como al utilizar la tecnología Frame Relay, una VPN basada en Internet utiliza la infraestructura distribuida y abierta del Internet para transmitir datos entre dos ubicaciones de la corporación. Las compañías utilizan una VPN basada en Internet para establecer enlaces a los puntos locales de conexión (POPs, Points of Presence) de su proveedor de Servicios de Internet (ISP). Este asegura que los datos son transmitidos a su destino, vía el Internet, y se encarga soportado en la infraestructura del Internet de los demás detalles de conectividad.

Debido a que el Internet es una red pública con transmisión abierta de información, las VPN´s basadas en Internet incluyen medidas para el paso de datos encriptados entre diferentes sitios (VPN sites), lo cual protege su envío y evita el acceso a ellos por partes no autorizadas. Las VPN´s no están limitadas

a ubicaciones corporativas y oficinas-sucursales. Una ventaja adicional consiste en que una VPN puede proveer conectividad segura para trabajadores móviles. Estos trabajadores contactan a su compañía de VPN marcando hacia el POP de un ISP local. Esto disminuye la necesidad de llamadas de larga distancia y los recargos por instalación y mantenimiento de grandes bancos de modems en las Instalaciones Corporativas.

2.2.2. Definición de Red Privada Virtual.

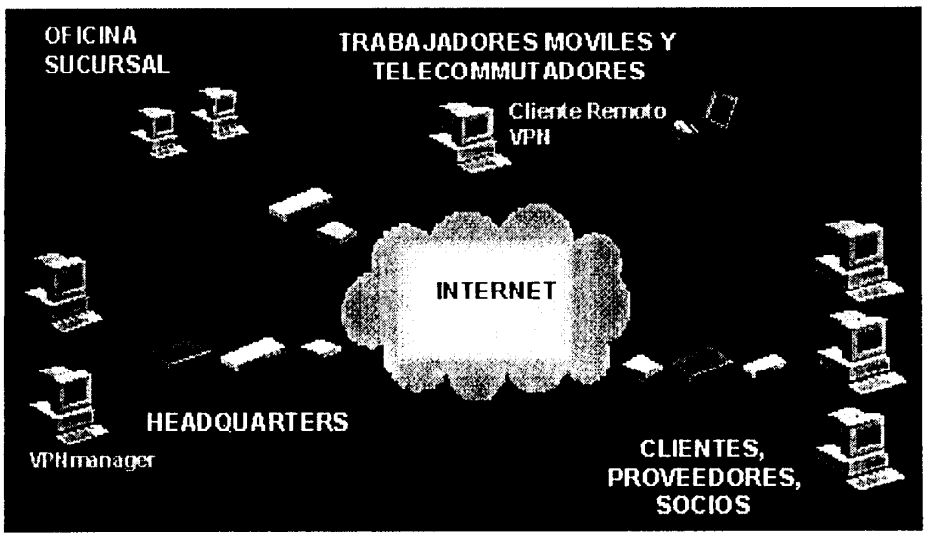


Figura 2.1. Solución VPN completa, considerando Extranets, Intranets y Acceso de usuarios remotos.

Es una red que extiende el acceso a usuarios remotos sobre una infraestructura compartida. Todos los usuarios parecen estar en el mismo segmento de LAN, pero en realidad están a varias redes (generalmente públicas) de distancia. En VPN´s, la palabra virtual implica que la red es dinámica, con conexiones establecidas de acuerdo a las necesidades particulares de las empresas. Esto significa que la red está formada lógicamente, sin considerar la estructura física de la red.

Las redes privadas virtuales que utilizan Internet crean un túnel o conducto dedicado de un sitio a otro, donde las firewalls ubicadas en ambos lugares permiten una conexión fiable a través del Internet; mantienen las mismas seguridades, prioridades, confiabilidad y conservan igual tipo de administración que las ofrecidas por una red privada.

Es un método bastante conveniente, en cuanto a costos, puesto que permite establecer enlaces punto a punto entre usuarios remotos y la red Interna de la empresa. Las VPN basadas sobre IP, reúnen requerimientos de diferentes usuarios para extender la intranet propia de la empresa y dar acceso a oficinas remotas, usuarios móviles y telecommutadores.

2.3. Características.

La meta de una Red Privada Virtual es usar una red de datos pública para mantener una comunicación segura a niveles de rendimiento comparables a las facilidades que ofrecen la mayoría de enlaces WAN dedicados. Por este motivo una solución VPN debe procesar, de forma intensiva, la seguridad de los datos entregados y maximizar el ancho de banda que la red comparte.

Existe variedad de métodos para desarrollar VPN's bajo las circunstancias actuales. El mercado de VPN es popularizado por el uso de productos puntuales y soluciones incompletas enfocadas en un tipo de aplicación de VPN's. La mayoría de proveedores de VPN's ofrecen productos que solamente otorgan autenticación y encriptación, por lo cual los clientes piensan que esos componentes aislados comprometen la totalidad de una VPN. Sin embargo, la encriptación y la autenticación -por si solas- son inadecuadas para implementar los diferentes tipos de VPN's que cumplen con funciones específicas, demandadas hoy por las empresas.

No todos los productos VPN, generalmente, proveen un control de acceso adecuado. La mayoría de proveedores de VPN aún venden sus productos como un sistema de redes que los clientes deben administrar de forma separada y, de alguna manera, integrar a las políticas de seguridad empresarial.

La mayoría prefiere que aspectos tales como calidad de servicio o confiabilidad sean factores administrados por los proveedores de servicios y no le proporcionen al usuario las herramientas que necesita para poner la predicción del rendimiento en sus propias manos. Esta situación da pie a posibles amenazas a la seguridad, porque las VPN's no están integradas a las políticas de seguridad de una organización.

2.4. Arquitectura de Redes Privadas Virtuales.

Para el desarrollo de VPN's sobre Internet hay dos conceptos importantes a tomar en cuenta: seguridad y rendimiento. El Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP) y el Internet no fueron diseñados desde un principio con estas consideraciones porque el número de usuarios y las aplicaciones iniciales no requerían fuertes medidas de seguridad o un rendimiento garantizado.

Pero si las redes privadas virtuales, basadas en el Internet, van a servir como sustitutos para el alquiler de líneas dedicadas u otros tipos de enlace de redes de área amplia (WAN), deben adicionarse al Internet tecnologías que garanticen seguridad y rendimiento de la red debido a que las VPN's van a extender la red corporativa hacia oficinas distantes, a home workers (personal que trabaja desde sus casas), personal de ventas y socios de negocios.

Afortunadamente, los estándares para seguridad de datos sobre redes IP han evolucionado de tal forma que éstos pueden utilizarse para crear VPN's, aunque los trabajos para proveer rendimiento garantizado están en una etapa inicial de desarrollo. Hay proveedores de Internet que no han desarrollado aún estas tecnologías a un grado importante hasta la fecha.

Para lograr la funcionalidad de redes *seguras, privadas y virtuales, se* deben cumplir tres funciones principales:

- Pasar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos remotos de LAN no parezcan separados por dicha red.

- Agregar encriptación para que el tráfico que cruce por la red pública no sea espiado, interceptado, leído o modificado.

- Autentificar positivamente cualquier extremo del enlace de comunicación para impedir que una persona ajena a la compañía acceda a los recursos del sistema.

Existen importantes estrategias y razones económicas para migrar desde redes privadas a redes privadas virtuales. Son cuatro los desafíos para las compañías que implementan VPN's:

- Seguridad de los datos.

- Rendimiento de la red.

- Posibilidad de expansiones futuras.

- La administración empresarial.

2.4.1. Seguridad de los datos.

El Internet no fue diseñado para transmitir en forma segura datos corporativos de vital importancia, por lo que existen problemas relacionados a la seguridad en la red que se encuentran bien documentados. Para ser conveniente una red debe asegurar privacidad, integridad y autenticación de los datos que son transmitidos.

La base conceptual es la siguiente:

Tabla 2.1. Privacidad, Integridad y. Autenticación

Privacidad:	La información es codificada de manera tal, que si es interceptada, esta no puede ser descifrada, a excepción del receptor destino.
Integridad:	Los datos son transmitidos a prueba de interferencias. Si los datos son modificados, o si introducen datos extraños, este tipo de alteraciones son fácilmente detectadas y descartadas
Autenticación:	La identidad del emisor puede y debe ser verificada.

2.4.1.1. Ataques comunes a la seguridad.

Al transmitirse datos la mayoría de las amenazas serias a la seguridad ocurren dentro de la WAN. Los hackers pueden interceptar fácilmente y borrar o alterar datos importantes con pequeñas posibilidades de detección.

Algunos de los ataques más serios incluyen:

- Intromisión *captura de los* datos: Los paquetes son interceptados y/o leídos mientras transitan a través de la WAN. A veces los ataques impiden a los datos llegar a su destino, aunque lo usual es que si lleguen de manera que el emisor y receptor no perciban que una tercera persona ha tenido acceso a la información.

- Datos interferidos: Los paquetes son interceptados y su contenido modificado antes de seguir a su destino. En un proceso llamado *packet spoofing*, un hacker se enmascara como usuario legítimo o como site para insertar paquetes en la red. Estos ataques son, a menudo, los más agudos y destructivos.

- *Servicio denegado:* los atacantes impiden que una red funcione apropiadamente enviar exceso de tráfico hacia la red, lo que produce congestión y la posibilidad de colapsarla.

Estas amenazas tipifican las dificultades que deben prevenirse porque en buena medida las soluciones de seguridad están orientadas a la protección de la LAN y no de la WAN.

Mientras la mayor parte de los proveedores de soluciones VPN ofrecen autenticación y encriptación, estas dos tecnologías sólo otorgan privacidad para comunicaciones de datos. Los componentes de seguridad de una Red Privada Virtual deben incluir la totalidad de las tres tecnologías siguientes para garantizar la seguridad de las redes, la autenticidad de los nodos VPN y la privacidad e integridad de los datos.

2.4.2. Control de Acceso.

Especifica las libertades que un usuario tiene dentro de una VPN y regula el acceso de socios, empleados y otros usuarios externos hacia aplicaciones y diferentes porciones de la red. Una VPN sin control de acceso definido y completo protege la seguridad de los datos en tránsito pero no la red en sí.

Un control riguroso protege a la red entera de la corporación, incluida la información altamente confidencial, como la de propiedad intelectual de la

empresa y asegura que los usuarios de una VPN tengan acceso total a las aplicaciones y a la información que necesitan, pero a nada más.

Por los riesgos a los que está expuesta la red es necesario considerar la totalidad de los factores citados anteriormente para garantizar un completo control de acceso.

24.3. Autenticación.

Es el proceso que verifica si el emisor es realmente quién dice ser. Un esquema robusto y adecuado de autenticación es particularmente crítico para implementaciones VPN. Asegura que la privacidad de las comunicaciones tanto de gateway-to-gateway y cliente-to-gateway, así como la identidad de los dos sites corporativos y de sus usuarios individuales, sean debidamente verificadas. Una variedad de métodos de autenticación están disponibles según las necesidades de una VPN, incluyen la tradicional autenticación username/password, RADIUS o TACACS/TACACS + Servers, LDAP-compliant directory servers, certificados digitales X.509 y esquemas two-factor, incluso aquellos que involucran hardware tokens y smart cards.

Adicionalmente a la fortaleza del desarrollo de un esquema de autenticacíón, otros factores críticos a considerar son aplicaciones tipo broad, soporte y

escalabilidad. La legitimidad de los usuarios de cualquier servicio basado en IP debe ser verificada para establecer una sesión VPN segura. La escalabilidad es de interés particular para una VPN con acceso remoto cuando se espera que crezca el número de clientes móviles.

El esquema de autenticación implementado para una VPN en particular debe ser administrable y fácil de desarrollar para gran números de usuarios individuales.

2.4.4. Encriptación.

Mezcla datos para asegurar que quien tiene la clave es capaz de leer la información al decodificar el mensaje. Los algoritmos de encriptación garantizan que sea matemáticamente imposible decodificar los datos sin poseer la clave de encriptación apropiada. En líneas generales la seguridad de las comunicaciones encriptadas crece a medida que las llaves o claves son más grandes. Al seleccionar e implementar la longitud de la clave de encriptación se asegura su protección a través de un *Sistema de Administración de Claves, y* que consiste en un proceso de distribución de claves, actualizándolas a intervalos de tiempo específicos y caducándolas en cuanto sea necesario.

Infraestructuras de claves públicas (Public Key Infraestructure, PKI) son esenciales en las VPN´s que utilizan certificados digitales para autenticación y

encriptación cuando crecen en complejidad y tamaño ya que el número de claves a ser administradas cambia de forma exponencial.

2.4.4.1. Introducción a la encriptación.

El concepto clave relacionado a criptografía se basa en la emisión de un mensaje a receptor específico con la seguridad de que nadie mas pueda leerlo, alterarlo o duplicarlo, y garantiza así que lo reciba el receptor en mención y no cualquier otra persona. El mensaje inicial es conocido como plaintext, cleartext o texto original debido a que es legible para cualquier persona. Codificar el mensaje para que no sea legible se llama encríptacíón y se lo conoce como el ciphertext o texto codificado. El proceso de encriptacíón consta de un algoritmo y de una clave específica utilizada en esa ocasión y al modificarse la clave cambia la salida del algoritmo. En el lado de la recepción el texto codificado es devuelto al texto original al usar un algoritmo de desencríptacíón y clave.

La seguridad de la encriptacíón convencional depende de algunos factores:
El algoritmo de encriptación debe ser lo suficientemente robusto para que no sea práctico desencriptar un mensaje solo utilizando el texto codificado. La seguridad de la encríptación convencional depende de la clave utilizada y no de la confídencíalidad del algoritmo en sí, *no es obligatorio mantener el algoritmo en secreto pero sí la clave.*

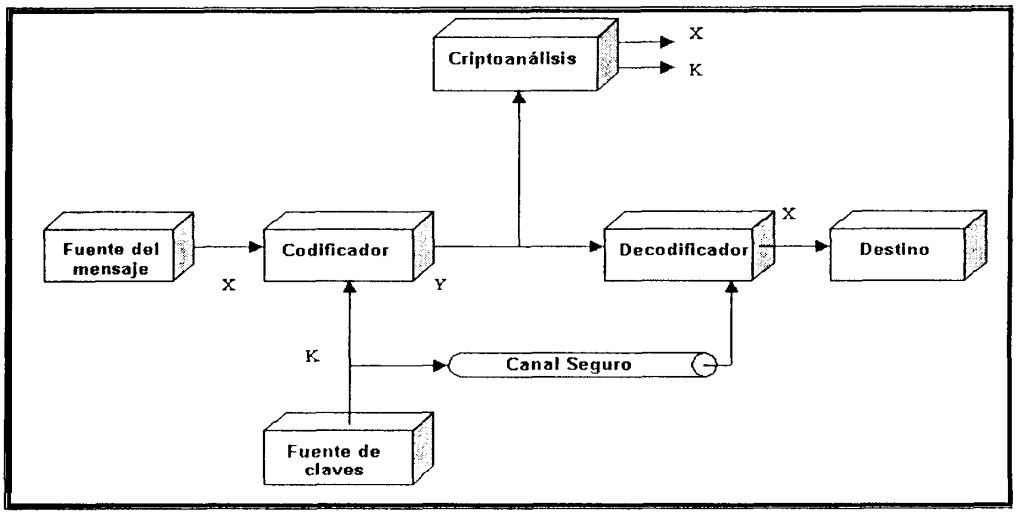


Figura 2.2. Modelo de un sistema convencional de encriptación.

Esta presentación de la encriptación convencional hace posible su amplio uso. El hecho de que los algoritmos no requieran reserva permite a los fabricantes desarrollar aplicaciones con un mismo algoritmo de encriptación, elaborando integrados a menor costo, hoy ampliamente disponibles e incorporados a una gran gama de productos.

Los algoritmos empleados en encriptar y desencriptar mensajes son llamados algoritmos criptográficos 0 *cipher algorithm* que utilizan funciones matemáticas con ese fin. Un algoritmo restringido o protegido es inadecuado porque una vez

revelado cualquiera puede cambiarlo y por eso los sistemas actuales de encriptación usan claves para controlar la encriptación y desencriptación. La clave es una información secreta requerida para codificar y decodificar el mensaje. Emisor y receptor deben de sincronizar sus claves para leer los mensajes enviados entre ellos.

2.4.4.2. Importancia de la encriptación.

La encriptación se expande en la era electrónica actual. Las personas son vulnerables, las compañías están expuestas, y las redes son susceptibles de varias maneras. Los *hackers* consideran juego o desafío el irrumpir en los recursos computacionales privados de una empresa para obtener información vital y probar que tienen recursos que destruyen códigos y ocasionan daños serios a una organización.

La mayoría de los esquemas de encriptación pueden ser rotos con suficiente tiempo y recursos y por eso la clave consiste en lograr que los costos de romper la seguridad del sistema exceda a los beneficios por obtener la información"

La encriptación de datos es utilizada para lograr lo siguiente:

1. Seguridad & Privacidad.- Significa proveer confidencialidad a la información susceptible impidiendo que el receptor sea sustituido.

2. Integridad.- Garantiza al receptor del mensaje para que verifique que éste, en su tránsito, no fue modificado por un intruso.

3. Autenticación.- El receptor del mensaje puede verificar su origen. Un intruso no debe ser capaz de enmascararse emisor autorizado.

4. No – Rechazo.- Impide que un emisor falsifique o rechace un mensaje enviado.

2.4.4.3. Sistemas basados en claves.

Existen dos tipos de sistemas basados en claves y son:

2.4.4.3.1. Simétrica o Clave Secreta.

La misma clave es utilizada tanto para encriptación como para desencriptación. Evitar que personas ajenas a la empresa lean y tengan acceso a los datos transmitidos exige que el transmisor y el receptor compartan la clave secreta que utilizan para comunicarse. Las desventajas son las siguientes:

- Se necesita una clave distinta por cada par de entidades que se comunican.
- Actualizar claves es complicado.

2.4.4.3.2. Asimétrica o Clave Pública.

Utiliza una clave de encriptación y otra de desencriptación. El usuario tiene dos claves, una pública y otra privada. Las claves públicas son ampliamente distribuidas y las privadas secretas.

Existen varios métodos que realizan cifrados asimétricos o de clave pública y utilizan claves diferentes para encriptar y desencriptar datos.

Supongamos una caja con dos llaves diferentes, la una abre y la otra cierra, entonces:

- Si cierro la caja con la llave i debo abrirla con la llave j.
- Si abro la caja con la llave j debo cerrarla con la llave i.

Una clave es pública cuando encripta los datos enviados a un usuario específico que dispone de la clave secreta para desencriptar el mensaje.

Este tipo de administración de claves es más sencillo que la gestión de claves simétricas, pero aún así necesita una autoridad de registro que asegure la pertenencia de la clave pública al usuario con quien deseamos comunicarnos. Existen pro y contras en ambos sistemas.

El sistema de claves secretas es más rápido que el de claves públicas porque éste requiere que las claves sean transmitidas hacia cada extremo. La longitud de la clave es tan importante como su tamaño ya que determina el número de valores posibles que la clave puede tomar, sin embargo, el algoritmo utilizado también es un factor crítico a considerar.

Claves de poca longitud, utilizadas con un tipo de algoritmo, pueden funcionar mejor que claves más grandes que emplean otro tipo algoritmo. Las claves simétricas pueden ser más pequeñas que claves asimétricas y proveer una protección similar.

La codificación de **clave combinada** funciona de la siguiente manera:

- Selección de una clave simétrica aleatoria.
- Codificación de los datos con la clave seleccionada.
- La clave aleatoria se codifica con la clave pública del receptor y se incluyen en el mensaje.
- El receptor decodifica la clave aleatoria temporal al usar su clave privada y desencripta los datos.

2.4.4.4. Técnicas de encriptación.

Los esquemas de encriptación iniciales eran relativamente simples y no usaron claves de encriptación o desencriptación. Aquel que conociera los algoritmos de encriptación podía desencriptar el mensaje, algoritmos mantenidos en secreto.

El proceso de encriptar o desencriptar un mensaje es mostrado en la siguiente figura:

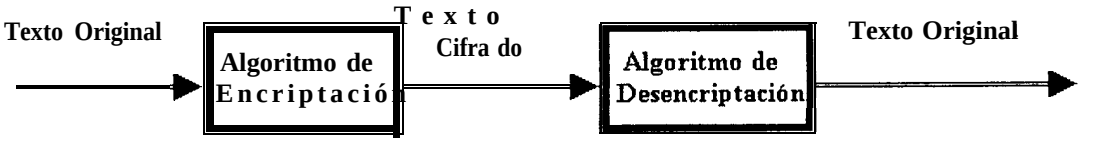


Figura 2.3. Encriptación y desencriptación de un mensaje.

2.4.4.4.1. Encriptación sin claves.

- Enct-iptación de Sustitución.- Cada carácter o grupo de caracteres en el texto original es sustituido por otro carácter o grupo de caracteres en el texto codificado.

- Encriptación de Transposición.- El mensaje original es el mismo sin que el orden del texto sea igual porque los caracteres se encuentran mezclados.

- Encriptación con Máquinas de Rotación.- Las máquinas de rotación son sistemas de encriptación mecánicos. La máquina tiene algunos rotores que al arrancar alteran la ubicación de cada uno de los caracteres del texto original.

2.4.4.4.2. Encriptación con claves.

- Libro de códigos.- Utiliza páginas numeradas y posicionamiento de palabras para codificar un mensaje que puede ser entendido por quién conoce que libro es usado como la clave.

- One time Pads.- Cadena de caracteres aleatorios acordados previamente entre dos sistemas de encriptación finales. El texto codificado está formado por la realización de la operación or – exclusivo de cada carácter del texto original con el próximo carácter de una cadena aleatoria llamada one *time pad.* De forma similar el texto original es restablecido por la ejecución de la función or – exclusivo sobre el texto codificado con el próximo carácter correspondiente de la cadena aleatoria de caracteres. El problema con este esquema es que la longitud de la secuencia aleatoria generada no puede repetirse otra vez.

2.4.4.5. Estándares de Encriptación.

En toda implementación de encriptación es importante seguir los estándares existentes. Crear un algoritmo de encriptación es un trabajo intenso y casi imposible de probar. Los mejores y confiables algoritmos se encuentran disponibles para uso general; han sido probados algunos años por el público por lo que se consideran confiables. Existen estándares para aplicaciones que usen claves simétricas y asimétricas.

2.4.4.5.1. Algoritmos de Clave Simétrica.

El sistema de encriptación de Claves Simétricas utiliza el mismo algoritmo de encriptación y la misma clave para codificar y decodificar. Los dos sistemas mantienen un contacto inicial, o quizá a través de una tercera parte confiable, para coordinar la clave secreta.

Existe la necesidad de mantener un contacto inicial y de coordinar el sistema de encriptación de claves simétricas más apropiado cuando solo se necesita comunicarse con un pequeño número de lugares y donde la distribución inicial de claves secretas, para cada par que necesite encriptación, no es una tarea agobiadora. El usuario deberá coordinar las claves secretas iniciales para el sistema una sola vez y ambos sistemas utilizarán un protocolo de administración de claves para levantar el empleo de claves de sesión que se usarán para

codificar los datos del usuario. Las claves de una determinada sesión pueden intercambiarse periódicamente por los dos sistemas para minimizar la cantidad de exposición, y reducir el riesgo de que la clave de determinada sesión sea ilegalmente interceptada.

Los siguientes son cuatro algoritmos simétricos más comunes:

1. DES(Data Encryptíon Standard)

- Desarrollado por IBM, analizado por la NSA y certificado por el NBS. DES tiene 20 años de antigüedad y ha sido extensivamente estudiado. Tiene 16 claves sencillas conocidas.

- Opera en modo de Codificación de Bloques (Block Cipher), agrupando datos en bloques de 64 – bit.

2. Triple DES.

- Variante mejorada de DES.

- Utiliza dos claves DES (56 bits cada uno). El texto codificado está formado por la encriptación del texto original (64 bits a la vez) con la primera clave DES, luego desencripta el resultado con la segunda clave

DES y, finalmente, otra vez encripta el resultado con la primera clave DES.

- La eficiencia de la clave es de ll 2 bits (2 veces más que la clave DES).

3. IDEA *(International Data Encryption Algorithm).*

- Desarrollado por la Universidad de Zurich en 1992. Fue registrado en Europa y USA. Hoy es patentada por Ascom Tech AG.

- Utiliza claves de 128 bits.

- IDEA también comprende un bloque codificado y datos encriptados en bloques de 64- bit.

4. RC4.

- Cadena de codificación con claves de tamaño variable desarrollada en 1987 por Ron Rivest RSA para Data Security Inc.

- En 1994, se lo presentó a nuevos grupos de usuarios de la red vía Internet desde sites ftp alrededor del mundo, ha sido discutido en conferencias y enseñado en cursos de criptografía.

- RC4 es empleado en productos criptográficos comerciales de la línea Lotus Notes, Apple AOCE y Oracle Secure SQL. El SSL (Secure Socket Layer) usado por Netscape puede utilizar RC4 o DES como codificador de datos de gran capacidad.

2.4.4.5.2. Algoritmos de Clave Asimétrica.

los algoritmos de clave pública son asimétricos y operan con dos claves: una pública y otra privada. Las dos claves están relacionadas sin que sea posible deducir la clave privada a partir de la pública. El texto original es codificado con la clave pública y decodificado con la clave privada. Los sistemas de la clave pública se basan en anagramas confiables de Issuing Authorities (IAs).

Una persona o sistema que desee utilizar algoritmos de claves asimétricas se registra con una clave pública del IAs que le asigna una clave pública y una privada. La clave pública es certificada con tecnología de *Firmas Digitales,* difícil de falsificar. La clave pública se distribuye libremente, en tanto que la privada solo la posee el propietario.

Para transmitir un mensaje encriptado a la persona A, se codifica el mensaje con la clave pública de A y se lo envía. El mensaje sólo puede desencriptarse con la clave privada de A, por lo que ningún sistema que espíe el envío es capaz de decodifìcar el mensaje.

Los sistemas de clave pública se diseñan para aplicaciones en las que se necesita autenticar y comunicarse con un gran número de usuarios sin tener que establecer contactos privados de forma separada para coordinar las claves. Sin embargo, la ventaja tiene límites.

El proceso de verificación de un mensaje codificado con clave pública exige procesar información intensivamente por lo que el sistema se vuelve demasiado lento para codificar una mayor cantidad de datos.

Los algoritmos de encriptación de clave pública más comunes son:

1. RSA (Denominado por sus inventores- Rivest, Shamir y Adleman)

- Es muy popular y se usa en encriptación y en firmas digitales. La encriptación de claves públicas es, por lo general, mucho mas lenta que los algoritmos simétricos. RSA, por ejemplo, implementando en software es 100 veces mas lento que DES y, aplicado en hardware 1000 veces menos rápido que DES.

2. DSA (Digital Signature Algorithm)

- DSA fue diseñada por NSA y aprobada por el NIST en 1993 como el Digital Signature Standard (DSS). Utiliza claves de 1024 bits y es empleado en la

verificación de firmas digitales. DSA es de 10 a 40 veces más lento que RSA en verificar firmas y no es conveniente para encriptar datos.

2.4.4.5.3. Algoritmos de Intercambio y Autenticación de Claves.

1. *Diffie-Hellman*

- El intercambio de claves Diffie – Hellman está basado en la exponenciación de números primos. La mayor ventaja de este algoritmo de intercambio de claves, es que ambos lados calculan la clave de sesión basándose en parte de la información que puede ser enviada por una red abierta.

- El valor de la clave de la sesión actual nunca es enviado sobre la línea de comunicación.

  El mayor problema sin embargo es la velocidad. El cálculo de potencias de números primos grandes y el muestrearlos de forma aleatoria representa lentitud, bajo el procedimiento de intercambio de clave única.

2. Kerberos

Es un protocolo de autenticacíón confiable de tercer grupo, diseñado para redes TCP/IP. Basados en Criptografía Simétrica (utiliza DES). El servidor Kerberos comparte diferentes claves secretas con cada entidad sobre la red. El conocimiento de la clave secreta equivale a probar la identidad del usuario.

ISAKMP/Oakley (IP Security Association Key Management Protocol)

Protocolo definido en IPSec para administrar el intercambio de claves secretas entre emisores y receptores de ESP y paquetes AH.

SAM (Security Association Message)

Un protocolo propietario de autenticación e intercambio de claves desarrollado por el equipo de encriptación NABU para el proyecto de encriptación 6500.

2.4.4.5.4. Algoritmo Hash (troceo) de una Vía

MD5

Es un algoritmo de troceo rápido que produce una firma de tamaño fijo para cualquier documento.

De forma análoga a CRC utilizado en tramas HDLC o Ethernet para verificar que una trama ha sido recibida apropiadamente. La diferencia principal es que el CRC utiliza un SEED universal fijo, mientras que MD5 utiliza una clave secreta como SEED.

2.4.4.6. Eficacia de Encriptación.

Las claves de encriptación y desencriptación son simplemente una cadena de números binarios (40 o 56 bits para DES y sobre 2048 bits para RSA).

El tamaño de la clave determina el número de posibles valores que la clave puede tomar y basándonos en esto determinamos la eficacia o el grado de seguridad de un sistema de encriptación, ej. : Una clave de 56-bits para una encriptación DES que tiene 7.2 x 10 E 16 combinaciones posibles. Cualquiera que trate de descifrar el texto codificado utilizando un método de fuerza bruta (primero desencriptar con la llave=...000, entonces probar la llave=...0001, 0002,....etc.) necesitará una enorme cantidad de recursos (energía de procesamiento y tiempo) para lograr su objetivo.

1. Clave DES de 40 bit da 1 .1 x 10 E 12 combinaciones.

2. Clave DES de 56 bit da 7.2 x 10 E 16 combinaciones.

3. Triple DES con dos claves (encriptar- desencriptar- encriptar (EDE) encriptar con la primera clave, desencriptar con la segunda clave, entonces encriptar otra vez con la primera clave) duplica la eficacia de la clave de una encriptación DES, resultando en claves de 80 o 11 2 bits con 10 E24 y 10 E33 combinaciones respectivamente. De manera interesante, encriptar y

desencriptar con claves de dos n-bit no da 2 E 2n combinaciones, en cambio el texto codificado puede ser desencriptado con 2E n+1 encriptaciones utilizando un algoritmo de ataque meet-in the middle en el texto original.

4. Claves de 128 bits dan 3.4 x 10 E 38 combinaciones.
5. Claves de 512 bits dan 1.3 x 10 E 154 combinaciones.

2.4.4.7. Historia del DES.

En 1972 y en 1974, National Bureau Standars (NBS), ahora el National Institute of Standars and Technology (NIST) envió un requerimiento para un diseño de un sistema de codificación estándar. Algunas compañías presentaron diseños pero la mejor alternativa fue la propuesta hecha por IBM basándose en un trabajo de encriptación realizado en 1970. NBS entonces fue requerido por la NSA's (National Security Agency) ayudando en la evaluación del algoritmo de seguridad.

En marzo de 1975, la NBS publicó tanto los detalles del algoritmo y las declaraciones hechas por IBM garantizando una licencia libre de derechos de autor para este algoritmo. En noviembre de 1976, el DES fue adoptado como un estándar Federal y fue autorizado para ser utilizado en comunicaciones gubernamentales no clasificadas. El estándar DES ha sido certificado en varias ocasiones 1987, 1993.

Como parte del estándar DES, NIST valida implementaciones de DES. La American National Standars Institute (ANSI) aprobó DES como un estándar del sector privado en 1981 y fue llamado Data Encryption Algorithm (DEA).

2.45 Rendimiento de la Red.

El uso de redes públicas de datos como reemplazo de redes privadas, debe alcanzar altos niveles de rendimiento. Las redes privadas aseguran niveles de rendimiento para garantizar acceso a determinada cantidad de ancho de banda, mientras que las redes públicas comparten el ancho de banda disponible entre múltiples usuarios. Las pérdidas reales o teóricas en el rendimiento de la red y la eficiencia actúa como barrera para ser aceptada dentro de algunas organizaciones. A pesar de sus ventajas, las VPNs no serán aceptadas ampliamente mientras no provean un rendimiento comparable con las redes privadas.

2.451 Control de tráfico.

Una consecuencia natural del incremento de la utilización del Internet para comunicaciones de negocios es la congestión de la red, la cual puede afectar adversamente el rendimiento de la VPN y aplicaciones críticas de la red.

Como una extensión de la red corporativa, una VPN naturalmente incrementa el tráfico en la red, así como el riesgo de que el rendimiento se vea afectado. Los beneficios de las VPN no serán completamente apreciados si los usuarios sufren de deficientes tiempos de respuesta, pérdidas de la señal, u otros retardos o fallas de la red. Debido a esto, una solución VPN debe garantizar confiabilidad y calidad de servicio para permitir a los administradores de la red el definir políticas de administración de tráfico que asignen de forma activa ancho de banda tanto para tráfico entrante y saliente basándose en un relativo mérito o importancia, es decir considerando prioridades.

Esto asegura el rendimiento efectivo de las principales aplicaciones de la red así como otras aplicaciones de alta prioridad sin descuidar tampoco las de baja prioridad. El burst y los efectos de retardo de tráfico de Internet son eliminados, permitiendo a los administradores, el optimizar el tráfico de la red tomando en cuenta las prioridades, límites y garantías de servicio. Esta optimización de la red permite mejorar el rendimiento y aliviar la congestión de la red, forzando de esta forma a esperar al tráfico de menos valor, mientras se establecen conexiones más importantes de una VPN.

La única manera de asegurar que el tráfico de una VPN no entorpezca el funcionamiento general de la red es una administración acertada del ancho de banda utilizado. Hoy en día las organizaciones que piensan implementar Redes

Privadas Virtuales necesitan una garantía de que los requerimientos de procesamiento adicionales a los procesos de encriptación basados matemáticamente no degradarán el rendimiento de la red. La mejor manera de lograr esta garantía es, el delegar todas las operaciones criptográficas a un co-procesador dedicado exclusivamente a la tarea de encriptar y desencriptar mensajes. Esto no solo optimiza el rendimiento, sino que provee una medida adicional de seguridad en el almacenamiento de claves utilizadas para las funciones criptográficas.

En resumen el combinar aceleración basada en hardware con una basada en software al proveer una solución VPN, permite ofrecer hoy en día un alto rendimiento, flexibilidad y escalabilidad, permitiendo a las VPNs escalar desde enlaces Tl hasta las altas velocidades de una ethernet sin disminuir los recursos de procesamiento (CPU).

2.4.6. Escalabilidad.

La amplia aceptación de las VPN depende por sobre su eficiencia y el costo efectivo del desarrollo de redes que varían en complejidad desde configuraciones de dos nodos hasta grandes redes empresariales- de la utilización equipos de redes que varían en costo y rendimiento desde ruteadores empresariales a modems dial-up. En suma, las VPNs deben proveer un servicio

en tiempo real así como garantizar velocidades adecuadas para los datos transmitidos, debido que las redes se encuentran en un continuo crecimiento.

Mientras las corporaciones están explorando la integración de las VPNs en sus redes basadas en enlaces T1 y T3, los carriers y fabricantes de ruteadores planifican sus ofertas para OC-3 y enlaces de mayor tamaño.

La tecnología VPN puede transformar las redes corporativas solamente si ellas proveen múltiples niveles de expansión (escalabilidad). La tecnología actual permite que consideraciones importantes como son: seguridad, rendimiento y escalabilidad sean temas de actualidad, pero todavía muchos productos basados en estas consideraciones han fallado o se han alejado un poco de la meta. ´ La mayoría de los productos diseñados para redes privadas tienen deficiencias en factores importantes para el correcto funcionamiento de una VPN como son: rendimiento, eficiencia, y costo cuando son aplicados en redes públicas.

Otras soluciones denominadas integradas, generalmente no son costosas permitiendo así un amplio desarrollo en un futuro. La tecnología VPN debe ser integrada a la red mientras se toman en cuenta algunas interacciones complejas entre ellas, y el impacto que esas interacciones tienen en la seguridad, rendimiento y escalabilidad de la red empresarial. Los productos deben

optimizar la cantidad de datos procesados, maximizar el ancho de banda compartido de redes públicas de datos, y mantener una alta eficiencia a un costo razonable para una red extensa.

2.4.7. Administración.

Hoy en día la infraestructura de las redes empresariales mantiene un continuo crecimiento, la habilidad de administrar una complejidad creciente es un diferenciador crucial para soluciones VPN. Como una Red Privada Virtual es una extensión de la corporación hacia el mundo externo, también es una extensión de la política de seguridad de la empresa. Es estrictamente necesario que la VPN pueda ser administrada desde la misma consola que se encuentra integrada a los demás elementos de seguridad de la organización. Este es un paso crítico en la implementación de una red segura y exitosa, sin importar el número de oficinas regionales o nodos que formen parte de una VPN.

El poder garantizar una completa seguridad de la organización con una administración centralizada basada en las políticas empresariales, ofrecerá un número de beneficios que se traducen en una rápida y fácil integración de nuevos usuarios, nuevas oficinas y nuevas aplicaciones, ofreciendo la flexibilidad necesaria para efectuar los cambios que una organización necesita.

La rápida adopción del concepto de “empresa extendida” ha ocasionado un incremento explosivo en el número de aplicaciones, usuarios, y direcciones IP en uso a través de algunas organizaciones. La administración de esta voluminosa cantidad de información de usuarios representa formidables desafíos tanto para redes y administradores de seguridad.

En suma, ningún sistema de seguridad en general, no una VPN específica son aplicaciones de plataforma única. Las redes actuales incluyen una conglomeración de plataformas heterogéneas y sistemas operativos. Una verdadera solución empresarial VPN debe ser capaz de trabajar a través de múltiples plataformas para poder ser efectiva. Para soportar un esquema de múltiples plataformas, una VPN debe ser capaz de interoperar entre diferentes soluciones y aplicaciones de varios proveedores. Por ejemplo, una VPN con socios de negocios, distribuidores y clientes deberá implementar una amplia variedad de soluciones de seguridad. La interoperabilidad basada sobre estándares industriales aseguran que la VPN será una efectiva herramienta de comunicaciones para establecer negocios, sin importar cual implementación de un proveedor específico haya sido seleccionada.

2.5. Ventajas y desventajas de utilizar redes VPN.

Mientras las VPN ofrecen ahorro de costos sobre otros métodos de comunicaciones (como son líneas dedicadas y llamadas de larga distancia), tienen además otras ventajas, entre las que podemos considerar, un ahorro indirecto de costos como resultado de requerir menor entrenamiento y menor cantidad de equipos, para proveer un incremento de la flexibilidad, y facilidades de expansión en un futuro (escalabilidad). Al hablar de ventajas debemos primero hacer énfasis en el ahorro de costos de las VPNs basadas en Internet, cuando son comparadas con las VPNs tradicionales.

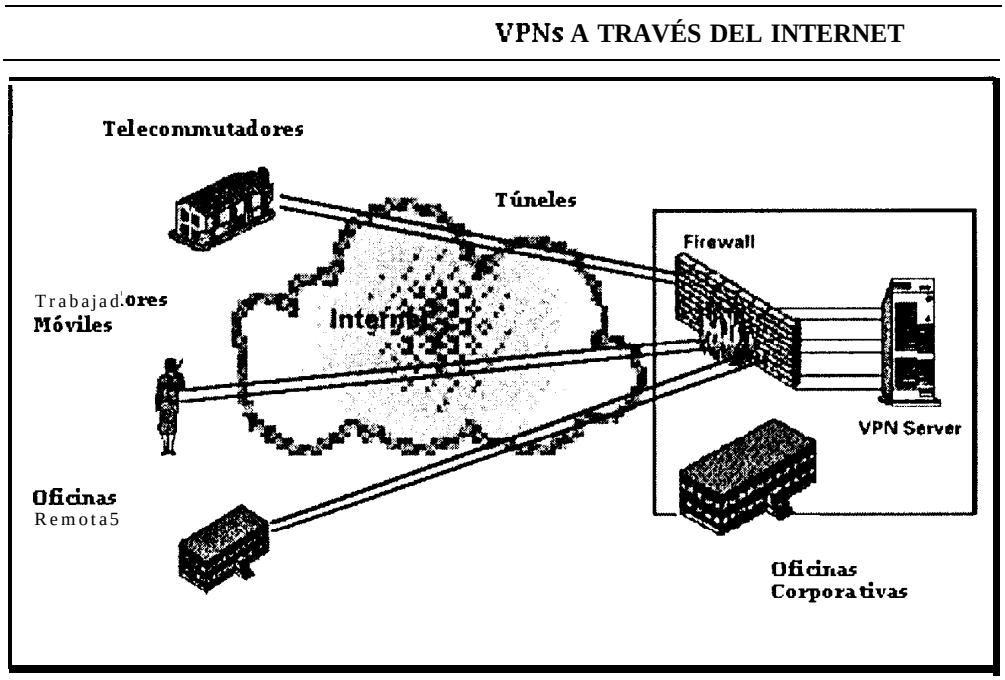


Figura 2.4. Solución VPN.

Una red corporativa tradicional es construida utilizando enlaces dedicados Tl (1.5Mbps), y enlaces T3 (45Mbps) contratados con tarifas que son estructuradas para incluir una cuota de instalación, un costo fijo mensual y una carga por distancia en millas, sumando además cuotas mensuales que son mayores que los valores típicos de conexiones a Internet a la misma velocidad. Las líneas dedicadas ofrecen otra ventaja en cuanto a costos porque algunos proveedores ofrecen precios que son relacionados de acuerdo al uso.

Es una buena opción el escoger los servicios de un ISP como un Tl expandible, para negocios que requieren el uso de un completo Tl o T3 solamente durante los tiempos picos del día pero no necesitan el ancho de banda completo la mayor parte del tiempo. Un Tl expandible provee un ancho de banda sobre demanda con flexibilidad en cuanto a precios. Por ejemplo un cliente que se suscribe para un Tl completo pero cuyo tráfico promedio son 512 Kbps. sobre el circuito Tl, pagará menos que un cliente cuyo tráfico mensual es 768 Kbps.

Como los enlaces punto a punto no son parte de VPNs basadas en Internet, las compañías no tienen soporte para cada clase de conexión, afortunadamente los equipos y soporte tienen costos reducidos. En cambio con redes corporativas tradicionales, el medio que cubre pequeñas oficinas sucursales, telecommutadores, trabajadores móviles (digital suscriber line xDSL), red digital

de servicios integrados (ISDN), y modems de alta velocidad, por ejemplo, debe ser soportada por equipos adicionales en las oficinas corporativas.

En una VPN no solo pueden ser utilizados enlaces T1 y T3 entre la oficina principal y el ISP, sino otros medios que permitan conectar pequeñas oficinas y trabajadores móviles a través del ISP llegando así a la red de la empresa, sin instalar equipos adicionales en su infraestructura de comunicaciones, claro está en los casos de empresas pequeñas que no necesitan una frecuente reconfiguración de equipos. En el caso de empresas de mayor tamaño las necesidades aumentan, se debe entonces implementar mayor cantidad de servicios y debe realizarse un estudio mas detallado.

25.1. Crecimiento de Redes Privadas Virtuales: análisis externo e interno.

Según estimaciones de Forrest Research se estima que el mercado de VPN que tuvo ingresos por US $205M en 1997, crecerá sobre el 100% para el año 2000, cuando este alcance los US$1 1.9B. Estas estimaciones se basan en 3 elementos principales: Productos VPN, Sistemas de Integración y servicios de ISP.

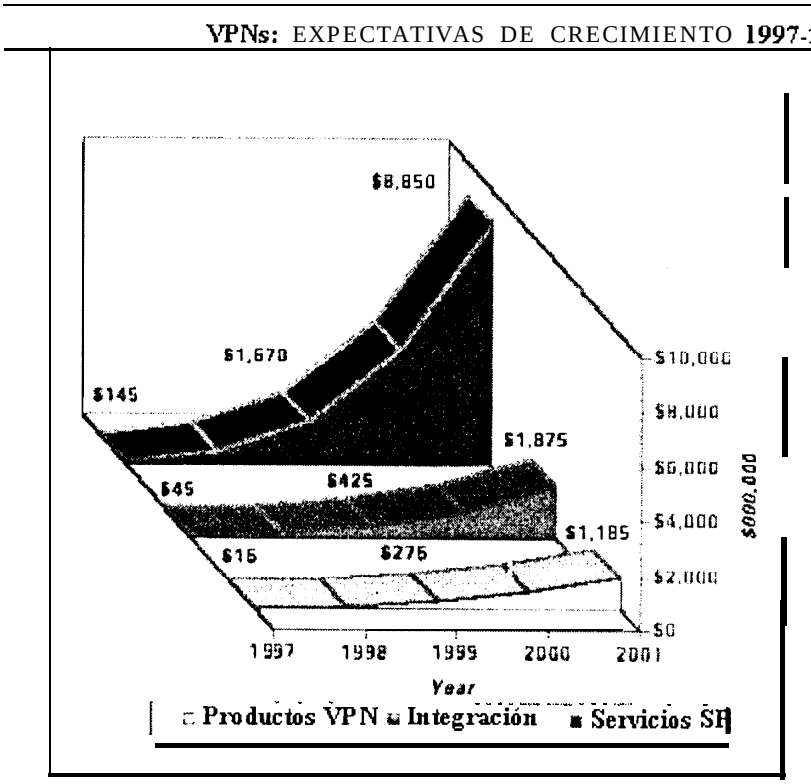


Figura 2.5. Expectativas de Crecimiento de las VPNs.

Como una gran oportunidad, las VPN son ofrecidas debido a un incremento en el número de Proveedores de Internet (ISP). Para marzo de 1998, 92% de los mayores proveedores de Internet ofrecieron alternativas VPN. Hablamos de proveedores como UUNet, BBN, Planet, Internet MCI, Sprint entre otros.

LA MAYORIA DE PROVEEDORES DE SERVICIO ESTAN OFRECIENDO VPNs

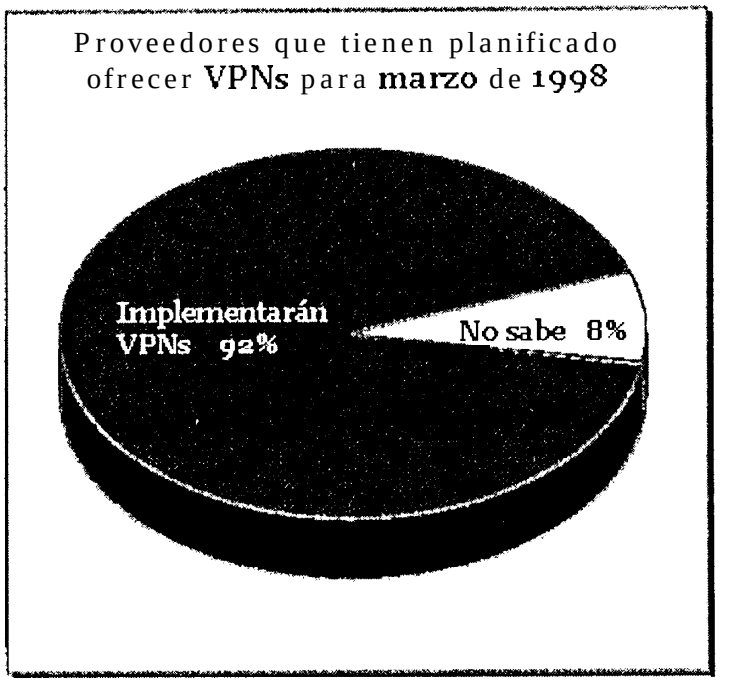


Figura 2.6. Proveedores de Servicios.

A pesar de que algunas redes empresariales y proveedores ISP se dan cuenta de que necesitan VPNs, sin embargo puede que ellos no sepan que las VPN tienen muchas variedades de implementaciones, y cada una hace consideraciones, como seguridad, rendimiento, conveniencia, costos y facilidades de administración. Afortunadamente la división de responsabilidades entre la administración interna de la empresa y el ISP tiene rangos que van desde la administración completamente interna hasta el completo outsourcing por parte del Proveedor.

Con todas estas expectativas que se observan en países con un avanzado desarrollo del alcance del Internet, podemos proyectar que debido al constante incremento del Internet en nuestro país, es una buena opción el trabajar con este tipo de opciones que permiten integrar empresas con sus sucursales a un menor costo, logrando de esta manera satisfacer la necesidad principal de las empresas que es lograr la integración de sus sucursales y mantenerlas comunicadas de forma efectiva.

El acceso a Internet desde el Ecuador aún es muy limitado debido a la reducida velocidad de los enlaces que existen en nuestro medio. A diferencia de otros países como por ejemplo de Estados Unidos, que cuentan con una red de Servicios Integrados lo cual facilita el acceso a la red. Los niveles de acceso en el Ecuador están limitados a lo que son usuarios finales y empresas proveedoras.

Es bien sabido que el Internet representa un potencial realmente grande en lo que se refiere a la comunicación de las comunidades a nivel mundial, esto es, hoy por hoy podemos hacer compras, de un auto último modelo hasta la consulta médica a través de la conocida “red” sin salir de casa, esto en los países desarrollados se aplica con mucha frecuencia y su uso es cada vez mas difundido. Pero debemos decir también, que en nuestro país, no ha tenido el mismo desarrollo, debido básicamente a que tanto proveedores como usuarios

del Internet en el Ecuador no han sido “muy exigentes”, y el uso del Internet se ha centrado básicamente en el usuario final, es decir una persona que entra a la para buscar información.

2.5.2. Precauciones a considerar.

Hay un número de problemas que se deben resolver, así como decisiones que se deben de tomar, en el momento de implementar una Red Privada Virtual en el mundo real.

- Algunos problemas fuertemente arraigados en las industrias, ya han sido superados, pero algunos son todavía objeto de debates y largos procesos para lograr la estandarización.

- El Internet no fue diseñado desde su etapa inicial tomando en consideración un esquema de alta seguridad, lo que significa que las corporaciones para poder enviar su información más sensible necesitan trabajo adicional para asegurar que solo las personas correctas tengan acceso a la red de la corporación (es decir puedan autentificarse positivamente), y además tener la certeza de que los datos no puedan ser leídos por personas ajenas a la organización.

- El Internet no fue diseñado tampoco para garantizar rendimiento y entrega segura de la información. Las aplicaciones diseñadas para trabajar en una red con una determinada latencia (latency), quizá no funcionen de forma adecuada en el Internet.

- Finalmente, existen algunas técnicas diferentes que permiten implementar VPN sobre el Internet. Tres de las más populares son PPTP (Point to point tunneling protocol) esta es una clase de L2TP (Layer 2 tunneling forwarding) y el IPSec (IP Security).

2.6. Implementaciones típicas de VPN.

Hay varios tipos de implementaciones de Redes Privadas Virtuales, cada una con un grupo específico de requerimientos tecnológicos. Sin embargo, el desarrollo de las VPN se puede agrupar dentro de tres categorías primarias de acuerdo a la Topología de Red que presenten.

- *Intranet*: VPNs entre los departamentos corporativos internos y sus oficinas sucursales.

- *Acceso Remoto:* VPNs entre una red corporativa y empleados móviles o remotos.

- *Extranet*: VPNs entre la red corporativa, sus socios de negocios, clientes y proveedores.

2.6.1. Intranet.

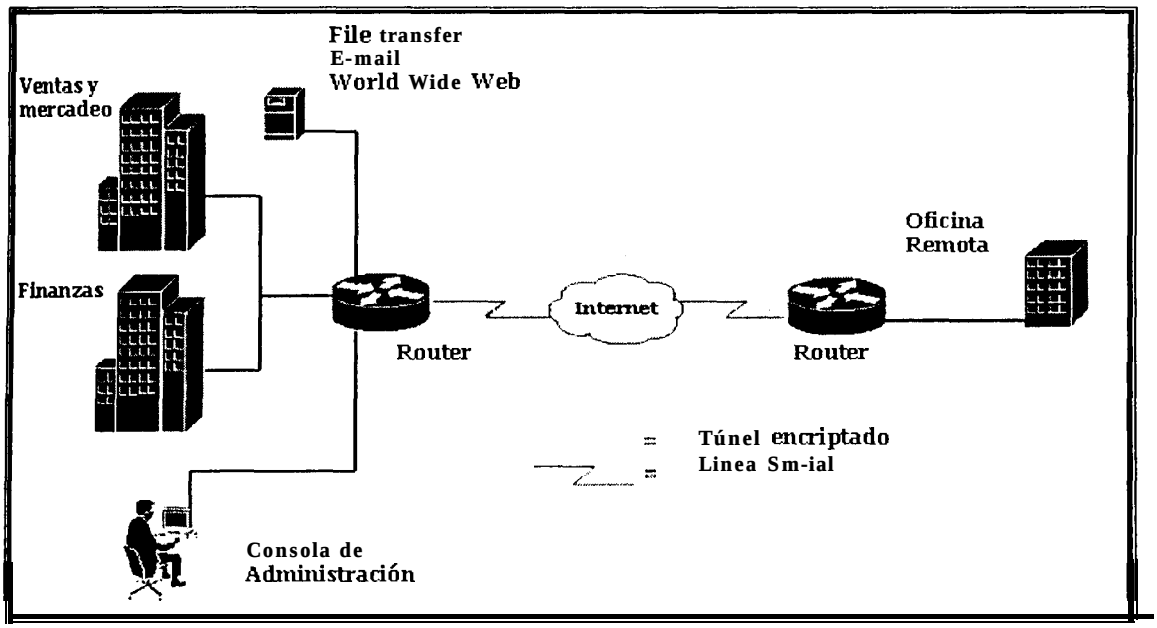


Figura 2.7. Implementación de una VPN tipo Intranet.

Los requerimientos tecnológicos primarios en una VPN tipo Intranet que facilita comunicaciones seguras entre los departamentos internos de una compañía y sus oficinas sucursales son: una encriptación de datos bastante robusta para proteger información sensible; confiabilidad para asegurar la prioridad de ciertas aplicaciones críticas, como sistemas ERP, ventas y administración de la base de datos de los clientes, e intercambio de documentos; y administración expandible

para asimilar el rápido crecimiento de nuevos usuarios, nuevas oficinas y nuevas aplicaciones.

2.6.2. Acceso Remoto.

El Acceso Remoto de VPNs entre una red corporativa y empleados móviles o remotos tienen diferentes requerimientos. Una autenticación bastante confiable es un elemento crítico para verificar la identidad de usuarios móviles o remotos de la manera más exacta y eficiente posible. En el lado administrativo, el acceso remoto a VPN requiere una administración centralizada y un alto grado de posibilidad de expansiones futuras para manipular un amplio número de usuarios que tienen acceso a la VPN.

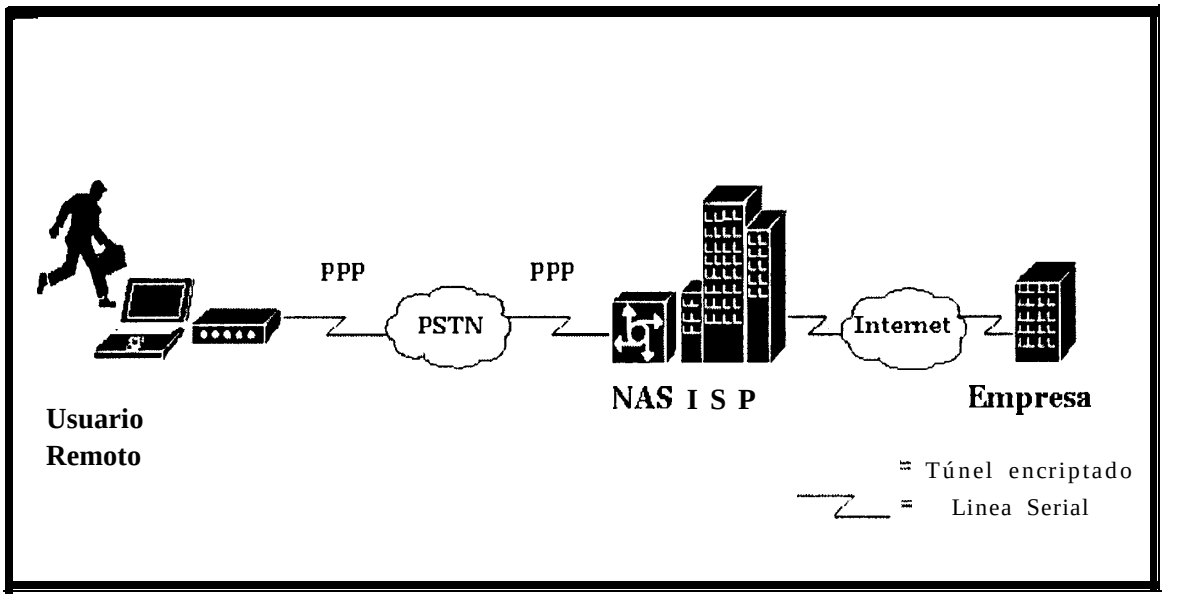


Figura 2.8. Implementación de una VPN tipo Acceso Remoto.

2.6.3. Extranet.

Finalmente, una VPN tipo Extranet entre una compañía y sus socios estratégicos, clientes y proveedores requieren apertura así como, diseños basados en estándares que aseguren interoperabilidad con diferentes soluciones que las sociedades de negocios puedan implementar. El estándar aceptado para VPNs basadas en Internet es el Standard Internet Protocol Security (IPSec). Algo importante que se debe considerar es el control del tráfico para eliminar cuellos de botella en los puntos de acceso a la red, NAP (Network Access Point) garantizando una rápida entrega y mejorando los tiempos de respuesta para datos críticos.

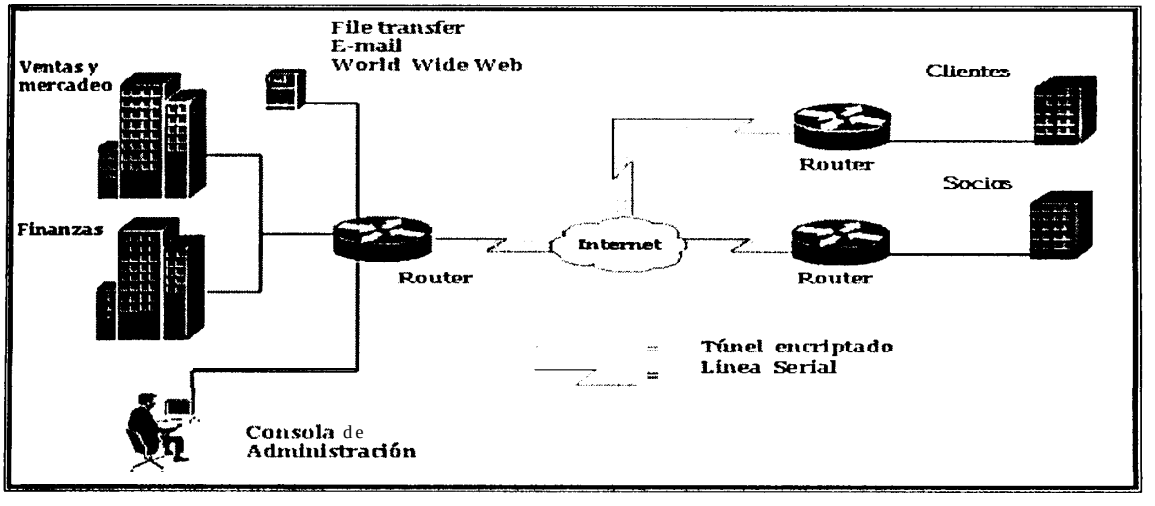


Figura 2.9. Implementación de una VPN tipo Extranet.

Como las VPN representan solo un componente en una completa política de seguridades, el desafío es proveer un esquema bastante comprensivo de una solución integrada.

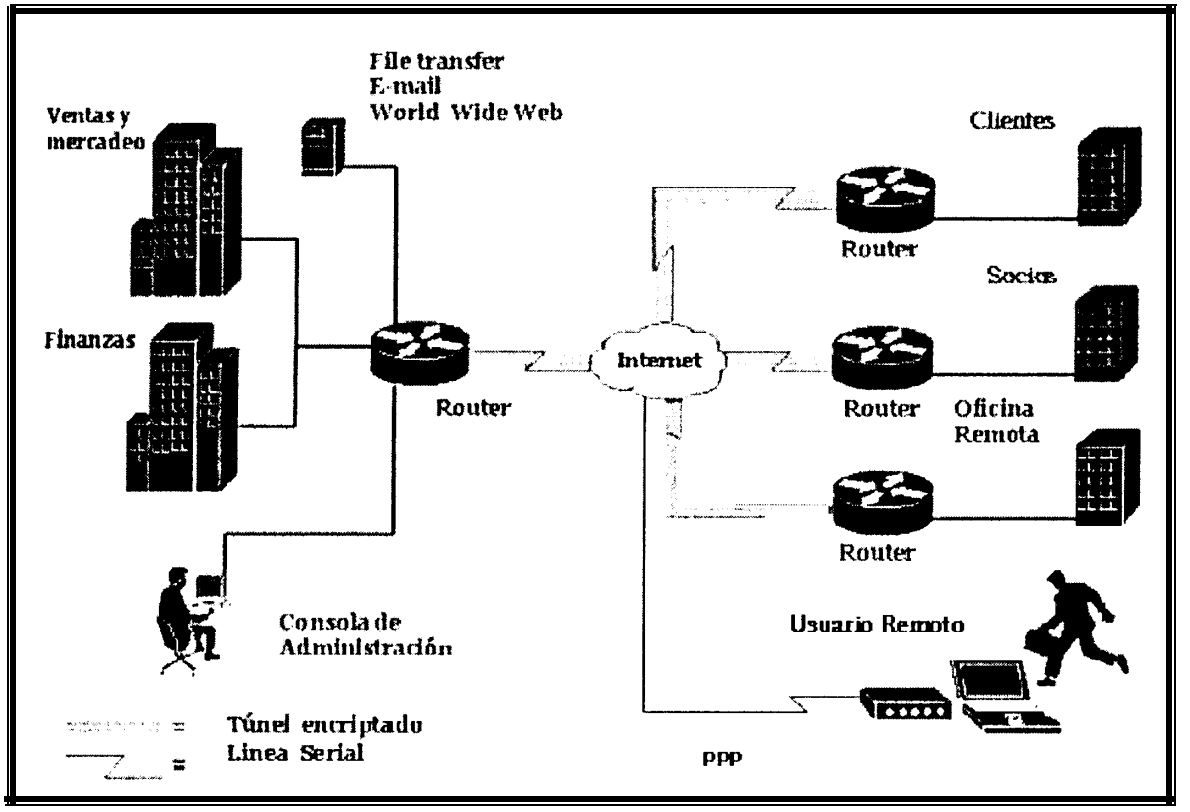


Figura 2.10. Implementación completa de una VPN.

En el mercado de las VPN no se aplica siempre el mismo esquema. La mayoría de los proveedores de VPN hoy en día, proveen soluciones que encajan en alguna de estas implementaciones VPN debido a que, como la

mayoría de las compañías tienen sucursales que seguramente necesitan enlazarse, incrementar la fuerza de trabajo móvil, y la facilidad que ofrece el Internet para mantener cercanos tanto a los clientes como a los socios de negocios. Una solución VPN debe soportar cualquiera de las tres aplicaciones, permitiendo de esta manera a las oficinas alrededor del mundo accesar a los recursos de la red corporativa, a los trabajadores móviles enlazarse a las intranets corporativas, a los clientes realizar pedidos y a los proveedores, chequear niveles de inventarios, todos estas facilidades dentro de una administración segura y menos costosa.

Mientras en la actualidad una corporación puede planificar la implementacíón de uno de estos tres tipos de VPN, es muy necesario que la solución VPN que se seleccione ofrezca la posibilidad de ampliarla en un futuro (dependiendo de las expectativas de crecimiento de la empresa) hacia uno o ambos tipos de implementaciones adicionales.

2.7. Clasificación de Redes VPN.

Como las VPN varían en propósito, tamaño, alcance y complejidad. Aún no están totalmente claras las reglas para clasificar a las VPN tomando en cuenta toda esta amplia variedad de factores. La clasificación de las redes en “ clases” ofrece un esquema bastante claro y breve, tanto para usuarios como para

proveedores de servicios para determinar rápidamente los tipos de tecnologías que sean necesarias desarrollar, basadas en las aplicaciones que se necesiten implementar. Los servicios que ofrece una VPN, dependen del tamaño y necesidades que se presenten en la red.

2.7.1. VPN Clase 0.

Este tipo de VPNs generalmente es utilizado para compañías pequeñas, que cuentan con un enlace al proveedor (ISP) y un número limitado de trabajadores remotos. Esta VPN es la más simple y menos costosa de implementar, utiliza PPTP y filtrado de paquetes para intranets. Como un mínimo necesita la instalación de Windows NT, o para añadir un leve nivel de seguridad, un software de VPN instalado en un servidor.

Las VPN de clase 0 proveen acceso al correo electrónico y a una base de datos interna en la oficina principal, así como acceso a archivos para un promedio de 50 usuarios remotos, a través de conexiones dial-up. La oficina principal tiene acceso al proveedor de servicio a través de una fracción de Tl. Esta es la más básica de las VPN y por ende la más simple y económica de implementar.

Ofrece una fácil manera de probar el funcionamiento del acceso remoto. Las debilidades de las VPN de este tipo son la poca flexibilidad para los enlaces

entre oficinas sucursales, así como los grandes tiempos que pueden transcurrir hasta solucionar los problemas, si el software que reside en un servidor falla.

2.7.2. VPN Clase 1.

Este tipo de VPN es óptima para compañías de tamaño pequeño a medio con múltiples oficinas sucursales que necesitan ser enlazadas, con conexiones al Internet de cerca de un Tl, y con sobre 250 usuarios remotos. Las VPNs de clase 1 ofrecen seguridad básica con IPSec, con encriptación DES, y autenticación de password para acceso remoto hacia archivos, correo electrónico y a bases de datos internas. Estas VPN son implementados a través de un hardware llamado VPN gateway con un software versión cliente para acceso remoto con IPSec. Los beneficios son el fácil diseño e instalación, bajo costo, enlace entre oficinas así como usuarios remotos, y gran seguridad sin degradación de rendimiento. Sin embargo, extranets no son soportadas a menos que la implementación IPSec utilizada haya sido certificada para interoperabilidad.

2.7.3. VPN Clase 2.

Son aplicables para compañías de tamaño medio con usuarios remotos sobre los 500 y más de diez oficinas sucursales, como firmas de ingeniería o publicidad, y agencias de mercadeo que tienen propiedades de gran valor

intelectual. Las conexiones de las oficinas sucursales son provistas por uno o algunos enlaces Tl. Las VPNs de clase 2 ofrecen altas seguridades, con encriptación 3DES y un robusto sistema de autenticación de usuarios (factor dos), utilizando un método tal como software tokens. La escalabilidad puede ser incrementada a través del uso de servidores RADIUS para administrar los nombres de usuarios, passwords y políticas empresariales. Las VPNs de clase 2 pueden coexistir con firewalls y proporcionar NAT (Network Address Translation) para permitir que los sites sean direccionados privadamente y sean enlazados sin requerir cambios en los esquemas de direccionamiento de las LAN existentes.

Entre los beneficios de las VPNs de clase 2 se encuentran los siguientes: el proveer una alta seguridad, reducción de costos, y soporte para comunicar entre distintos sites como con accesos remotos. La debilidad de esta clase de VPN es la carencia de soporte para extranets y aplicaciones en tiempo real.

2.7.4. VPN Clase 3.

Este tipo de VPN dan soporte a compañías de tamaño de medio a grande con miles de usuarios remotos y cientos de oficinas se incluye también a socios de negocios y clientes de la empresa para de esta forma; enviar y recibir estados de cuenta de los clientes, proveer transacciones en cadena, y transacciones

e-commerce (comercio electrónico). Usuarios de este tipo podrían ser proveedores de insumos médicos, compañías de seguros, fábricas o compañías que son parte de una extensa cadena de proveedores. Los enlaces de las oficinas sucursales comprenden típicamente valores fraccionarios de un enlace Tl, un Tl completo o múltiples Tl. Las conexiones de la oficina principal al ISP pueden ser enlaces Tl, fracciones de T3 o enlaces full T3. Usuarios remotos pueden accesar mediante enlaces xDSL o conexiones cable – módem, o acceso dial. Este tipo de VPNs utilizan un proveedor de servicios que ofrece niveles de calidad de servicio QoS, niveles que permiten garantizar tiempos de respuesta aceptables para aplicaciones críticas que corren entre sites corporativos conectadas al backbone del proveedor. El uso de sistemas de certificación de interoperabilidad IPSec, habilita extranets para usuarios que se encuentran dentro de diferentes redes con diferentes tipos de equipos.

En suma las posibilidades de autenticación, considerando usuario y nivel de acceso, tales como autenticación tokens two-factor o tarjetas inteligentes (smart cards), dan soporte accesos remotos seguros, y habilita el servicio de niveles de acceso para usuarios a información disponible para ellos, como reportes o facturación. Para una administración con facilidades de crecimiento a futuro, las VPN de clase 3 emplean servicios de directorios para almacenar y recuperar políticas de la empresa (grupo de usuarios que tienen acceso a determinados

recursos), así como almacenamiento de certificados digitales utilizados para autenticación de usuarios.

Por este motivo siempre es necesario ya sea, un certificado de autorización in-house, un servicio de certificación administrado externamente o algún método de administración de una infraestructura de claves públicas (PKI). Una implementación de este tipo de VPN requiere bastante habilidad debido a que se basa en diseños mas sofisticados, necesita también una administración constante y va a demandar mayor cantidad de recursos.

En suma, la implementación de políticas sofisticadas para el control de acceso tanto para empleados como para socios, necesita, desarrollo, implementación y administración de la totalidad de una política de seguridades corporativa.

2.7.5. VPN Clase 4.

Son las redes más seguras, flexibles y con posibilidades de crecimiento futuro. Ellas dan soporte para transacciones con altas seguridades para empresas multinacionales, con mas de 10.000 usuarios y cientos de sites corporativas, que tienen extensas cadenas de sociedades de negocios y necesitan un alto grado de outsourcing (administración externa), como agencias gubernamentales e instituciones financieras. Las oficinas sucursales pueden ser conectadas sobre enlaces fraccionarios T1/E1, completos T1/E1, o múltiples T1/E1, y las oficinas

matrices pueden tener acceso a Internet a través de enlaces fraccionarios T3, full T3 o líneas OC3. El rango completo de alternativas de acceso remoto comprende desde accesos dial a xDSL y cable módem. La utilización de una red de proveedores de servicio que ofrezca calidad de servicio en tiempo real QoS y SLAs en conjunto con soporte para administración de ancho de banda, y convergencia de aplicaciones como el uso de voz sobre IP e IP vídeo conferencia. Las VPN de clase 4 hacen un extenso uso de los servicios de directorio y de tecnologías PKI para administrar las políticas empresariales, verificación del rol de los usuarios así como su identidad. Estas VPN pueden dar soporte a sofisticadas relaciones de confianza entre extranets involucrando de esta manera a múltiples socios así como independientes y múltiples sistemas PKI. VPNs de clase 4 son bastante complejas y costosas de implementar, y requieren una eficiente administración de toda la información saliente.

Capítulo 3.

3. Descripción de los protocolos a utilizarse.

3.1. Introducción a los protocolos a emplearse en el diseño.

Los protocolos actúan en los procesos que establecen comunicación entre computadoras distintas, desde la transmisión de un flujo de bits a través de un medio físico (proceso de bajo nivel) hasta los que comparten o transfieren información desde **un** computador a otro de una red (proceso de alto nivel).

Los protocolos describen los formatos que presentan los mensajes a intercambiar por los equipos de cómputo y definen las reglas a seguir para obtener una comunicación exitosa.

Los protocolos interactúan entre sí, dialogando con otros protocolos del mismo nivel de una computadora remota.

Aquí especificaremos en forma técnica el software que utilizan las redes virtuales privadas con énfasis en la descripción de los protocolos que emplean, referidos a dos aspectos básicos que son: establecer sus funciones y principales características.

Explicamos qué es el protocolo TCP/IP, para qué fue desarrollado y cómo funciona. Sabemos que él constituye la columna vertebral sobre la cual se asienta el Internet por permitir que la información, organizada en paquetes, viaje de un lugar a otro de la red en forma fiable.

Describimos el protocolo Frame Relay, un protocolo de transporte, que transmite datos de forma segura a altas velocidades y que optimiza los tiempos de respuesta de las redes.

Nos parece interesante explicar el funcionamiento de estos protocolos porque son, en sí, el esquema en que se apoyan los protocolos que sustentan las redes privadas virtuales; además, son los protocolos estándares manejados por cualquier red conectada a Internet, de allí nuestro interés.

3.2. Protocolo TCP/IP.

3.2.1. Origen.

En las puertas de los años 70, ARPA (Agencia de Proyectos Avanzados del Departamento de Defensa de los EE.UU.), que a la postre se conocería como DARPA, conjuntamente con algunas universidades y otros organismos de investigación de los EE.UU, iniciaron un programa para crear tecnologías que permitieran transmitir paquetes de información entre redes de distintos tipos y características.

El proyecto tuvo como meta principal interconectar redes, por lo que se llamó “Internetting” , y la familia de computadoras que surgió de esta investigación se denominó “Internet”.

Así se construyó ARPANET (Advanced Research Projects Agency Network) primera red de conmutación de paquetes. Ésta, en su etapa experimental, empezó a funcionar en 1969 con cuatro nodos experimentales.

De esta forma empezó a crecer hasta cubrir la totalidad de los EE.UU. y quedar a cargo de la Agencia de Telecomunicaciones para la Defensa DCA (Defense Communications Agency). Aún es considerada una red de investigación.

Cerf y Kahn, en 1974 propusieron utilizar un nuevo núcleo de protocolos que constituyeron la base del protocolo de Internet IP y del protocolo de Control de Transmisión TCP. Estos protocolos, de mayor rapidez y menor tasa de errores, reemplazaron a los anteriores que venían siendo utilizados por ARPANET.

En 1978, por medio de exigentes pruebas, los nuevos protocolos demostraron su eficiencia y, a partir de 1980, toda la red ARPANET se volcó a su uso. En 1990, ARPANET dejó de funcionar oficialmente, lo que fue marcando el inicio del Internet que conocemos ahora.

3.2.2. Principales características.

El TCP/IP fue diseñado para conectar equipos no compatibles de diferentes fabricantes. Esta característica, la independencia, en la cual el protocolo establece el enlace no siendo necesaria la compatibilidad entre el hardware y software, es definitiva para el nacimiento del esquema de múltiple acceso que se brinda a todos los usuarios en una misma red, que hoy se conoce como Internet; de esta forma éstos pueden accesar a servicios genéricos y compartir recursos.

La arquitectura, otra característica, se refiere al mecanismo para ejecutar procedimientos de manera progresiva, no simultánea, porque se requiere el resultado del proceso anterior para ejecutar el siguiente.

3.2.3. Arquitectura.

El conjunto de protocolos TCP/IP realiza los siguientes procedimientos:

- Estructura los datos en paquetes o datagramas IP.
- Determina la ruta a seguir por estos paquetes para llegar a su destino.
- Los transmite por el medio físico.
- Regula la tasa de envío de los paquetes de acuerdo con el ancho de banda disponible y la capacidad del receptor.

- Reconstruye las tramas que llegan en la secuencia correcta.

- Comprueba si hay tramas repetidas.

- Notifica al transmisor los datos recibidos correctamente.

- Entrega los datos a la aplicación correcta.

- Maneja los eventos de errores y problemas.

El software de comunicaciones es complejo y, por esta razón, está organizado en módulos diversos. Significa que para comprender su trabajo se dividió la tarea global de comunicar, en funciones específicas llamadas capas atribuidas a cada módulo. Las funciones que realiza cada capa deben estar relacionadas, por ejemplo, si existen varias acciones dedicadas sólo a enlazar una comunicación podemos agruparlas en una capa a la que llamaremos capa de enlace.

Este enfoque se llama programación modular porque realiza programas específicos para cada módulo y no para todo el sistema de comunicación.

La arquitectura TCP/IP está basado en el modelo OSI, es una arquitectura de interconexión de sistemas abiertos. En la Figura 3.1 presentamos un diagrama que permite observar el diseño de ambas.

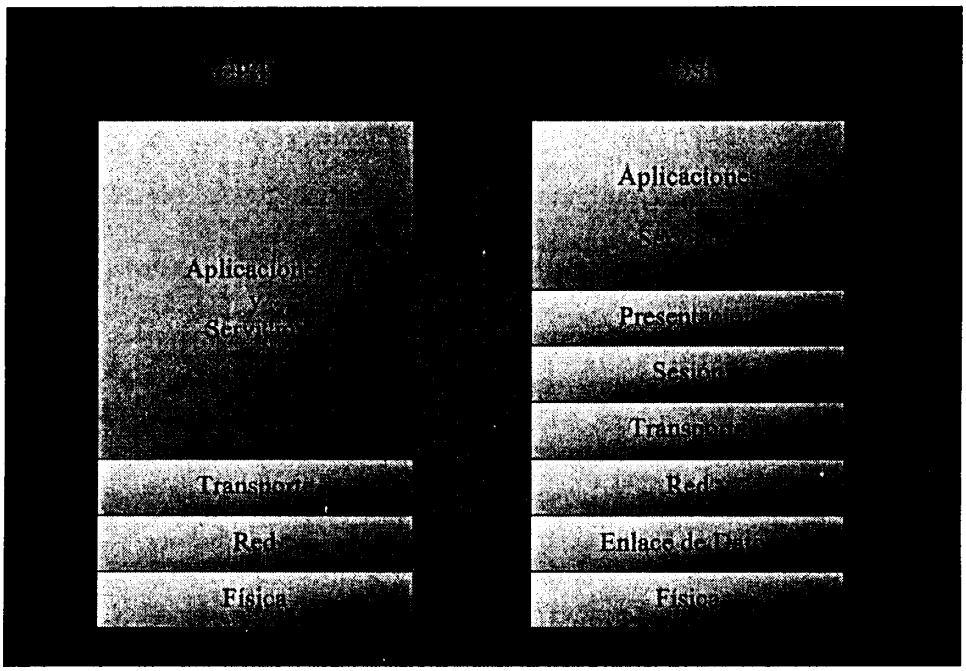


Figura 3.1. Capas de TCP/IP y de OSI.

El primer módulo del protocolo TCP/IP es la capa física que corresponde, exclusivamente, al hardware. En de este nivel se encuentran los protocolos ARP y RARP.

El protocolo ARP (Address Resolution Protocol) convierte las direcciones IP en direcciones físicas. Es indispensable, para que dos computadoras puedan comunicarse, conocer la dirección física de la máquina receptora. La máquina emisora del mensaje sólo conoce la dirección IP del destino, lo que hace necesario traducirla a su equivalente física, esto se hace con el protocolo ARP.

El protocolo RARP (Reverse Address Resolution Protocol) opera en forma inversa al protocolo ARP; su función es asignar una dirección IP a cada dirección física.

El segundo módulo del protocolo TCP/IP es la capa de red que permite el control de la comunicación entre un equipo y otro. Entre sus funciones consta la de conformar los paquetes de datos a enviar por la capa inferior, desencapsularlos cuando son recibidos y pasar, de inmediato, a la capa superior la información dirigida a una aplicación.

El protocolo de Internet IP (Internet Protocol) realiza las funciones de la capa de red al encaminar los datos entre los diversos sistemas. Los datos se transportan en unidades (datagramas o paquetes IP) que pueden viajar independientemente por enlace único o por varios enlaces de una red internet.

El tercer módulo del protocolo TCP/IP es la capa de transporte, la encargada de proveer el servicio de comunicación, extremo a extremo desde un programa de aplicación a otro.

El transporte de datos es confiable: garantiza la entrega de éstos sin errores y en la secuencia correcta. Coordina también múltiples aplicaciones para que interactuen en forma simultánea con la red de manera tal que los datos que envíe una aplicación sean recibidos correctamente por la aplicación remota.

En esta capa trabajan los protocolos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol).

El protocolo TCP de control de transmisión realiza las funciones de la capa de transporte. Proporciona servicio de conexión segura de datos a todas las aplicaciones. Posee métodos de chequeo de errores, control del flujo y capacidad de interrupción que, en suma, garantizan que la transmisión de datos sea exitosa: sin errores, en secuencia y sin omisiones. Es un protocolo orientado a conexión, por lo que forma un circuito en que el flujo de datos entre origen y destino parece continuo. TCP proporciona un circuito virtual llamado conexión.

El protocolo UDP autoriza el envío de paquetes independientes llamados paquetes UDP de una aplicación a otra, tal cual lo hace el protocolo TCP. Es un protocolo no orientado a conexión, no forma circuitos virtuales y además no ofrece garantías de que la información llegue a su destino.

El último módulo del protocolo TCP/IP es la capa de aplicaciones y servicios, en la cual constan todas las aplicaciones y servicios disponibles para los usuarios como son TELNET, FTP, SNMP. A continuación citamos algunos de éstos y explicamos brevemente, en qué consisten:

- Transferencia de archivos. Utilizan el protocolo FTP (File Transfer Protocol), que faculta a los usuarios para copiar archivos, ya sean de texto ASCII o de datos binarios, transferirlos a otro sistema y accesar a sistemas lejanos a fin ejecutar tareas básicas.

- Comunicación entre aplicaciones. Existen dos tipos: Enlace orientado a conexión de TCP, conveniente con un flujo de datos continuo y, enlace corientado a la no conexión UDP, recomendable para transmitir mensajes esporádicos entre una aplicación y otra. Poseen una interfaz de programación de conectores y otra de programación de llamadas a procedimientos remotos RPC (Remote Procedure Call).

- Terminal virtual. Funciona con el protocolo de terminal virtual de Telnet que vuelve compatible los sistemas existentes.

- Correo electrónico que utiliza el protocolo simple de transferencia SNMP (Simple Mail Transfer Protocol).

- Servicio World Wide Web que permite elaborar documentos con adición de imágenes y sonidos, puestos en enormes archivos de información a los que se tiene acceso si posee Internet.

- Sistema de dominio de nombres DNS (Domain Name System) que permite, a usuarios y programas identificar computadoras remotas por medio de un nombre sencillo, y contar con la información necesaria para encaminar, adecuadamente, el correo electrónico. Para esto los protocolos DNS traducen cada uno de estos nombres en la dirección de host correspondiente.

- Noticias electrónicas

- Software comercial, desarrollado lógicamente sobre la base de protocolos TCP/IP.

- Acceso a archivos remotos, como si se tratara de locales, y servidor de archivos que mantiene directorios a los que pueden accesar ciertas computadoras. Para esto el TCP/IP incluye el Sistema de archivos de red NFS (Network File System).

- Administración de red por medio de programas compatibles con TCP/IP como el caso del SNMP (Simple Network Management Protocol).

En lo referente al mecanismo empleado para transmitir datos, se conoce como empaquetamiento y consiste en añadir cabeceras correspondientes a cada capa que atraviesa la información en su viaje. Se aprecia mejor en el gráfico de la Figura 3.2.

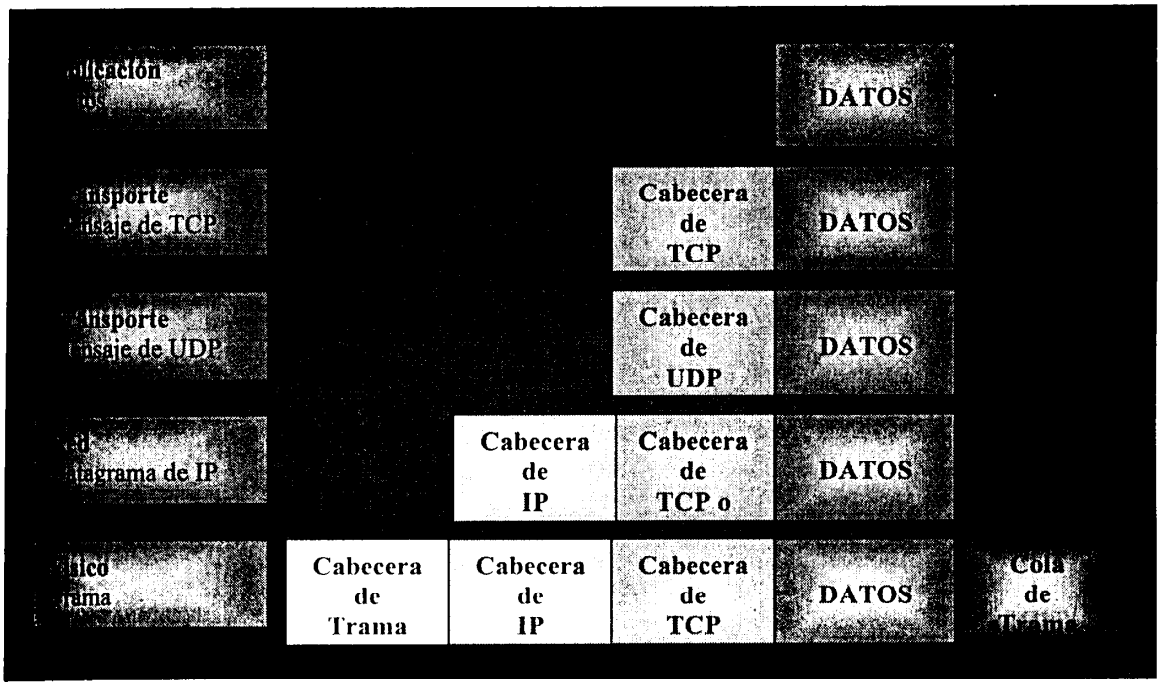


Figura 3.2. Empaquetamiento de los datos para transmisión.

El nombre genérico para cada cabecera es unidad de datos del protocolo PDU (Protocol Data Unit). Una cabecera TCP es una PDU de la capa de transporte.

En la Figura 3.3, se indican los protocolos varios que sirven de interfaz entre el usuario y la máquina empleados en forma independiente por los diferentes módulos o capas del protocolo TCP/IP.

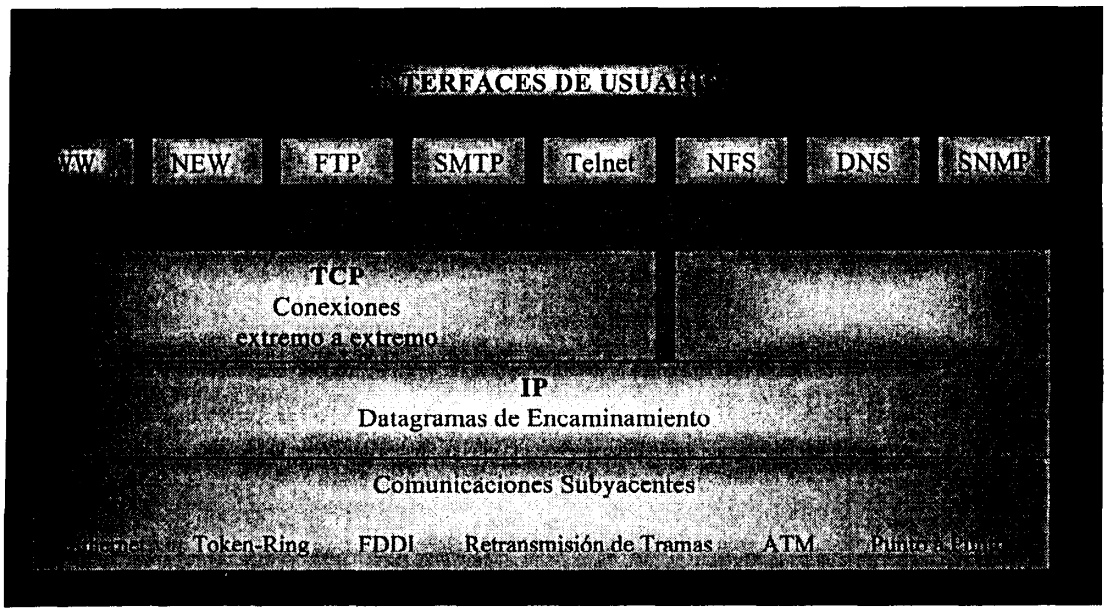


Figura 3.3. Componentes del conjunto de protocolos TCP/IP.

3.2.4. Esquema de funcionamiento.

Para entender cómo trabaja el protocolo TCP/IP hay que conocer la manera cómo se conforma una interred: agrupación de redes independientes más sencillas como las redes de área local LANs (Local Area Network), las de área amplia WANs (Wide Area Network) y la unión de éstas. Todas, sin excepción, soportan el conjunto de protocolos TCP/IP.

La Figura 3.4 muestra los tipos de redes aisladas que existen y la Figura 3.5 describe los routers o encaminadores de IP cuya función es interconectar redes entre sí de manera que constituyan una red más grande (interred).

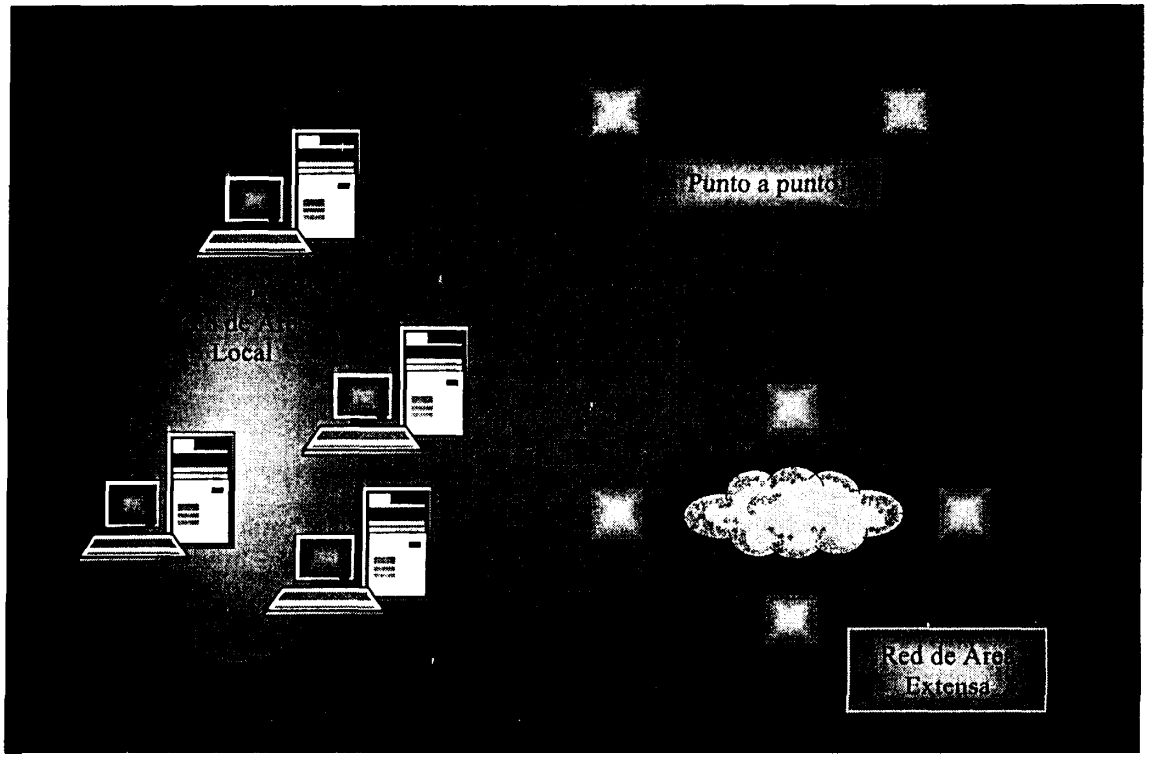


Figura 3.4. Redes independientes.

La función del protocolo TCP/IP es permitir que una red heterogénea, en lo que al uso de tecnologías y topologías se refiere, trabaje como una red virtual homogénea. Cuando se desea enviar datos a un computador remoto, se comunica este requerimiento al router o encaminador de la red origen. Este, gracias a la información que posee en tablas de encaminamiento y a la ejecución simultánea de varios protocolos de encaminamiento, transmite el requerimiento al encaminador de la red destino o al encaminador de la red del siguiente salto y así, sucesivamente, hasta que la información llegue a su destino.

El protocolo TCP es un protocolo dúplex porque actúa simultáneamente, como transmisor y receptor. El mecanismo para transmitir información se basa precisamente en esta interacción. El transmisor numera cada segmento que conforma el mensaje global y establece un tiempo límite para que el receptor confirme el arribo del paquete, caso contrario lo retransmite. El receptor debe al recibir los paquetes enviar el ACK (mensaje que indica un exitoso recibimiento de paquetes), ordenar y descartar los paquetes repetidos.

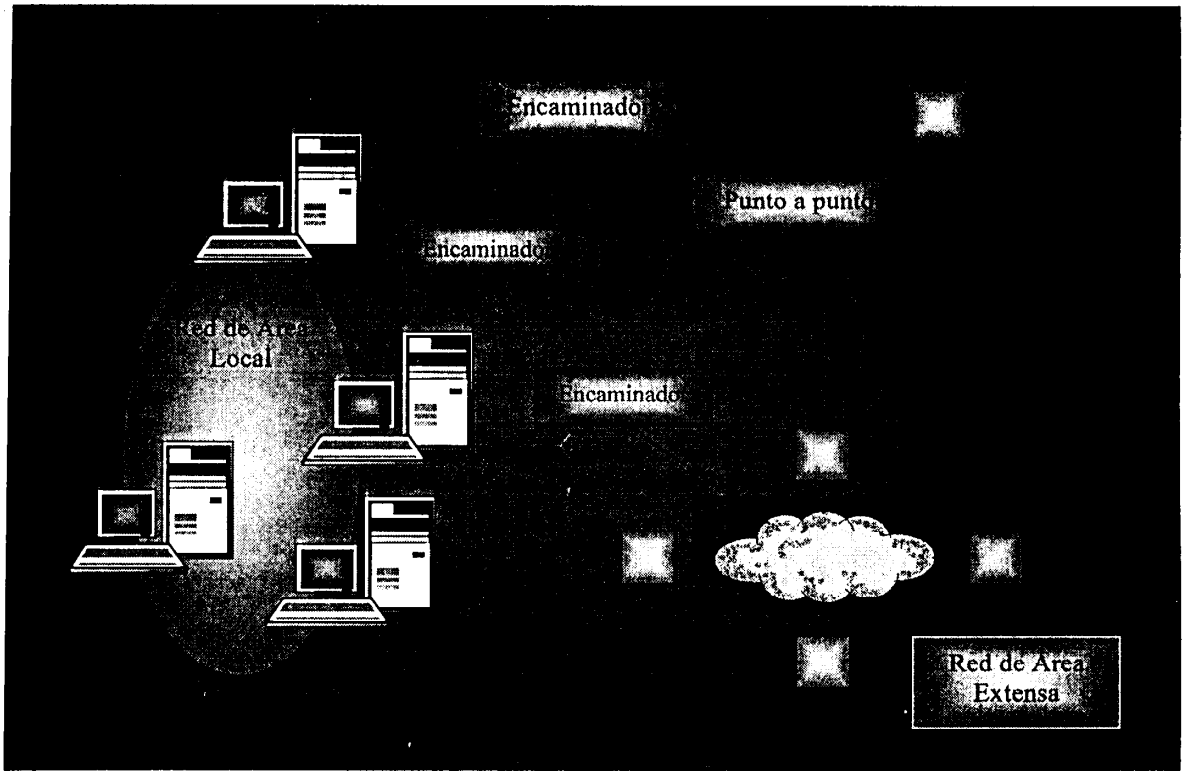


Figura 3.5. Interconexión de redes con encaminadores.

El protocolo **UDP** no garantiza la entrega de paquetes, sólo los transmite, por lo que la responsabilidad de confirmar la entrega recae en los usuarios y programas de aplicación.

TCP/IP utiliza mecanismos que permiten salvaguardar la información que transmite como la de autenticación de los usuarios, integridad de la información enviada por una internet y su confidencialidad.

A breves rasgos así se explica el funcionamiento del TCP/IP para transmitir información a través de una interred. Quedan aspectos sueltos como el que TCP/IP identifica a cada componente de la red, entre otros. A esto nos vamos a referir a continuación.

3.2.5. Identificadores universales.

Un sistema de comunicaciones proporciona *Servicio* Universa/ cuando permite que cualquier computador anfitrión establezca comunicación con otro computador, cualquiera que sea. Esto exige un método universal que identifique cada computador conectado a dicho sistema de comunicación.

Los identificadores universales se clasifican en nombres, direcciones y rutas. Los nombres distinguen un objeto en particular; las direcciones, la ubicación de dicho objeto; y, las rutas señalan las distintas formas que existen para llegar al objeto en cuestión.

Los nombres, direcciones y rutas son representaciones de bajo nivel de identificadores de anfitrión. Las personas, en general, prefieren dar a las diferentes máquinas nombres, pero el software trabaja más eficientemente con los identificadores llamados direcciones: números binarios que corresponden a los nombres. A cada nombre distinto corresponde una dirección diferente y viceversa.

El organismo encargado de asegurar que los nombres sean únicos es el Servicio de registro de InterNIC (InterNIC Registration Service) fundado en 1993.

3.2.5.1. Asignación de nombres y su estructura jerárquica.

Los nombres están conformados por etiquetas separadas por puntos y, toda agrupación de nombres, con la misma terminación, se conoce como dominio. En el gráfico 3.6. se observa la clasificación primaria de dominios en el ámbito mundial.

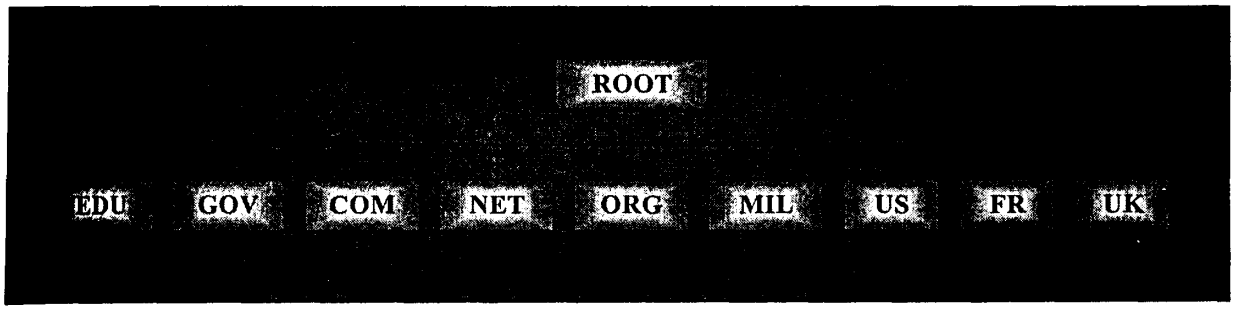


Figura 3.6. Árbol mundial de nombres.

3.252. Direcciones IP.

Son utilizadas por el protocolo IP para encaminar la información desde su origen a su destino, ocultar los detalles de las redes físicas y hacer que la red de redes parezca un solo ente uniforme, conocido como red virtual. Todo direccionamiento dentro de una interred (red virtual) es fundamental para proporcionar la apariencia de red transparente, homogénea y única, lo que se consigue por medio de un esquema de direccionamiento independiente de la dirección física.

Las direcciones de protocolo se utilizan como destinos de una interred virtual en la misma forma que las direcciones de hardware se utilizan como destino de las redes físicas. Por ello el protocolo IP define un esquema de direccionamiento abstracto en el que cada host es identificado por medio de una dirección única e írrepetible dada por el software.

Cada computadora en red tiene asignado un nombre asociado a una dirección IP específica. Así es posible efectuar la conversión de los nombres a su correspondiente dirección IP en el momento de una búsqueda, al consultar su base de datos.

El protocolo que define el direccionamiento es el protocolo de *Internet*.

De acuerdo con la norma IP, una dirección IP es un número binario que consta de 32 bits (cuatro octetos) que codifica la identificación de la red en particular a la cual se conecta el anfitrión (computador), así como también, la identificación de un anfitrión (computador) único a dicha red.

Tiene dos formas de representación: binaria y la decimal. En el equivalente decimal de la dirección IP, cada octeto pasa de su forma binaria a su correspondiente forma decimal y se separa mediante puntos por cuestiones de facilidad. Una dirección IP se escribe en su forma binaria o, se utiliza la notación punto que constituye su forma decimal; por ejemplo:

10000010100001000001001100011111 (Forma binaria)

130.132.19.31 (Forma decimal)

3.2.5.2.1. Formato.

Una dirección IP de 32 bits posee una jerarquía de dos niveles. Esta proporciona eficiencia y efectividad al proceso de enrutamiento de la información desde su origen hacia su destino. Para ello, cada dirección está dividida en dos partes: un prefijo (netid) y un sufijo (hostid). El prefijo identifica la red física a la cual está conectado el anfitrión (computador). El sufijo identifica un anfitrión (computador) particular de esa red. El prefijo es el número o dirección de red y, el sufijo es el número de servidor o dirección local.

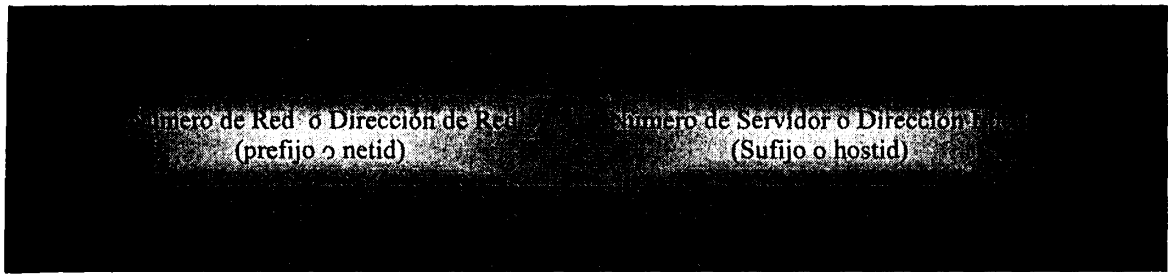


Figura 3.7. Formato de una dirección IP.

A cada red física se le asigna un prefijo único y a cada servidor, dentro de una misma red física, se le asigna un sufijo único. Si computadoras de diferentes redes tienen sufijos iguales nunca tendrán prefijos idénticos por pertenecer a redes distintas.

La jerarquía de las direcciones IP garantiza dos importantes propiedades para el enrutamiento de la información:

- Cada computadora tiene asignada una dirección única e irrepetible.
- Pese a que la asignación del número de red se coordina a nivel mundial, la del número del servidor puede hacerse a nivel local.

3.2.5.2.2. Clases.

Existen tres tipos primarios de direcciones IP, cuyo formato depende, exclusivamente, del tamaño de la red que se quiera conectar al Internet. Éstas son:

- Direcciones IP clase A.
- Direcciones IP clase B.
- Direcciones IP clase C.

La diferencia básica entre estos tipos de direcciones está dada por el número de bits asignados al prefijo (netid) y sufijo (hostid) de la red, lo que garantiza, dentro de una red virtual, que existan direcciones únicas. Nótese que el aumento de bits para el prefijo disminuye su número para el sufijo y viceversa. Así es posible direccionar un gran número de redes físicas de una interred limitando sus tamaños o a la inversa, es factible direccionar un menor número de redes físicas de un gran tamaño.

En la Figura **3.8** podemos apreciar el formato que corresponde a cada una de las tres clases de direcciones.

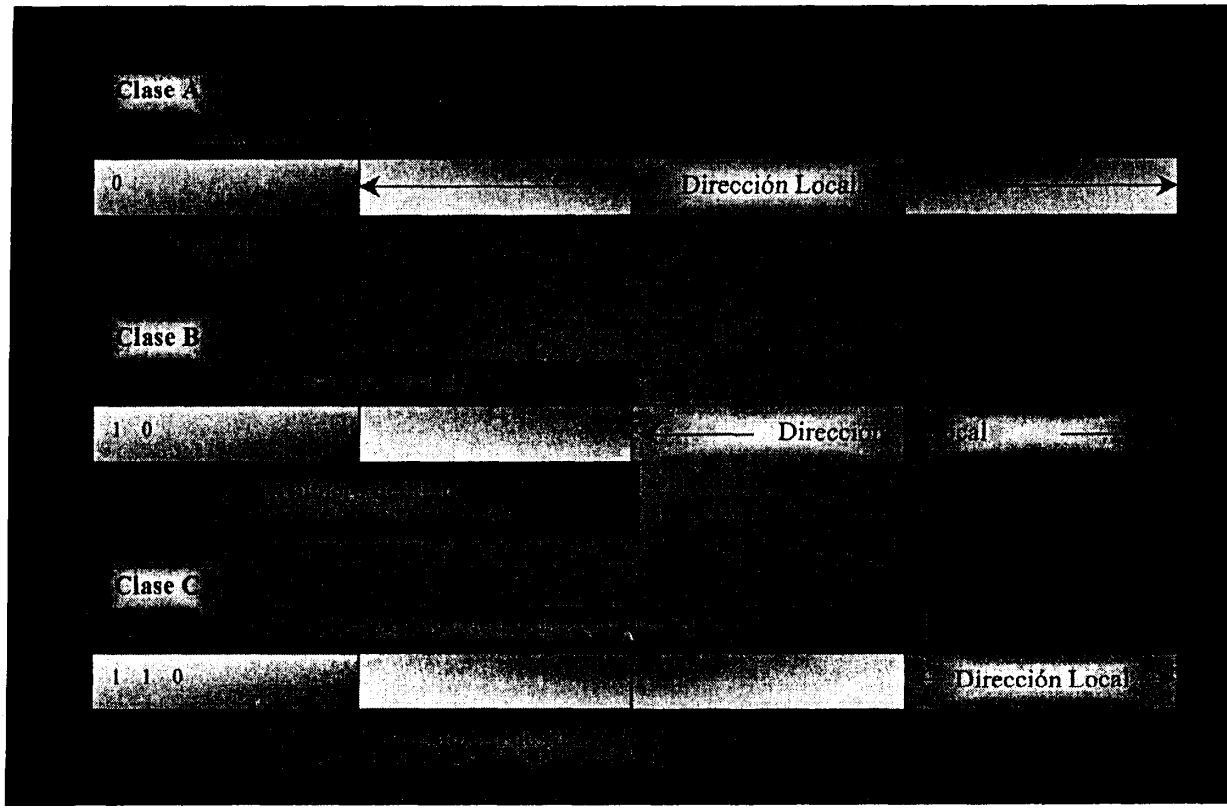


Figura 3.8. Clases tradicionales de direcciones IP.

La clase A es aconsejable si se tiene un gran número de servidores conectados a una red. Si se divide la dirección IP en cuatro campos, de ocho bits cada uno (octetos), al primer campo (primeros 8 bits) corresponde el número o dirección de red. Los otros tres campos corresponden al número del servidor (dirección local) que identifica al anfitrión.

La clase B se aplica a redes de tamaño medio. En este formato los dos primeros campos corresponden al número de red y los dos restantes, pertenecen al número del servidor.

La clase C se aconseja si la red es de tamaño pequeño. Aquí los tres primeros campos conforman el número de red y, el último, conforma el número del servidor.

Es sumamente sencillo percibir de qué tipo de dirección IP se trata gracias a que cada uno de estos tipos comienza con un número en particular. En las direcciones clase A, el bit de orden más alto siempre es cero. Los otros siete bits que completan el primer octeto, asignan números al identificador de la red que van desde 0 hasta 127 ($2^7 - 1 = 127$). Los restantes 24 bits, tres octetos, representan el identificador del servidor, por ello existen 126 redes y 16'777.214 servidores por red.

En las direcciones clase B los dos bits más significativos son el binario 10 por eso el número identificador de la red oscila entre 128 hasta 191 lo que permite 16.384 redes y 65.534 servidores por red.

En las direcciones clase C los tres primeros bits son el binario1 10 por lo cual el número identificador de red está entre 192 hasta 223, lo que permite 2'097.152 redes y 254 servidores por red.

Nótese que el valor máximo, que constituye el límite entre una clase y otra, depende del número máximo de bits asignado al número de red.

Tabla 3.1. Resumen de las direcciones IP tradicionales

[illegible]	1 – 126 *	W	X.Y.Z	126	16'777.21[illegible]
[illegible] B	128 – 191	W.X	Y.Z	16.38[illegible]	65.5[illegible]
[illegible] C	192 – 223	W.X.Y	Z	2'097.15[illegible]	[illegible]

* La dirección clase A 127.X.Y.Z está reservada a las pruebas de loopback y a la comunicación interprocesos en la computadora local.

Tabla 3.2. Rangos de las clases de los identificadores de red

Clase A	1.0.0.0	126.0.0.0
Clase B	128.0.0.0	191.255.0.0
Clase C	192.0.0.0	223.255.255.0

Tabla 3.3. Rangos de las clases de los identificadores de servidor

Clase A	1.0.0.0	126.0.0.0
Clase B	128.0.0.0	191.255.0.0
Clase C	192.0.0.0	223.255.255.0

Existen dos tipos más de direcciones IP. Éstas son:

- Direcciones IP tipo D y,
- Direcciones IP tipo E.

Las direcciones IP clase D se emplean en transmisiones simultáneas a todas las computadoras de una red o de algunos sistemas a la vez. Este concepto se visualiza mejor en la Figura 3.9 y se conoce como transmisiones multicast o de multienvío.

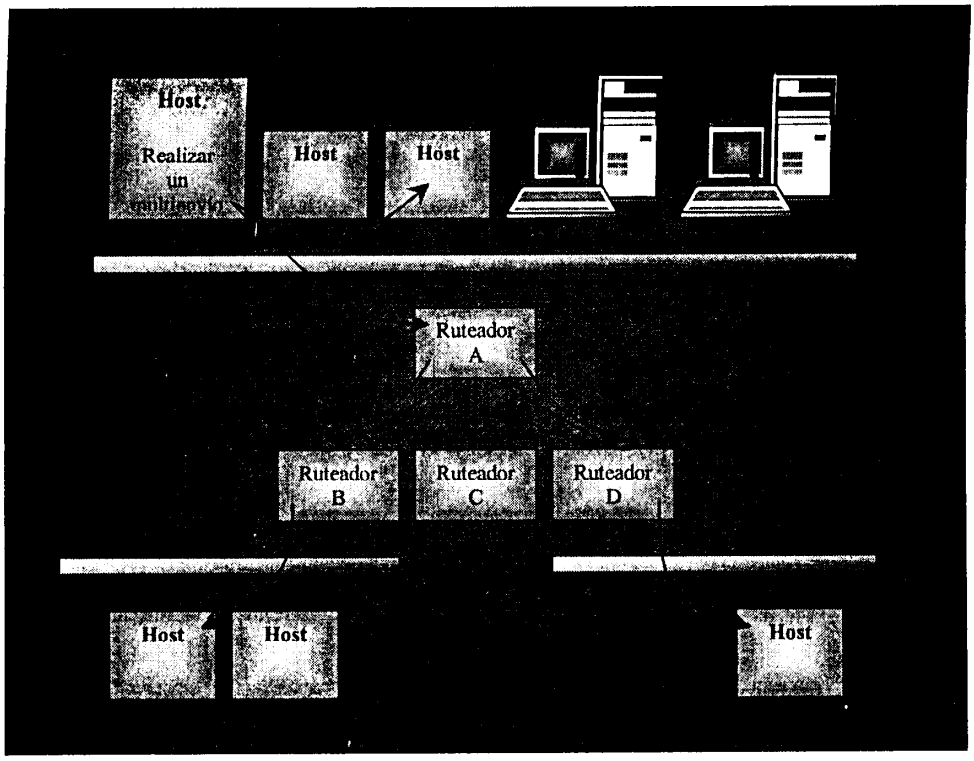


Figura 3.9. Propagación de los datagramas multienvío.

El concepto de *grupo de multienvío* está constituido por un conjunto de sistemas que tienen asignada una dirección de multienvío sin perder su identidad única.

El formato de una dirección IP clase D se ve en la Figura 3.10. Es posible reconocerla porque los cuatro primeros bits son el binario ll 10 y su identificador de red oscila entre 224 y 239.

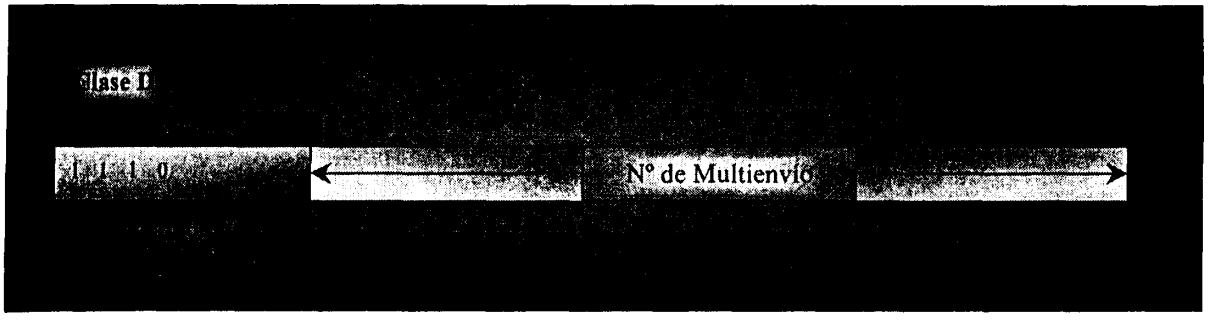


Figura 3.10. Formato de las direcciones tipo D para datagramas IP multienvío.

Las direcciones IP clase E están reservadas para aplicaciones futuras y empiezan con el número binario 1111.

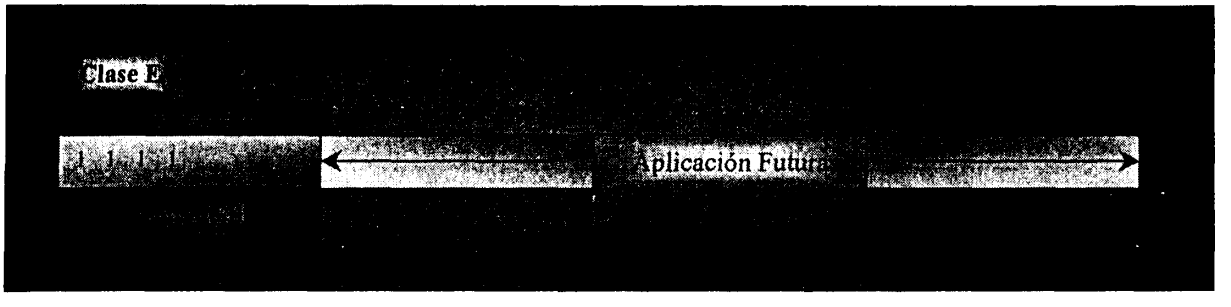


Figura 3.11. Formato de una dirección IP tipo E.

3.2.5.2.3. Direcciones especiales reservadas.

Las direcciones especiales reservadas realizan tareas específicas y denotan ciertos grupos de redes, por lo que no se asignan a ningún servidor.

Así la dirección de red no es propiamente la dirección destino de un paquete, sin embargo identifica una red al resaltar el prefijo que le corresponde, para ello el protocolo IP reserva un formato en el cual el número del servidor (sufijo) es cero. La dirección 128.211 .O.O, por ejemplo, se refiere a la red que tiene asignado el prefijo clase B 128.211 y la dirección 108.0.0.0 denota una red identificada con el prefijo clase A 108.

La dirección de difusión dirigida es útil cuando se requiere enviar un paquete de información a todos los hosts de algunas redes físicas que conforman la interred. En este caso el formato de la dirección contiene, en el prefijo, la dirección de la red física a la cual se envía la información y, en el sufijo, todos los bits deben ser uno para indicar que la entrega se realizará a todos los servidores de dichas redes.

La dirección de difusión limitada se utiliza para enviar una misma información a todos los servidores de una red LAN. Su formato infiere que tanto el prefijo como el sufijo contengan bits unos.

La dirección de esta computadora se asigna por el protocolo IP cada vez que se envía un paquete luego de reiniciar una máquina. Es imposible obtener una

dirección de fuente correcta luego del arranque de un computador y todos los paquetes transmitidos requieren de una dirección fuente y la dirección destino. Se identifica esta clase de dirección por su formato en el cual todos los bits, que conforman el prefijo y el sufijo, son bits ceros.

Tabla 3.4. Resumen de las formas especiales de direcciones IP.

Ceros	Ceros	Esta computadora	Se usa en el arranque
Red	Ceros	Red	Identifica una red
Red	Unos	Difusión dirigida	Difusión en una red especificada
Unos	Unos	Difusión limitada	Difusión en una red de área local
127	Cualquiera	Retrociclo	Pruebas

3.2.5.2.4. Subredes y máscaras de subredes.

Las direcciones IP se diseñaron para acomodar tres tipos diferentes de redes de acuerdo con su tamaño reflejado en el número de redes y servidores por red que necesiten. En la práctica resultó poco práctico el uso de las direcciones clase A y clase B debido a lo extenso de su dominio de transmisión. Por esta razón, en un intento de aprovechar en mejor forma los bits que conforman el identificador del servidor o dirección local, reduciendo el dominio de transmisión, se crearon las subredes.

Las subredes son redes de menor dimensión limitadas por un enrutador que tiene asignado un identificador de subred único como muestra la Figura 3.12.

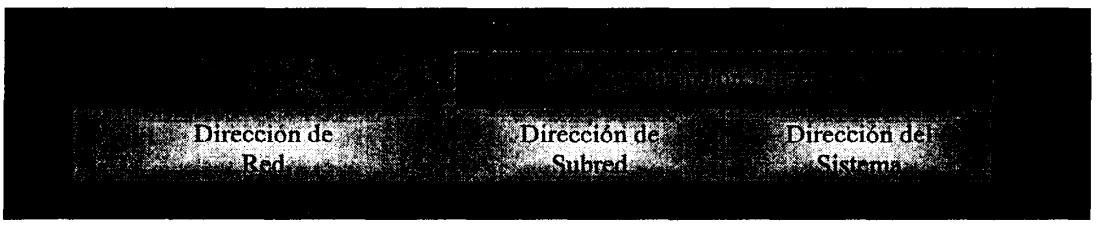


Figura 3.12. Subdivisión de las direcciones locales.

Se necesita aquí un nuevo elemento, conocido como máscara de subred, que permite al ruteador discernir y extraer correctamente los identificadores de red de una dirección IP sin irnportar si estos corresponden a clases de direcciones o a una subred.

El RFC 950 se refiere a la máscara de subred como máscara de dirección y la define con un número de 32 bits en el cual son puestos en 1 todos aquellos que pertenecen a la dirección de red (identificador de red) y en 0, los restantes que corresponden a la dirección local (identificador de servidor).

Así podemos establecer que todos los nodos TCPIIP, servidores y ruteadores, necesitan una máscara de subred que permita a cualquier host establecer el número de bits de la dirección IP que corresponden al identificador de la red y, por diferencia, al identificador del servidor.

Al igual que las direcciones las máscaras de subred, suelen ser expresarse por la notación decimal punteada. Una máscara de subred no es una dirección IP, aunque está basada en éstas, tal como lo expresa la tabla 3.5.

Tabla 3.5. Máscaras de subred por defecto en notación decimal punteada

[illegible]	11111111 00000000 00000000 00000000	255.0.0.0
[illegible]	11111111 11111111 00000000 00000000	255.255.0.0
[illegible]	11111111 11111111 11111111 00000000	255.255.255.0

Las máscaras que corresponden a las subredes o a las superredes son máscaras personalizadas. Por ejemplo el 138.96.58.0, es un identificador de red de clase B para subredes. La máscara de subred correspondiente contendría 24 bits y se expresaría de la siguiente manera 255.255.255.0. Aquí podemos apreciar, claramente, que de los 16 bits del identificador de servidor los 8 primeros son utilizados para definir la subred.

La dirección IP, para el ejemplo anterior con su respectiva máscara de subred en notación simplificada, sería:

138.96.58.0/24

Estas máscaras se ayudan del prefijo de red de la máscara de subred, una manera abreviada de la misma se denota de la siguiente forma: /(No de bits que

ene el identificador de red). En la tabla 3.6 mostramos las máscaras de subred
on sus respectivos prefijos.

Tabla 3.6. Máscaras de subred por defecto utilizando la notación de prefijo de red para misma.

Clase A	11111111 00000000 00000000 00000000	/8
Clase B	11111111 11111111 00000000 00000000	/16
Clase C	11111111 11111111 11111111 00000000	/24

a máscara de subred es útil para extraer el identificador de red de una rección IP cualquiera. Para efectuar a cabo este proceso el protocolo IP aliza una operación lógica AND entre la dirección IP y su respectiva máscara e subred. Recordemos los fundamentos de una operación lógica AND (Tabla 7).

Tabla 3.7. Operación AND.

		AND
0	0	0
0	1	0
1	0	0
1	1	1

La tabla anterior permite analizar la operación AND entre un 1 y ϕ, que puede tener valor de verdad 0 o 1. El resultado depende de dicho valor de verdad: si ϕ es 1, el resultado es 1 y si ϕ es 0, el resultado es 0. Por lo que, la operación lógica AND entre la máscara de subred y su dirección IP, dará por resultado el identificador de red (dirección de red). Analice el siguiente ejemplo. Note que al traducir el identificador de red a su forma decimal punteada tendríamos 129.56.176.0.

10000001	00111000	101 ll 101	00101001	Dirección IP
11111111	11111111	11110000	00000000	Máscara de subred
10000001	00111000	10110000	00000000	Identificador de red

3.253. Liga de direcciones de protocolo.

El esquema de direccionamiento IP asigna direcciones de protocolo de alto nivel a los hosts y enrutadores. Ello porque los elementos del hardware que poseen direcciones físicas o de hardware no entienden la relación existente entre una dirección virtual y una física. El hecho es que, antes de enviar cualquier paquete a través de la interred, se debe resolver la dirección física a partir de la dirección virtual. De ello se encarga el protocolo ARP (Address Resolution Protocol).

Las direcciones de protocolo son abstracciones que ofrece el software para que el conjunto de redes de conformación heterogénea no lo parezca.

El hardware de red no puede identificar un destino a partir de direcciones de protocolo, por lo que necesita conocer la dirección de hardware antes de enviar los paquetes que contienen la información. Por esta razón existen mecanismos que ejecutan la respectiva conversión.

Este proceso que traduce la dirección de protocolo (virtual), de una computadora a su dirección de hardware (física) equivalente, se llama resolución de dirección y tiene una restricción. Una computadora puede resolver la dirección física de otra si ambas se encuentran conectadas a la misma red. Nunca podrá resolver direcciones de computadoras remotas.

Considere la Figura 3.13. En ella, los servidores A y B pertenecen a una misma red y, de forma similar, los servidores C y D y, los E y F. Si el servidor A envía información al B, A resuelve la dirección física de B antes de transmitirla. Si se envía información desde el servidor A al F, A determina, primero, que F no pertenece a dicha red y, segundo, que el próximo salto corresponde al enrutador R_1 por lo que resuelve su dirección antes de enviar los datos. Este proceso se repite en la siguiente red y, una vez ya en el enrutador R_2, se resuelve la dirección física de F. Así es como la información viaja a través de la interred.

La condición para que una computadora resuelva la dirección física de otra es que pertenezcan a la misma red.

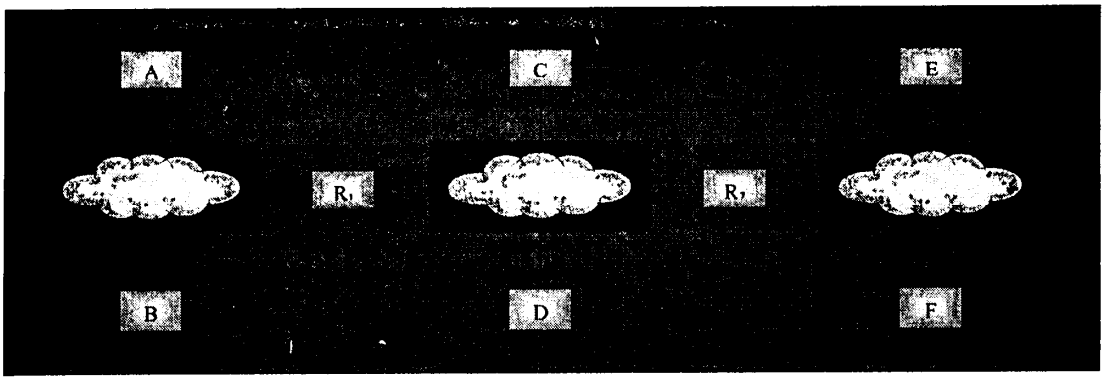


Figura 3.13. Interred sencilla en la que los ruteadores R_1 y R_2 conectan tres redes.

3.2.5.3.1. Técnicas de resolución de direcciones.

El uso de algoritmos para resolver direcciones está ligado al tipo de direccionamiento y al hardware que emplea. Esto significa, por ejemplo, que es necesario que el computador maneje varios de estos módulos de resolución si está conectado a varias redes, como es el caso de los ruteadores.

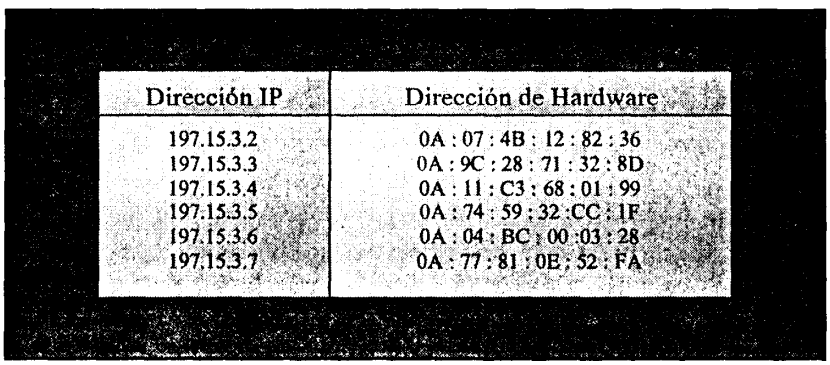
Básicamente, los algoritmos de resolución de direcciones se dividen en tres categorías, que son:

- ***Búsqueda en tabla.*** **En** ella las ligas son salvadas en la memoria de una tabla a la cual accesa el software para resolver una dirección.

- Cálculo de ***forma cerrada.*** En donde a partir de operaciones lógicas y de aritmética básica, se convierte la dirección de protocolo en su equivalente física.

- Intercambio de *mensajes.* Se transmiten mensajes solicitando la información requerida.

La Figura 3.14 contempla el ejemplo de una tabla de liga de direcciones. Note que todas las direcciones IP tienen el mismo prefijo ya que sólo se encuentran las ligas de las computadoras de una misma red.



Dirección IP	Dirección de Hardware
197.15.3.2	0A : 07 : 4B : 12 : 82 : 36
197.15.3.3	0A : 9C : 28 : 71 : 32 : 8D
197.15.3.4	0A : 11 : C3 : 68 : 01 : 99
197.15.3.5	0A : 74 : 59 : 32 :CC : 1F
197.15.3.6	0A : 04 : BC : 00 :03 : 28
197.15.3.7	0A : 77 : 81 : 0E : 52 : FA

Figura 3.14. Ejemplo de una tabla de liga de direcciones.

Este método tiene ventajas y son:

- La generalidad. Las direcciones de protocolo pueden correlacionarse con direcciones de hardware arbitrarias.

- Este algoritmo es sencillo y fácil de programar.

2.5.3.2. Protocolo ARP.

protocolo TCP/IP utiliza cualquiera de los tres algoritmos de resolución de ección explicados en base al tipo de direccionamiento del hardware. Por emplo, el algoritmo de búsqueda en tabla se emplea para resolver direcciones en una WAN; el de cálculo de forma cerrada lo usan las redes configurables el algoritmo de intercambio de mensajes se aconseja cuando el hardware de a LAN tiene direccionamiento estático.

protocolo ARP (Address Resolution Protocol) resuelve las direcciones y su mato define dos clases de mensajes: solicitudes y respuestas. Un mensaje licitud tiene una dirección IP y demanda la dirección de hardware rrespondiente. Un mensaje respuesta contiene la dirección IP, enviada en la licitud, y la dirección de hardware.

2.5.3.3 Mensajes ARP.

norma ARP establece que los mensajes de solicitud ARP deben colocarse en área de datos de un cuadro de hardware y difundirse a todas las nputadoras de la red. Este proceso se llama encapsulamiento y se aprecia la Figura 3.15. Así cada computadora examina si la dirección IP de la icitud coincide con la suya y solo en el caso de coincidir, contesta enviando el nsaje respuesta, de lo contrario, descarta la solicitud inicial.

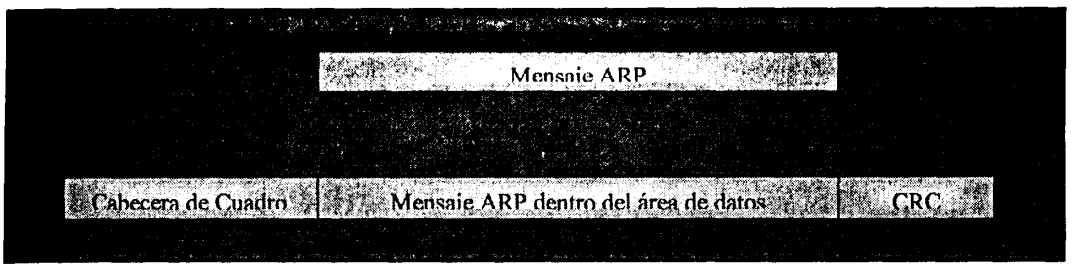


Figura 3.15. Mensaje ARP encapsulado en el área de datos de un cuadro Ethernet para que el hardware de red no interprete ni modifique su contenido.

El mensaje respuesta se coloca en otro cuadro de hardware y envía únicamente a la computadora que generó la solicitud. La Figura 3.16 presenta cómo se lleva a cabo un intercambio ARP entre computadoras de una Ethernet.

El formato de los mensajes ARP se adapta a diversas tecnologías de red porque no dispone de campos fijos para direcciones de hardware y de protocolo sino que permite seleccionar su tamaño, por lo que incluyen un campo para definir la longitud de las direcciones físicas y de software. Esto hace, en teoría, que el protocolo ARP pueda emplearse en ligar direcciones de hardware arbitrarias con direcciones de protocolo igualmente arbitrarias. Se trata de un protocolo extremadamente flexible.

En la práctica, el protocolo ARP es usado para ligar direcciones IP de 32 bits (4 octetos) con direcciones Ethernet de 48 bits (6 octetos). La Figura 3.17 ilustra el formato específico del mensaje ARP.

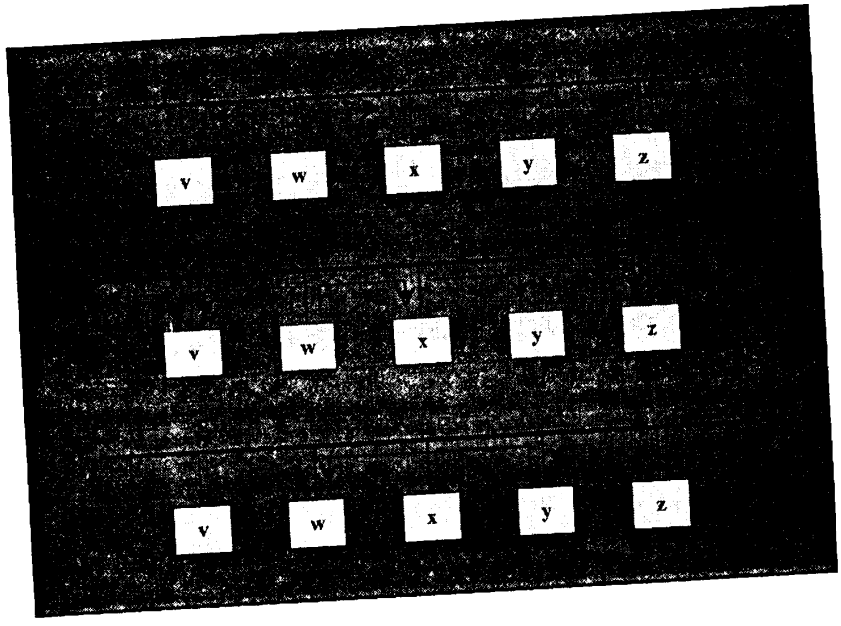


Figura 3.16. Intercambio de mensajes ARP. (a) La computadora W difunde una solicitud ARP con la dirección IP de la computadora Y. (b) Todas las computadoras reciben dicha solicitud. (c) La computadora Y transmite la respuesta directamente a W.

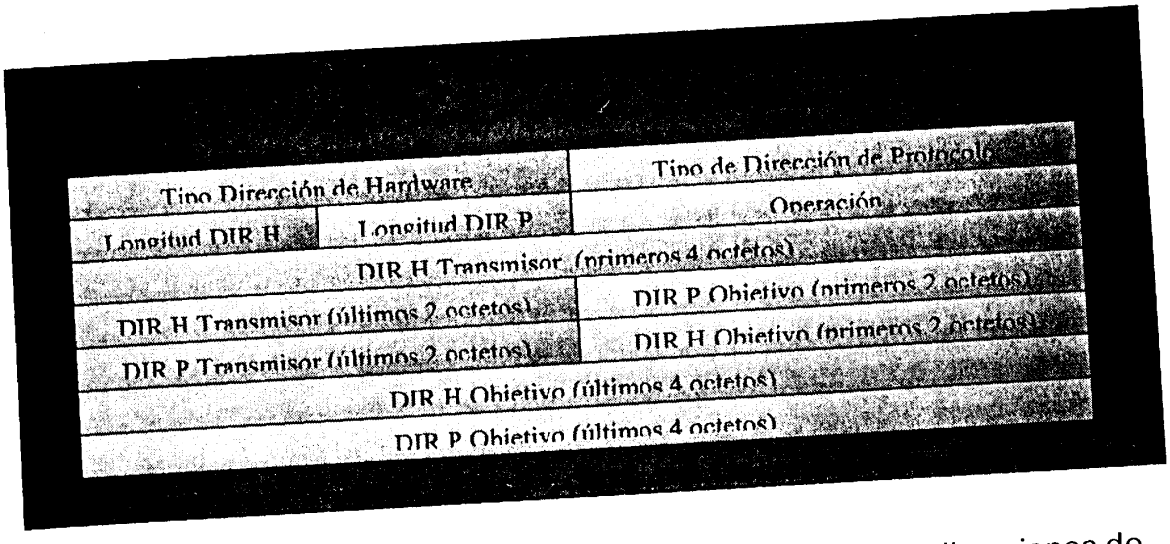


Figura 3.17. Formato de un mensaje ARP usado para ligar direcciones de protocolo IP con direcciones de hardware Ethernet.

Note que este mensaje tiene 224 bits. Los primeros dos campos de 16 bits especifican el tipo de dirección de hardware y de protocolo. En los campos Longitud DIR H y Longitud DIR P se definen la cantidad de octetos de las direcciones de hardware y protocolo respectivamente. El campo Operación establece si el mensaje es una solicitud (número 1) o una respuesta (número 2) y, por último, los campos DIR H Transmisor, DIR P Transmisor, DIR H Objetivo y DIR P Objetivo contienen las direcciones de hardware y de protocolo del computador que hace la solicitud (transmisor) y del que responde dicho requerimiento (objetivo).

Para identificar los cuadros ARP se utiliza un campo que se encuentra en su cabecera y que define el tipo de cuadro.

El protocolo ARP posee mecanismos para almacenar ligas de direcciones en forma temporal en una memoria pequeña llamada caché. Así se reduce el tráfico generado en la red al enviar dichas solicitudes, haciendo el proceso más eficiente. Antes de transmitir una solicitud ARP, efectúa una búsqueda de la liga en su memoria caché y sí no consta, difunde la solicitud.

Cuando un mensaje ARP arriba al receptor, primero se extrae la liga de dirección del transmisor a fin de actualizar los datos de la memoria caché, y, segundo, examina el campo de operación y determina si es solicitud o respuesta. Si es respuesta debió antes enviar una solicitud. Y si es una solicitud, debe comparar la dirección de protocolo objetivo con la suya y enviar

una respuesta si son iguales. Para hacerlo cambia el campo de operación del mensaje, invierte las ligas del transmisor y del objetivo y añade su dirección de hardware en el campo de dirección de hardware transmisor.

3.2.6. Transmisión de los datos por la interred.

3.2.6.1. Encapsulamiento.

Técnica que permite que la información viaje a través de redes que no entienden su formato, base de la compatibilidad de los sistemas existentes y de importancia trascendental.

Antes de transmitir los datos por una red, se encapsulan. El datagrama IP se coloca en el área de datos de un cuadro de hardware al que se añade una nueva cabecera que posee como dirección destino la dirección física del siguiente salto, previamente calculada por el hardware transmisor.

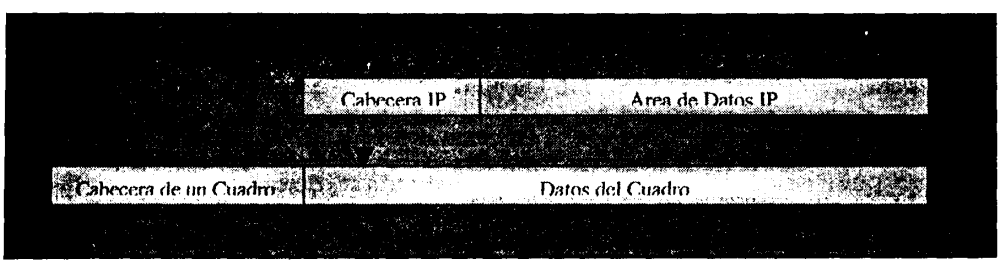


Figura 3.18. Datagrama IP encapsulado en un cuadro de hardware dentro del área de datos.

La cabecera asigna un valor exclusivo al campo del tipo de cuadro, que se acuerda entre transmisor y receptor previamente, para que el receptor del paquete pueda identificar el tipo de datos que contiene el cuadro.

La técnica del encapsulamiento se aplica a una transmisión a la vez. Cuando el cuadro llega a la dirección del siguiente salto el receptor remueve el paquete IP del área de datos del cuadro y descarta su cabecera; lo almacena en memoria sin la cabecera adicional y, si aún no llega a su destino, lo enruta de la forma más conveniente, volviendo a traducir la dirección IP del siguiente salto en la dirección física y creando así una nueva cabecera.

Los formatos de los cuadros y los tamaños de las cabeceras pueden variar de acuerdo con la tecnología de hardware que use la red. Así, si la red 1 es una red Ethernet tendremos como cabecera del cuadro 1 una cabecera Ethernet. Y en forma similar, si la red 2 es una red anillo FDDI, la cabecera del cuadro 2 es una cabecera FDDI.

En la Figura 3.19 vemos que durante el viaje del datagrama IP a su destino final, los hosts y los enrutadores transmisores añaden al paquete IP una cabecera acorde al tipo de red, los receptores guardan en memoria el datagrama sin la cabecera adicional y, si es necesario agregan otra cabecera, hasta que la información arribe a su destino. El descarte de cabeceras cada vez que llegan los paquetes su destino, hace más eficiente el uso del ancho de banda por transmitir más información que caracteres de control.

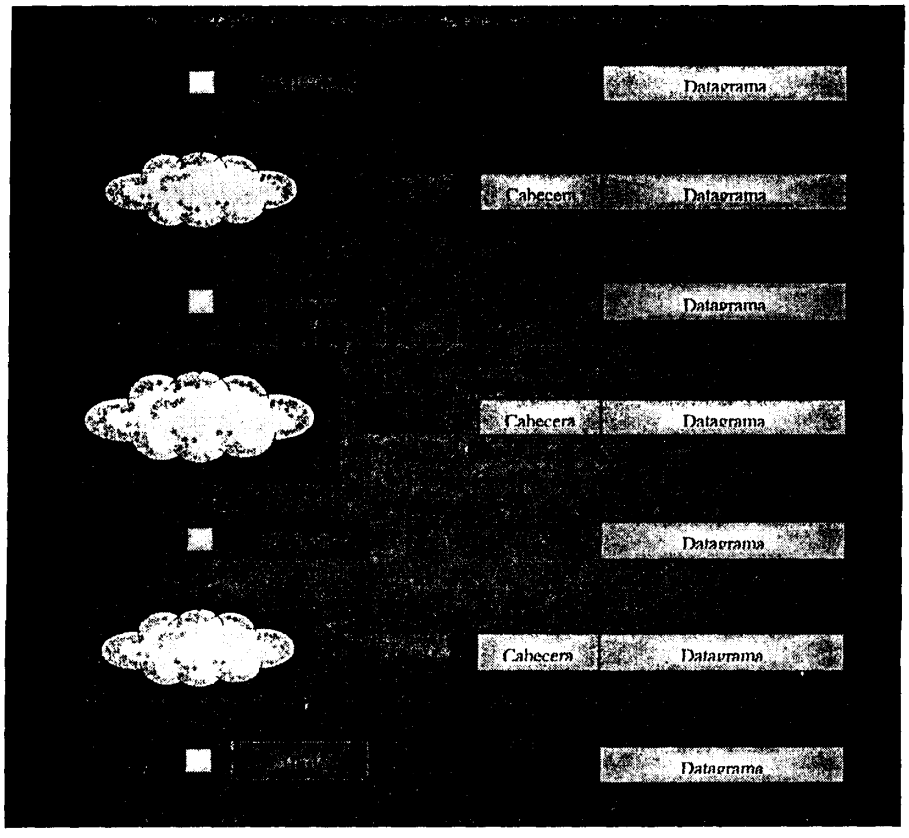


Figura 3.19. Datagrama IP según como aparece en cada paso en su viaje por una interred. El datagrama se encapsula en un cuadro adecuado a la red por la que viaja.

Las tecnologías de hardware especifican un tamaño máximo conocido como la *unidad máxima de transmisión* MTU (Maximun Transmission Unit). Para que los datagramas puedan ser encapsulados sus tamaños tienen que ser menores o iguales a la unidad máxima de transmisión de la red correspondiente.

En una red heterogénea pueden existir inconvenientes al transmitir datagramas IP por que el MTU puede variar de una red a otra.

Analicemos el caso que se muestra en la Figura 3.20.

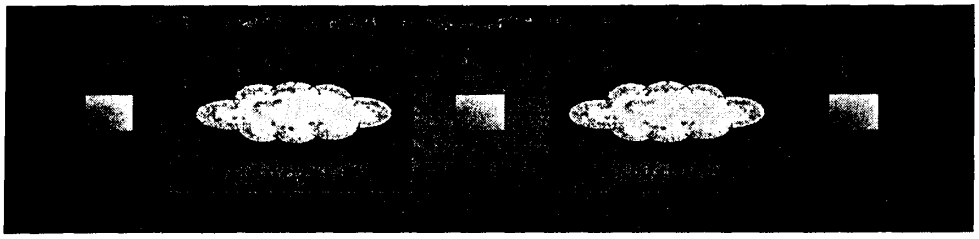


Figura 3.20. Enrutador que conecta redes con diferente MTU.

Se observa un enrutador que une a las redes 1 y 2, que poseen MTUs de 1500 y 1000 respectivamente. El host 1 se conecta a la red 1 y solo envía datagramas con 1500 o menos octetos. El host 2 conectado a la red 2, recibe datagramas de 1000 o menos octetos. Este es un ejemplo típico donde el ruteador puede recibir datagramas del host 1 sin poder enviarlos por la red 2 al host 2 debido a la restricción del MTU. Note que el caso inverso si se puede dar.

3.2.6.2. Fragmentación.

La solución al problema anterior se conoce como ***fragmentación.*** Consiste en dividir el datagrama en ***fragmentos,*** a fin de transmitirlos por la siguiente red. Sólo se utiliza esta técnica cuando el MTU de la siguiente red, por la que debe trasmitirse el mensaje, es menor que el MTU de la red por la cual se transmitió.

Cada fragmento, como se aprecia en la Figura 3.21, posee una copia de la cabecera original IP con una modificación y una parte de la información.

El ruteador modifica la nueva cabecera -en el campo de banderas- con el propósito de indicar que los datos contenidos son un fragmento de la información original.

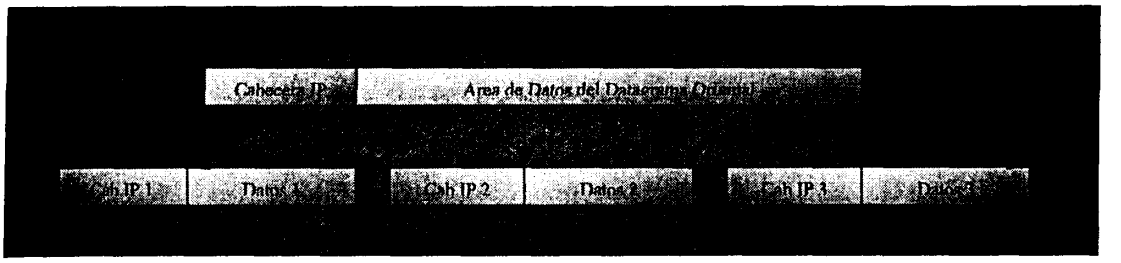


Figura 3.21. Datagrama IP dividido en tres fragmentos.

El ruteador determina el número de fragmentos y su longitud mediante cálculos que usan el MTU de la red y el tamaño de la cabecera del paquete IP.

326.3. Reensamble.

Proceso contrario a la fragmentación que no se lleva a cabo en los ruteadores. Es posible porque cada fragmento tiene por cabecera IP una copia de la cabecera original y la misma dirección destino del datagrama del que provienen. Además, el último fragmento dispone de un bit adicional en su cabecera para indicar al receptor final si llegaron en buen estado los otros fragmentos.

Existe el riesgo de que al transmitir información esta llegue a su destino en desorden o de que simplemente se pierda ya que IP no garantiza su entrega.

Para evitarlo el transmisor coloca un número de identificación, a cada uno de los datagramas salientes, en el campo de identificación. Si un datagrama es fragmentado el ruteador copia este número en cada fragmento. Para ordenar los fragmentos, el receptor utiliza este número de identificación y la dirección IP fuente del datagrama. Emplea también el campo de desplazamiento del fragmento porque indica al receptor el orden en el que van.

3.2.6.4. Problemas.

Para hacer frente a los problemas que origina la pérdida y retraso de fragmentos, IP posee un mecanismo que proporciona un tiempo determinado para el arribo de fragmentos a un Host final, luego de que el primero arribó. Los fragmentos que arriban dentro del plazo de tiempo estipulado se almacenan en la memoria del receptor para ser reensamblados sólo en el caso de que sus fragmentos lleguen en el tiempo previsto.

El mecanismo de IP no permite al host destino saber si el paquete que llega es un fragmento o el resultado de una fragmentación múltiple. Sólo reconstruye el datagrama original sin reensamblar subfragmentos primero. Ello ahorra tiempo y reduce la cantidad de información colocado en las cabeceras.

3.3. Frame Relay.

3.3.1. Introducción.

Frame Relay es un protocolo de conmutación de paquetes sencillo, rápido y eficiente. Está orientado al manejo de tráfico dentro de redes LAN a altas velocidades sin usar un gran ancho de banda. Esto se debe a que, en determinados instantes, las ráfagas de paquetes de datos de tráfico LAN sobrepasan hasta en un 20% la capacidad de utilización del medio físico.

Esta tecnología de multiplexación de datos para networking (multíplexed data networkíng technology), muy útil en ambientes WAN, provee conectividad entre equipos de usuarios y soporta transmisión de datos sobre circuitos orientados a conexión.

Los datos se dividen en tramas, de longitud variable, con información acerca del direccíonamiento. Las tramas se envían a la red Frame Relay que las entrega en una dirección específica usando una conexión virtual asignada.

La diferencia más significativa entre Frame Relay y X.25, otro protocolo, es que Frame Relay trabaja en el nivel 2 del modelo OSI mientras que la conmutación de paquetes de redes X.25 lo hace en el nivel 3.

X.25 consideró en su diseño los errores y la forma de superarlos durante la transmisión de datos por lo que cuenta con procedimientos que garantizan que

los datos sean recibidos por el receptor sin errores y en la secuencia correcta. Ello implica verificaciones y correcciones en nodos intermedios y por tanto, una disminución de la velocidad con la que se procesa la información.

Por su parte, Frame Relay se basa en que las redes WAN son, cada día, más fiables debido a que los dispositivos que utilizan son mayormente digitales y a que su medio de transmisión es la fibra óptica, tendencia puede apreciarse en la Figura 3.22.

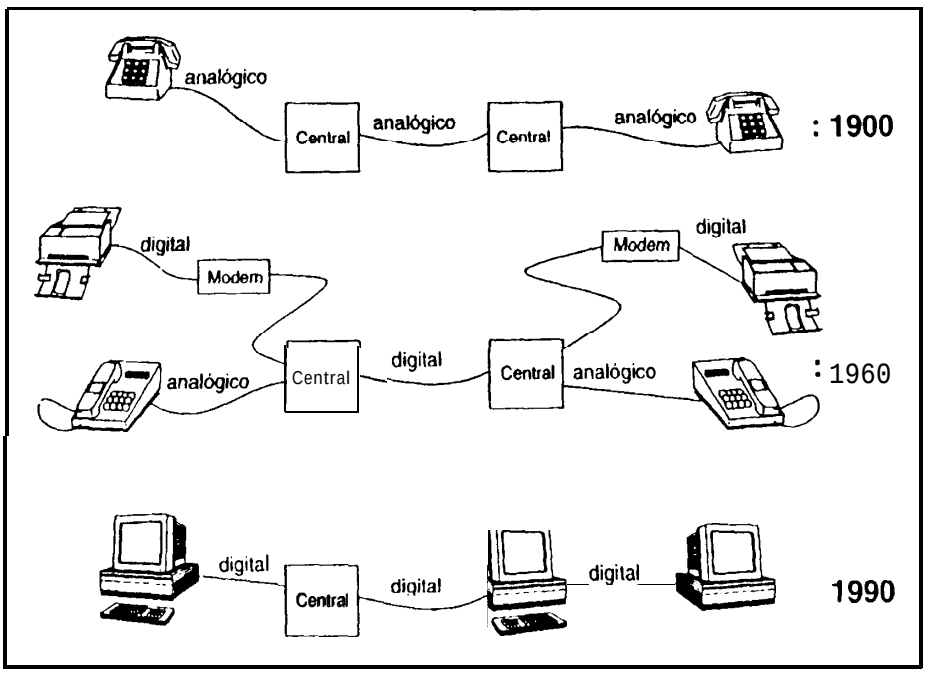


Figura 3.22. Digitalización de redes telefónicas que va desde los centros de conmutación y arterias principales, hasta el bucle de abonado.

Además, el desarrollo de sistemas finales y enlaces de transmisión determinan que:

- El coeficiente de la probabilidad de error pase de un bit erróneo cada 10^6 bits a menos de 1 cada 10^{10} bits.
- Y que las aplicaciones que usan las máquinas sean lo suficientemente inteligentes para detectar errores e implementar mecanismos que recuperen la información.

Ello determina que Frame Relay alcance un alto rendimiento de velocidad en la red. Los principios en que basa dicho incremento son:

- Al producirse un error en una trama ella se descarta sin intentar por recuperarla.
- Los sistemas finales se encargan de salvar cualquier situación de error.

Frame Relay ejecuta un subconjunto de funciones, propias del nivel dos, que son:

- Chequea la posibilidad de error y, de producirse, descarta la trama.
- Lee información de direccionamiento de la trama entrante y la ubica en la salida que le corresponde.

- Verifica si un nodo Frame Relay está congestionado. En tal caso, descarta tramas o modifica los bits de notificación de congestión.

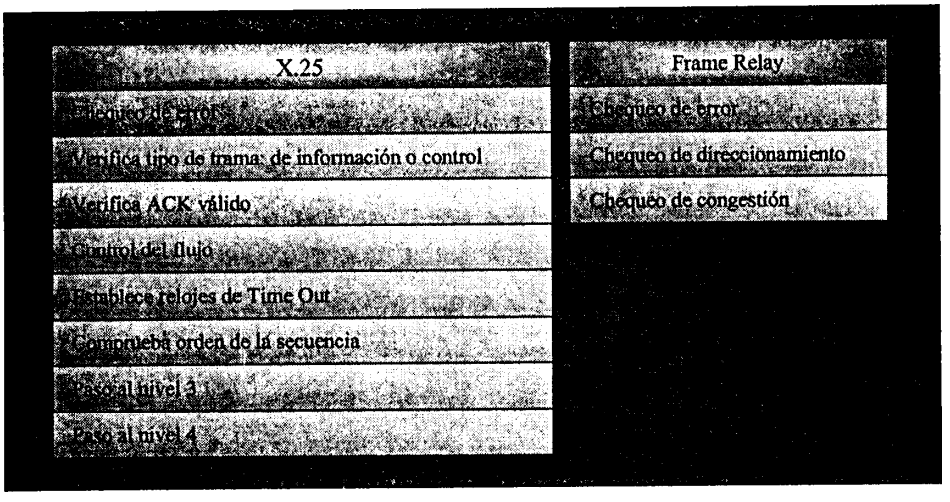


Figura 3.23. Procesamiento de información de X.25 Vs. Frame Relay.

3.3.2. Definición y características.

Frame Relay es una tecnología de conmutación rápida de tramas, basada en estándares internacionales, utilizable como protocolo de transporte y de acceso en redes públicas o privadas para proporcionar servicio de comunicaciones. Un protocolo simplificado de transmisión de tramas de datos que usa sólo los dos primeros niveles del modelo OSI. Permite la conexión a través de circuitos virtuales permanentes (PVC) y está -especialmente- adaptado a la transmisión de información en flujos esporádicos, a manera de ráfagas sobre una red digital. Las velocidades a las que está disponible fluctuan entre 64 Kbps y 2 Mbps.

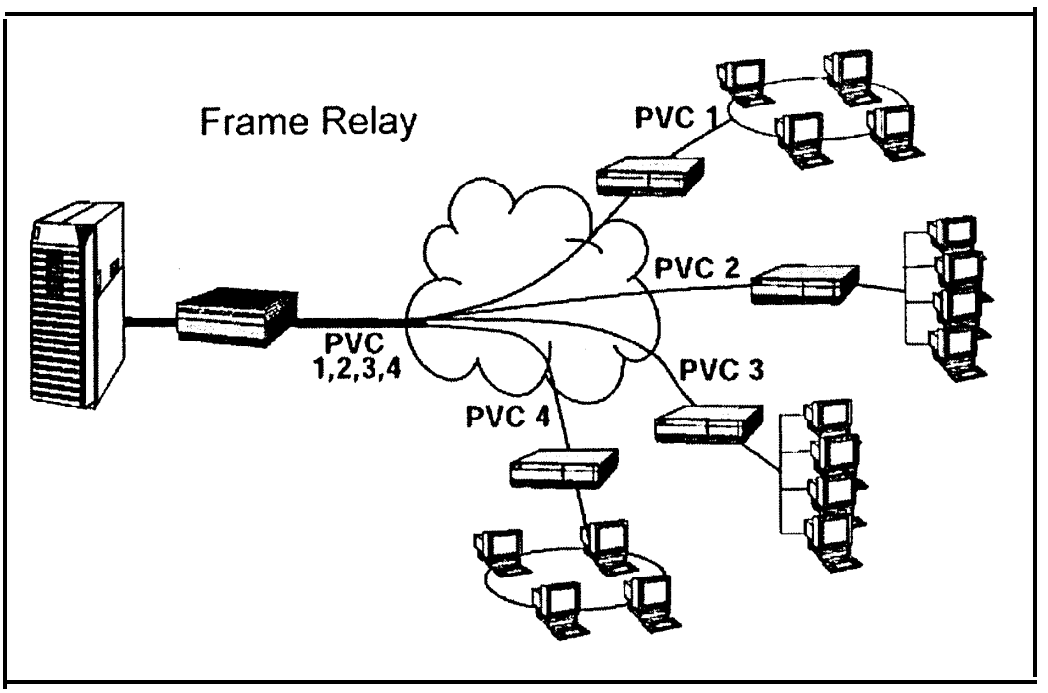


Figura 3.24. Frame Relay soporta circuitos virtuales permanentes (PVC).

Entre las principales características que posee este protocolo se encuentran:

- High throughput.
- Bajo retardo de propagación del paquete.
- Trabaja en capas 1 y 2 del modelo OSI.
- No proporciona servicio de corrección de errores.
- Puertos de alta velocidad (hasta $Mbps).
- Paquetes individuales multiplexados sobre el mismo medio físico.

- Uso racional y más efectivo del ancho de banda.
- Presencia internacional extensa.
- Conectividad independiente porque cada ubicación puede conectarse a las restantes ubicaciones de la red.
- Total disponibilidad por ser la red redundante, y permitir el redireccionamiento del tráfico sorteando así cualquier dificultad.

3.3.3. Aplicaciones.

Frame Relay facilita el uso común y la actualización de la información en tiempo real dentro del ámbito empresarial. Posee numerosas aplicaciones como las siguientes:

- Correo electrónico.
- Transferencia de ficheros.
- Transferencia de imágenes.
- Impresión remota.
- Aplicaciones host – terminal.
- Aplicaciones cliente – servidor.

- Acceso remoto a bases de datos.

- Construcción de bases de datos distribuidas.

3.3.4. Funcionamiento.

El mecanismo usado por Frame Relay es similar al **empleado por** redes orientadas a la multiplexión estadística.

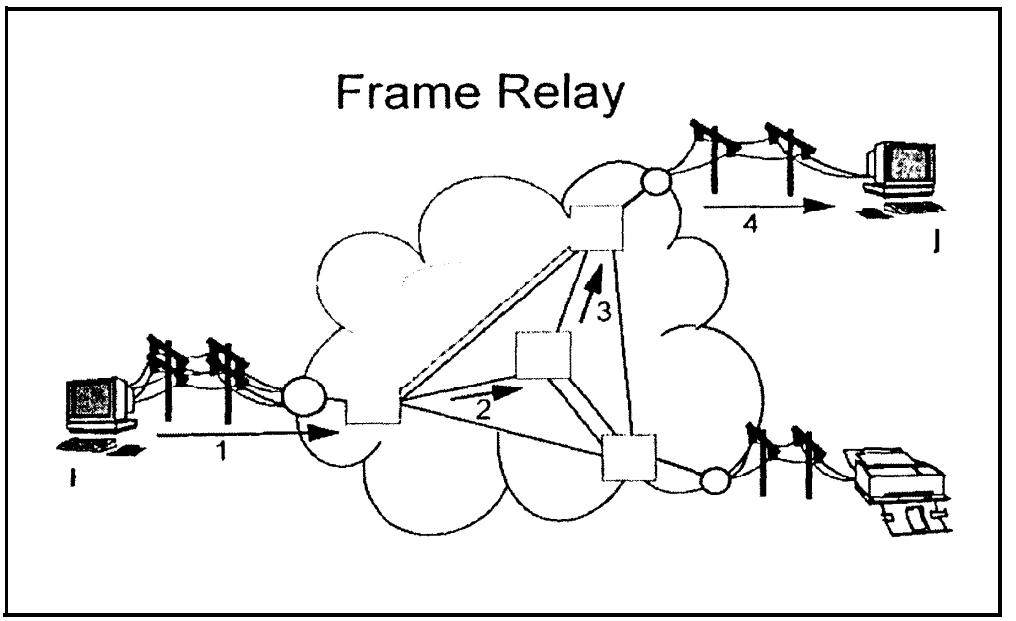


Figura 3.25. Los usuarios I y J establecen una comunicación con Frame Relay.

Suponga que los usuarios I y J, de la Figura 3.25, requieren enviarse información. El primer paso consiste en establecer una ruta para que la información pueda ser transportada.

Para ello se verifica la existencia de un circuito virtual en caso de utilizar conexiones permanentes (PVC) o se establece uno si se usa conexiones conmutadas (SVC). Luego la información es entregada a la red por los usuarios para dividirla en tramas, añadirles cabeceras y delimitadores de sincronismo. La cabecera de cada trama contiene el campo Data Link Connection Identifier (DLCI) que determina el direccionamiento que seguirá el paquete dentro de la red. Es prefijado en el caso de circuitos virtuales permanentes (PVC) o asignado dinámicamente si se trata de conexiones conmutadas (SVC).

Transmitidas las tramas llamadas frames son conmutadas en cada nodo, de acuerdo con unas tablas que asocian cada DLCI de entrada a un puerto de salida y un nuevo DLCI, hasta que alcanzan su destino. Allí son reensambladas y desprovistas de cabeceras. Estos identificadores, que no son direcciones de usuarios finales, constituyen referencias que determinan el direccionamiento en cada nodo, limitado al contexto de cada enlace ya que se modifican a lo largo del circuito virtual.

Ello determina mayor eficiencia si consideramos que la dirección completa ocupa más espacio, incrementa el congestionamiento y el tiempo de proceso de la información en cada nodo. El DLCI permite multiplexar las conexiones al compartir puertos y medios de transmisión, por lo que es más eficiente aún en lo que a la utilización de recursos se refiere.

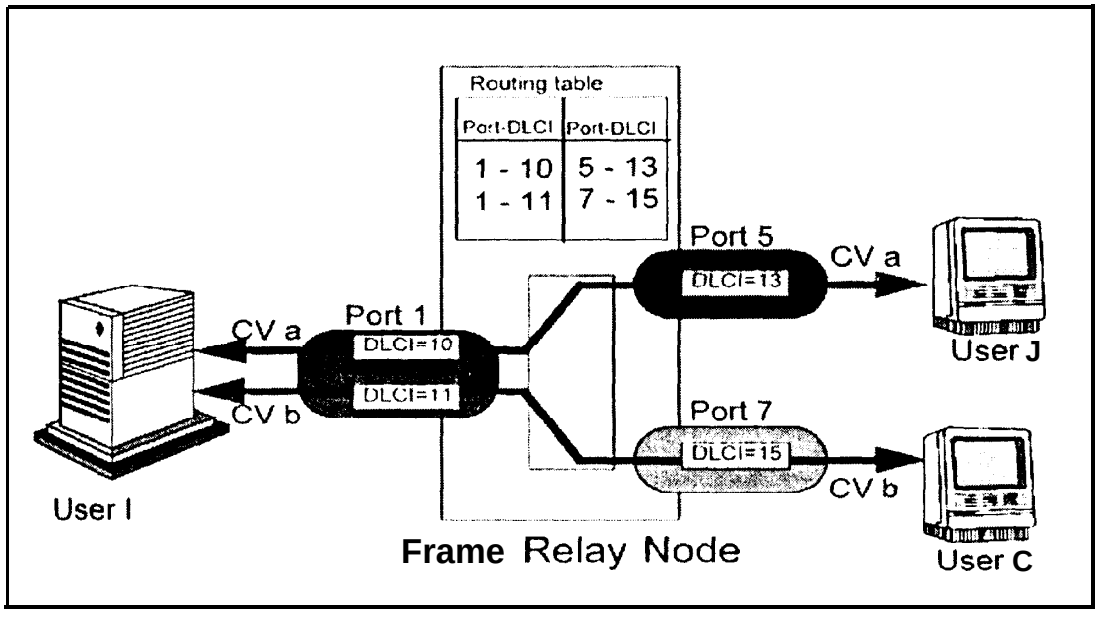


Figura 3.26. Los nodos Frame Relay de conmutación contienen tablas para el direccionamiento de la información.

3.3.4.1. Estructura de tramas.

El formato de la trama Frame Relay es simple y aparece en la Figura 3.27.

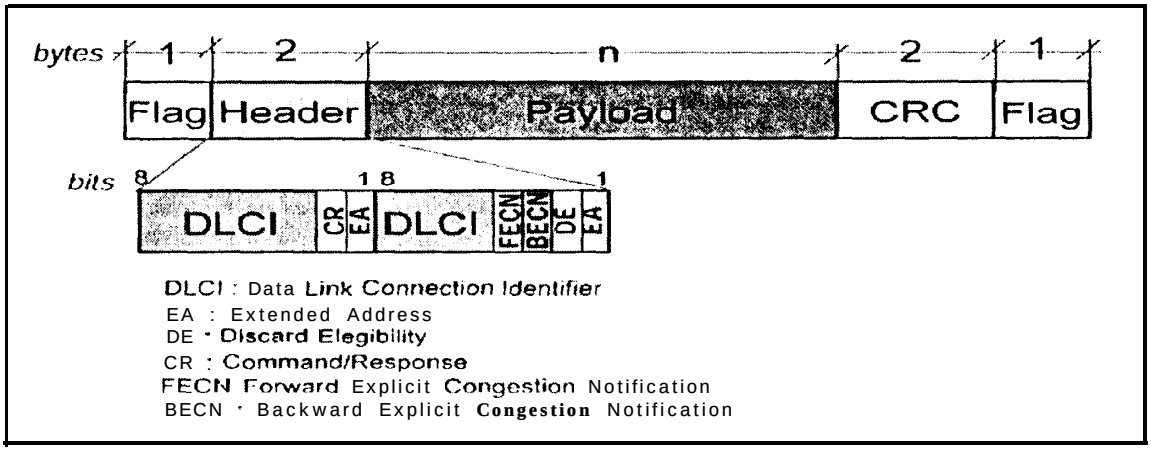


Figura 3.27. Estructura y formato de cabecera de trama Frame Relay.

Se aprecia que las tramas Frame Relay se inician y terminan con una bandera (flag), campo de 8 bits que corresponde a la secuencia 01 ll ll 10. A continuación está la cabecera o campo de 16 bits con información fundamental para el direccionamiento de la trama. Luego viene el campo destinado a la información que tiene longitud variable de máximo 1600 bytes. Y, finalmente aparece un campo de 16 bits que contiene el CRC (Cyclic Redundancy Check) de la trama, obtenido a través del polinomio CCITT $x^{16} + x^{12} + x^5 + 1$, que es un mecanismo de detección de errores.

En la cabecera encontramos:

- El identífícador **de conexión de enlace DLCI (Data Link** *Connection Identifier*), número de 10 bits que determina el direccionamiento de la trama.

  En la Figura 3.28 se muestra los diferentes usos de los DLCIs.

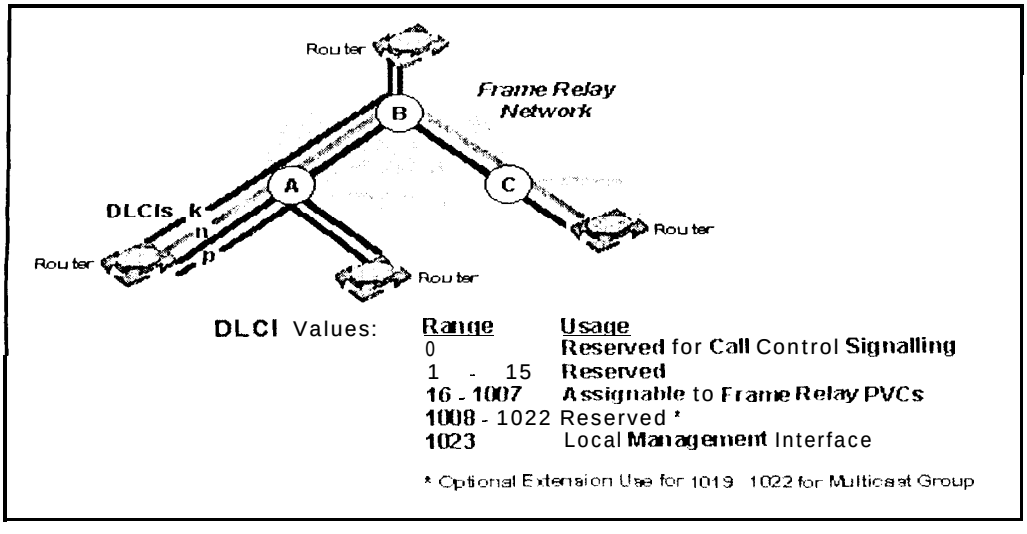


Figura 3.28. Usos del DLCI.

- El bit indicador comando respuesta C/R (Comand / Response) no es utilizado actualmente.

- El campo de la dirección extendida EA (Address field extension bit) determina si la longitud del campo de la dirección es de 10 bits o más.

- El bit de notificación de congestión hacia delante FECN (Forward Explicit Congestion Notification) usado por la red para indicar que existe la posibilidad de congestión en la dirección que sigue la trama.

- El bit de notificación de congestión hacia atrás BECN (Backward Explicit Congestion Notification) se activa cuando existe peligro de congestión en dirección opuesta a la que sigue la trama.

- El bit de posibilidad de descarte DE (Discard Eligibility) si está activo indica que la trama debe descartarse.

3.3.4.2. Circuitos virtuales.

Frame Relay usa múltiples circuitos virtuales unidireccionales para conectividad punto a punto bidireccional. Los circuitos virtuales son conexiones lógicas a varios puntos finales de usuarios en un ambiente WAN. Existen dos tipos. Los circuitos virtuales permanentes PVCs (Permanent Virtual Circuit), similares a las líneas dedicadas, son los más usados.

Los circuitos virtuales conmutados SVCs (Switching Virtual Circuit) optimizan el ancho de banda al requerir del inicio y término de una llamada. Se conocen también como circuitos virtuales dinámicos.

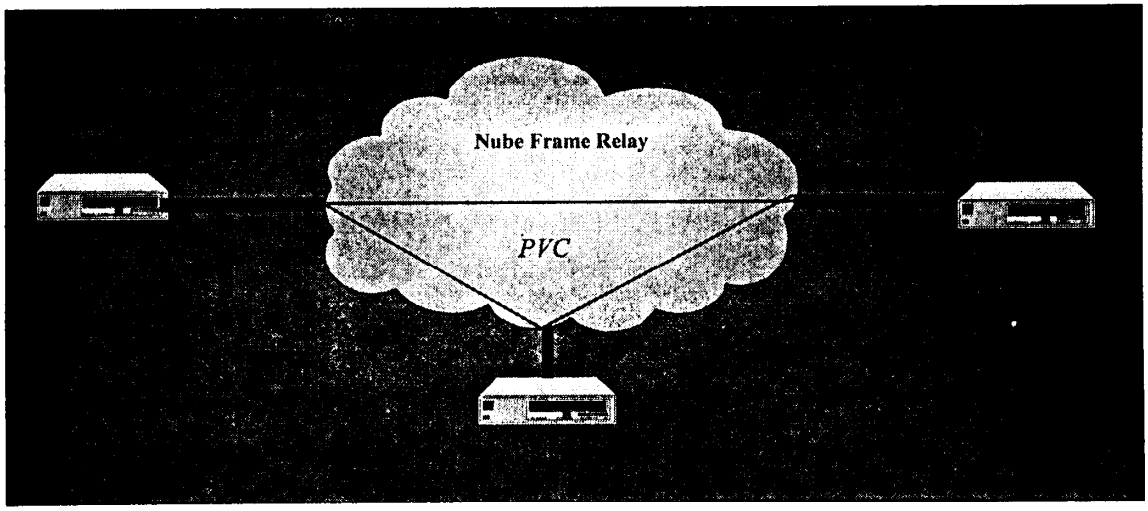


Figura 3.29. Red Frame Relay con circuitos virtuales permanentes.

3.3.4.3. Parámetros a dimensionarse.

Al hablar de Frame Relay términos tales como CIR, B_c, B_e y velocidad de acceso aparecen. A continuación se los explica brevemente.

CIR (Committed Information Rate) o coeficiente de infomación comprometido es la tasa promedio de procesamiento de información que el usuario puede esperar de un circuito virtual permanente PVC cuantificado en bits por segundo.

En teoría el usuario puede de transmitir datos en forma continua sin problemas sobre un PVC Frame Relay a esta tasa "promedio de bits por segundo". El CIR es configurable para cada PVC en los switches y en el equipo CPE.

B_c (Committed Burst) o tamaño de exceso comprometido es el número máximo de bits que el usuario puede transmitir sobre un circuito Frame Relay en un periodo determinado de tiempo T_c, con garantía de entrega en condiciones normales. Este parámetro es configurable para circuitos PVCs.

B_e (Excess Burst) o tamaño de sobreexceso es una cantidad de datos en bits por encima del B_c que si son transmitidos por el usuario dentro del tiempo T_c, la red intentará entregar. B_e es configurable para cada PVC. La ITU y ANSI consideran a todo lo que está por encima de este parámetro como información a descartar.

T_c es el período calculado al dividir el B_c para el CIR. Es usado para determinar el tiempo desde el cual los datos serán cuantificados, en total de bits, a fin de determinar si el usuario está dentro de sus acuerdos. T_c no es un parámetro que configurado directamente pero se deriva de valores introducidos para el B_c y el CIR.

Access rate o velocidad de acceso corresponde a la máxima velocidad con que los datos se colocan en la red definida por el tipo de línea que une al usuario a la red.

Cuando se realiza una suscripción a un servicio Frame Relay el usuario elige una velocidad de acceso que corresponde a la de la línea de conexión, un CIR y un B_e determinado, que son parámetros que afectan el rendimiento de la red a nivel de acceso. Veamos ahora un ejemplo de cómo se relacionan estos parámetros entre sí.

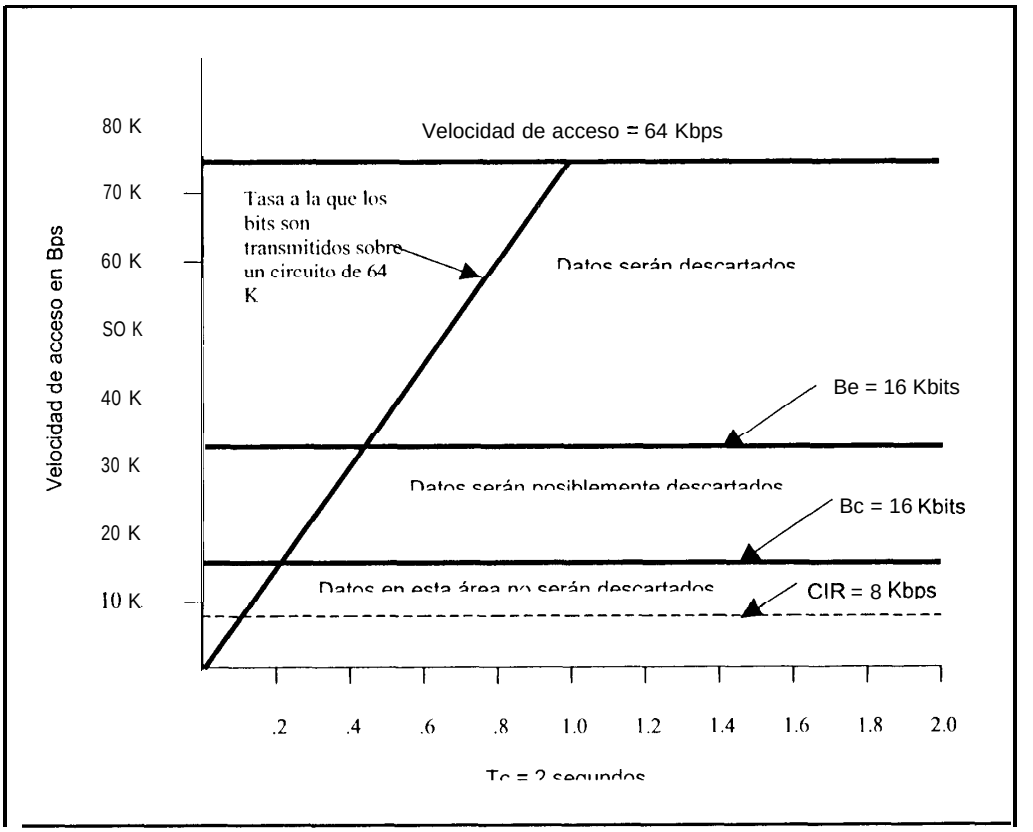


Figura 3.30. Tratamiento de datos en Frame Relay.

La Figura 3.30 es un ejemplo de cómo las tramas transmitidas sobre Frame Relay son tratadas.

El gráfico displaya una interfase de 64 kbps con específicos valores de CIR, Bc y Be. De acuerdo al gráfico 16 kbits pueden transmitirse cada dos segundos (Tc). Si el CIR fuese mejorado a 16 Kbps el período Tc se reduce a un segundo lo que dobla la cantidad de información procesada y afecta al Be por permitir que 16 kbits por encima del Bc se procesen cada segundo y no cada dos.

3.3.4.4. Gestión y prevención de la congestión.

Parámetro que permite cuantificar y mantener la calidad del servicio asignada a cada circuito virtual. Depende de la velocidad de salida del retardo y de la cantidad de tramas que llegan a su destino sin errores.

La calidad del servicio hace necesario mantener el control sobre la congestión, y eliminarla cuanto antes sí llegara a presentarse.

La primera medida consiste en el control del acceso de los usuarios. Para ello cual se definen tres parámetros, que ya vimos y mencionamos: el CIR, el Bc y el Be.

La segunda medida, referida a los procedimientos usados por Frame Relay para establecer el control de flujo de información, consta de mecanismos que notifican las condiciones de congestión en los nodos. Así los ruteadores disminuyen su velocidad de transmisión y alivian la congestión presentada por el empleo de los siguientes bits de notificación:

- FECN (Forward Explicit Congestion Notification), bit que indica al ruteador receptor que la trama pasó a través de uno o más nodos Frame Relay congestionados camino hacia su destino.

- BECN (Backward Explicit Congestion Notification), bit que señala al ruteador receptor que las tramas que él transmitirá encontrarán congestión antes de ellas alcanzar su destino.

- DE (Discard Elegibility), bit seteado por los ruteadores en las tramas para indicar que cierto tráfico es más apropiado para el descarte que otro. Cuando un switch Frame Relay encuentre congestión y sea necesario empezar a descartar tramas, éstas deben tener activado el bit DE. Si algún parámetro no ha sido correctamente configurado puede provocar que se active el DE en tramas que han sobrepasado el Bc.

Normalmente los bits FENC y BENC no se activan en todas las tramas afectadas por congestión, pero sí en aquellas responsables de la misma o en tramas de baja prioridad. La red descarta así las tramas apropiadas para mantener la calidad del servicio.

Además, estos bits, FECN y BECN, se comunican a través de tramas de datos porque no hay otro modo de generar mensajería de control. Entonces, existe una limitación para notificar congestión pues la red debe enviar datos hacia el usuario que la provoca.

A continuación, los criterios usados para disminuir la transmisión de datos si existe congestión:

Caso FECN: Si el número de tramas con FECN activo es mayor o igual al número de tramas con FECN inactivo, en un período de 4 veces el tiempo de propagación de un sistema final a otro, la velocidad de transmisión se reduce a 1/8 de su valor actual. En el caso inverso el usuario incrementa su velocidad de transmisión hasta en 1/16 igualando su CIR asignado.

Caso BENC: Se necesita determinar S o coeficiente de máxima salida aceptado por la red. Parámetro que se calcula en base al CIR, el Bc y el Be. Si la carga del usuario es mayor al CIR debe igualarse en primera instancia al CIR contratado. Si se recibe un número de tramas consecutivas, con BENC activo, el usuario debe reducir su carga a 0.675 veces el CIR la primera vez, 0.5 la segunda vez y 0.25, la tercera vez. Y después de reducir su carga, cada vez que se reciba S/2 tramas con BECN activo, el usuario debe incrementar su salida 0.125 veces.

Otra forma de detectar congestión es mediante la pérdida de tramas en la red debido a que, se supone, que la probabilidad de error es bien pequeña. En tales casos y si se detecta la pérdida de una sola trama, se sugiere al usuario reducir su velocidad de transmisión ¼ de su valor actual, y cada vez que se perciba la inexistencia de pérdidas de tramas en un período de tiempo determinado, debe incrementarse la salida del usuario en 1/8.

3.3.4.5. Estrategia de descarte de tramas.

Frame Relay se fundamenta en la estrategia de descarte de tramas: cuando surge una eventualidad ignora las tramas y las descarta. Corresponde al sistema final recuperar la información perdida mediante mecanismos de retransmisión de tramas. Muchas veces el extravío de una trama amerita la retransmisión de más de una de ellas por efecto de sincronización, pudiendo generar congestión al reusar recursos y generar tráfico extra; por ejemplo, cuando el usuario A envía cuatro paquetes de información al usuario B, y se pierde la trama 1, se volverán a enviar las tramas 1, 2, 3, 4.

3.3.5. Ventajas.

Frame Relay ofrece múltiples ventajas a quienes implementan su servicio de comunicaciones sobre esta plataforma; entre éstas:

- Flexibilidad del servicio porque se adapta a las necesidades dinámicas de sus clientes. Sobre un acceso de red, por ejemplo es posible establecer circuitos virtuales permanentes diversos que incorporen, sencilla y rápidamente, nuevas redes a la red del cliente.

- Posibilidad de contratación de CIR (clase de caudal).

- Empleo de tecnología de punta con altas prestaciones que determinan gran capacidad, bajos retardos y una elevada confiabilidad.

- Optimización y control de los costos de las telecomunicaciones porque Frame Relay admite la transmisión simultánea de tráfico generado por diversas comunicaciones y aplicaciones hacia diferentes destinos en un mismo recurso de red. Esto lo convierte en un multiprotocolo al soportar protocolos y aplicaciones comunes en el ambiente LAN como TCP/IP, IPX de Novell, SNA, SBR, TB, DECnet, Appletalk, etc.

3.4. Network address translation (NAT).

3.4.1. Introducción.

Es un esquema de enrutamiento que soporta conectividad al utilizar esquemas no únicos de direccionamiento. NAT reduce el número de clases de direcciones asignadas por IANA por reusar direcciones enrutables, que traduce desde un esquema de direccionamiento no enrutable, usado en una intranet, a uno enrutable, en el que las direcciones son únicas.

El mecanismo permite que redes direccionadas privadamente accesen a otras redes registradas por IANA sin requerir del registro del direccionamiento de la subred privada (intranet). Montaje que elimina la necesidad de renumerar el esquema de direccionamiento existente para soportar los requerimientos del sistema host de Internet.

Con NAT, la red privada es un esquema de direccionamiento interior que permite el uso continuado del esquema de direccionamiento existente, privado u obsoleto.

NAT convierte los esquemas de direccionamiento interno en otros, legalmente registrados, antes de enviar los paquetes a la red Internet pública definida como "el lado externo". NAT se aplica a ruteadores debido a que están físicamente conectados a ambos lados del esquema de direccionamiento.

El NAT se valora por su habilidad de llevar a cabo dicha traducción. En suma, simplifica la administración de la red por soportar requerimientos menos estrictos sobre el esquema de direccionamiento, es totalmente transparente al final del sistema, es muy flexible al soportar varias aplicaciones y protocolos; y, conduce mejor el perfomance del sistema.

3.4.2. Definición.

Es una aplicación que opera sobre un ruteador ubicado en la frontera entre el lado privado de un esquema de direccionamiento y su lado público. Las funciones de traducción conjuntamente con otras características de ruteo, permiten un acceso transparente al Internet desde un servidor privado remoto. Esta solución que reusa direcciones, simplemente asigna a la dirección del lado interno una dirección del lado externo. Entonces, la dirección del lado interno aparece del lado externo como una dirección legalmente registrada.

Esta solución fue originalmente diseñada para comunicar un pequeño número de servidores privados con servidores públicos, siendo esto totalmente escalable y deseable para las ISPs, las cuales requieren de esquemas de interconexión a gran escala, siendo beneficioso en la medida de que ahorran el costoso registro de un gran número de clases de direcciones.

El NAT elimina la importancia end to end del direccionamiento IP para permitir incrementar el reuso del esquema de direccionamiento. TCP, protocolo orientado a conexión, en forma esencial ejecuta el reuso de direcciones de cada salto; NAT simplemente extiende ese reuso al nivel de red.

3.4.3. Funcionamiento del NAT.

Desde que el NAT realiza el mapeo IP uno a uno, el paquete que ingresa a un ruteador NAT, ya sea desde el interior o desde el exterior, sufre una transformación. En su forma más simple, el campo de la cabecera de la dirección IP es traducido y reemplazado por uno nuevo.

En suma, para cambiar la dirección IP en su cabecera, el mecanismo de control de error para el paquete IP debe ser recalculado y verificado para garantizar su integridad. Además, debido a que la cabecera TCP contiene un mecanismo de control de error que se calcula a través del análisis del socket, el cual es una combinación de direcciones de puerto TCP y direcciones IP, la cabecera TCP tiene que ser modificada también.

Para hacer al NAT transparente a los niveles de aplicación, el proceso debe también convertir cualquier paquete de aplicación que se relacione a un esquema de direccionamiento a un nuevo esquema. Estos son FTP, ICMP,SNMP, encriptación.

3.4.4. Ventajas y desventajas.

La ventaja principal de los NATs es que éstos conservan el esquema de direccionamiento legalmente registrado para permitir la privatización de una intranet. Este escenario, por supuesto, tiene sus repercusiones al reducir considerablemente el número de clases de direcciones registradas y centralizar el modo de acceso a Internet.

Otra ventaja es la flexibilidad. El diseño de la red se simplifica por las limitantes disponibles en el esquema de direccionamiento ofrecido de acuerdo con las conveniencias administrativas y operacionales de crecimiento. Además, cuando las empresas emergen, los NATs tienen en cuenta la fusión de red sin divisiones, mientras mantiene el esquema existente de direccionamiento.

La reducción del traslape en el esquema de direccionamiento es otra ventaja. Si un esquema se monta originalmente dentro de una intranet, y luego la intranet se conectada a Internet sin traducción de sus direcciones, existe la posibilidad de ocurrencia de un traslape. Serio problema porque los protocolos de ruteo no proveen direccionamiento confiable si éstos son ambiguos.

Para salvaguardar esos problemas, las ISPs utilizan filtros de ruteo, los cuales proveen de un método seguro para evitar traslapes en los NATs, en tanto conservan total *conectividad* con Internet.

Por otro lado, la desprivatización de una red requiere de renumerar toda la red existente. Los costos se encuentran asociados al número de servidores que requieren convertirse al nuevo esquema de direccionamiento. La ventaja del uso de los NATs radica en que éstos permiten que el esquema de direccionamiento existente se conserve, a la vez que soporta el nuevo esquema de direccionamiento público asignado.

Entre las desventajas, la más grande es la dificultad de localizar paquetes de información ya que su numeración está sujeta a cambios en cada uno de los múltiples saltos. Este escenario hace, de cualquier manera, que exista la tendencia de migrar hacia enlaces más seguros, en el cual los hackers no puedan descubrir el origen del paquete o su destino.

Otra desventaja la constituyen los retardos introducidos por la traducción de cada dirección IP dentro de la cabecera del paquete. Dicha modificación es una limitación del diseño de interconexión dentro de la intranet.

NAT también fuerza a aplicaciones usadas por el esquema de direcionamiento IP a detener su funcionamiento porque esto oculta el end to end de una dirección IP.

Las aplicaciones que usan direcciones IP físicas en lugar del nombre de un dominio calificado no alcanzarán su destino a menos que sea traducidos por un ruteador NAT. Algunas veces esto se evita implementando para ello el mapeo de NAT estático.

Se trata de un servicio normalizado según los estándares y recomendaciones de UIT-T y ANSI, lo que garantiza la interoperatividad de este protocolo con cualquier otro también estandarizado.

3.5. Tecnología utilizada en Redes Privadas Virtuales VPN.

Por lo general se utilizan cuatro protocolos diferentes para crear Redes Privadas Virtuales sobre Internet y son los siguientes: PPTP (Point to Point Tunneling Protocol), L2F (Layer Two Forwarding), L2TP (Layer 2 Tunneling Protocol), IPSec (IP Security Protocol). Una razón para este número de protocolos se debe a que para algunas compañías, una VPN es un substituto para acceso hacia servidores remotos, permitiendo de esta manera a usuarios móviles y oficinas sucursales el acceso dial-up hacia la red protegida a través de un ISP local. Para otras una VPN puede consistir de tráfico viajando a través de túneles de seguridad sobre el Internet entre LAN protegidas. PPTP, L2F y L2TP son dirigidos hacia accesos dial-up a VPN, mientras el protocolo IPSec se encuentra principalmente enfocado para soluciones LAN a LAN.

3.6. Generalidades de protocolos utilizados en Redes Privadas Virtuales.

3.6.1. PPP.

3.6.1.1. Generalidades.

Point to Point Protocol fue una solución propuesta por el IETF y es conocido como PPP. Se puede utilizar sobre cualquier circuito duplex, ya sea síncrono orientado a bit o asíncrono orientado a byte. Se puede utilizar por líneas telefónicas lentas, líneas rápidas alquiladas, RDSI o incluso en líneas de Fibra Optica. Se diseñó para llevar la PDU (Protocol Data Unit) de varios protocolos: IP, IPX, DECnet, ISO y otros. Incluye varios subprotocolos como son:

- Protocolo de *control* de enlace, el cual establece, comprueba, configura y cierra un enlace.

- Protocolo de *control* de red, el cual inicializa, configura y termina el uso de un protocolo de red concreto. Se define un protocolo de red distinto para IP, IPX, DECnet, etc.

3.6.1.2. Escenario Típico de PPP.

1. PPP de origen envía una trama de Control de Enlace para empezar la sesión. Luego se intercambian tramas adicionales que establecen las opciones de uso del enlace.

2. Se intercambian tramas del protocolo de control de red para seleccionar y configurar los protocolos de la capa de red que se van a utilizar.

3. Se envían datos de los protocolos seleccionados por el enlace en tramas de PPP. Cada trama incluye un campo de cabecera que identifica el tipo de datos del protocolo que se envía.

4. Las tramas de Control de Red y del Protocolo de Control de enlace crean el enlace.

La cabecera de una trama PPP se parece mucho a una cabecera de PPP con un campo adicional que identifica el protocolo de la siguiente capa.

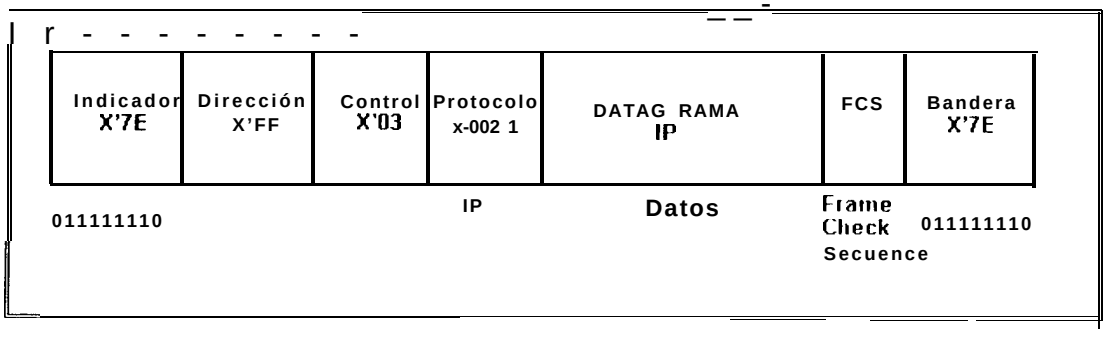


Figura 3.31. Formato de trama de PPP con un datagrama de IP.

X'FF significa a todas las direcciones.

X'03, información sin numerar.

X'0021, valor propio de datagramas de IP.

La compresión optimiza la utilización del protocolo PPP. En ella se suprimen octetos de dirección y control que generalmente se repiten en todas las tramas. Es decir, en cada extremo del enlace PPP establecido se puede coordinar el funcionamiento en *modo de compresión PPP.*

El campo protocolo indica la clase de la información contenida en la trama PPP, es decir, si es un mensaje de control de enlace, un mensaje de red o información (datagrama IP). Durante el establecimiento de un enlace de PPP, el campo protocolo empieza con un tamaño de 16 bits, siendo factible reducirlo a un campo de 8 bits. Con estas consideraciones la trama PPP comprimida quedaría como lo muestra la Figura 3.32.

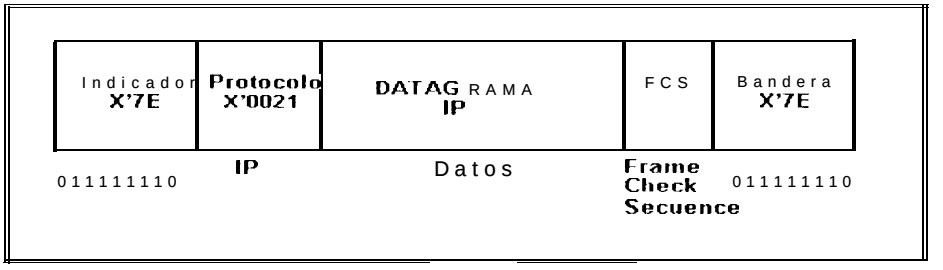


Figura 3.32. Trama de PPP con formato comprimido.

Autentificación: PPP conecta a un trabajador o usuario remoto en general a la red corporativa a través de una llamada telefónica, pudiendo en ocasiones conectar a un router, una LAN hasta la oficina central corporativa.

PPP dispone de dos métodos de autentificacíón:

- Protocolo de autentificación de contraseña PAP (Password Autentication Protocol). Envía una trama con la información del identificador de usuario y su contraseña durante el establecimiento del enlace.

- El protocolo de autentificación Challenge Handshake CHAP (Challenge Handshake Authentication Protocol).

El protocolo *Challenge Handshake* funciona de la siguiente manera:

- Envía el nombre del usuario en forma de texto a través del enlace.

- El extremo remoto envía de vuelta un mensaje de compromiso aleatorio.

- El sistema local realiza un cálculo de clasificación del mensaje, utilizando como entradas el mensaje de trabajo y la contraseña del usuario, y envía la respuesta de vuelta.

- El extremo remoto (servidor) examina la contraseña, realiza el mismo cálculo y compara los resultados.

3.6.1.3. Control de la calidad del enlace.

PPP proporciona una forma muy simple y efectiva de comprobar la calidad del enlace. Debido a que en ocasiones la calidad del enlace se degrada por alguna razón, bajo estas condiciones resultaría de gran ayuda tener un aviso de las condiciones del enlace para tomar alguna acción, por ejemplo, marcar

nuevamente, o (si el enlace es dedicado) se podría avisar al técnico responsable del problema pudiendo, en el caso de ser posible desviar el envío del tráfico hacia un enlace de back-up.

El proceso del control del enlace simplemente cuenta los números de tramas y octetos enviados y recibidos, así como las tramas descartadas y los errores. De forma periódica envía esta información al otro extremo del enlace, estos valores al ser analizados en conjunto van a permitir determinar las condiciones por las que atraviesa el enlace.

3.6.2. PPTP.

Uno de los primeros protocolos desarrollados para VPNs. Este protocolo se enfoca hacia soluciones dial-in en VPNs. Hasta Microsoft incluye soporte para RAS en Windows NT Server 4.0 y ofrece un cliente PPTP en un Service Pack para Windows 95. La inclusión de Microsoft como cliente PPTP en Windows 98 prácticamente asegura su continuo uso dentro de los próximos años, mas no sea respaldado por las normas de estandarización como la IETF (Internet Engineering Task Force).

Sin embargo, PPTP se construye sobre la funcionalidad del PPP, protocolo de acceso a Internet más usado, para proveer acceso remoto de manera que pueda ser encapsulado y enviado a través del Internet a una ubicación destino.

Por lo general, PPTP encapsula paquetes PPP utilizando una versión modificada de GRE (Generic Routing Encapsulation Protocol), que le da al PPTP la flexibilidad de manipular otros protocolos a parte de IP, como el IPX (Internet Packet Exchange), NetBEUI (Network Basic Input/Output System).

Tomando en cuenta la dependencia sobre PPP, PPTP utiliza los mecanismos de autentificación de PPP, los conocidos PAP (Password Authentication Protocol) y CHAP (Challenge Handshake Autentication Protocol). Debido a fuertes lazos existentes entre PPTP y Windows NT, se utiliza también una versión mejorada de CHAP, llamada MS-CHAP, que a su vez utiliza información ubicada dentro del dominio NT para seguridad.

De forma similar, PPTP utiliza encriptación de datos PPP y una versión mejorada incorporada por Microsoft llamado MPPE (Microsoft Point to Point Encryption).

La principal ventaja de este protocolo es que se diseñó para correr en la capa 2 del Nivel OSI (capa de enlace de datos), en oposición al IPSec, el cual corre en la capa 3, lo cual lo capacita para encapsular otros protocolos diferentes al IP. Pero a pesar de esta ventaja, PPTP tiene limitaciones, por ejemplo, no provee de fuerte encriptación para datos protegidos y, no soporta métodos basados en *tokens* (fichas) para autentificación de usuarios.

3.6.3. L2F.

El protocolo L2F ascendió en etapas iniciales del desarrollo de las VPNs. Al igual que PPTP, L2F se diseñó para encapsular tráfico desde usuarios hasta sus sites corporativos.

La mayor diferencia entre el PPTP y el L2F radica en un encapsulamiento no dependiente de IP, capaz de trabajar directamente con otros medios, como Frame Relay o Modo de Transferencia Asincrónica (ATM).

Al igual que PPTP, L2F utiliza PPP para autentificación de usuarios remotos, pero también incluye soporte para TACACS+ y RADIUS para autentificación. L2F difiere de PPTP porque puede dar sopor-te a través de un túnel a más de una conexión. Existen dos niveles de autentificación de usuarios, primero considerando la prioridad del ISP de establecer el túnel y luego cuando la conexión ya es establecida en el gateway corporativo. Como L2F es un protocolo de capa 2 ofrece al usuario la misma flexibilidad que el PPTP para manipular otros protocolos diferentes a IP, como son el IPX y NetBEUI.

3.6.4. L2TP.

L2TP está siendo diseñado por un grupo de trabajo IETF para constituirse en estándar. Es sucesor mejorado inmediato del PPTP y L2F.

L2TP utiliza PPP para proveer acceso dial-up que puede ser encapsulado a través del Internet a un site determinado. Sin embargo, L2TP define su propio protocolo de encapsulamiento. El transporte L2TP se define para una variedad de medios de empaquetamiento que incluyen X.25, Frame Relay y ATM. Además, fortalece la encriptación de los datos que manipula, utilizando métodos de encriptación IPSec.

Como L2TP utiliza PPP para enlaces dial-up, incluye mecanismos de autentificación de PPP, llamados PAP y CHAP. También soporta la utilización de un protocolo de autentificación expandible de PPP para otros sistemas de autentificación, como RADIUS, PPTP, L2F y L2TP, no todos incluyen encriptación o procesos de administración de claves de codificación requeridas para encriptación en sus especificaciones. El borrador actual del estándar L2TP recomienda que el IPSec sea utilizado para encriptación y administración de claves en ambientes IP.

3.65 IPSec.

Protocolo más importante que creció gracias a los esfuerzos por desarrollar un empaquetamiento IP tan seguro como la próxima generación de IP (IPv6), pudiendo también ser utilizado con protocolos IPv4.

Aunque el RFC que define al IPSec es parte de los estándares del IETF desde mediados del 95, sigue siendo revisado por Ingenieros y productos que aparecen en el mercado.

El protocolo IPSec provee servicios de seguridad a nivel de capa IP, puesto que permite que un sistema seleccione los protocolos de seguridad que sean necesarios y determine los algoritmos a ser utilizados, entre otras cosas.

IPSec se utiliza para proteger una o más rutas entre un par de hosts, gateways de seguridad, o un gateway y un host. El término gafeway de seguridad se referiere a un sistema intermedio que utiliza protocolos IPSec. Por ejemplo, un ruteador o un firewall con implementación IPSec constituye un gateway de seguridad.

El grupo de servicios de seguridad que IPSec proporciona incluye, control de acceso, integridad sin conexiones, autentifícacíón de origen de datos, rechazo de paquetes repetidos (una manera de integridad secuencial), confidencialidad (encriptación).

Estos servicios son provistos en la capa IP y pueden ser utilizados por cualquier protocolo de una capa superior, por ejemplo, TCP, UDP, ICMP, BGP, etc.

3.651. Funcionamiento.

IPSec utiliza dos capas de protocolos para asegurar el tráfico, Authentication Header (AH) y Encapsulating Security Payload (ESP).

- El IP Authenticaction Header (AH) proporciona integridad sin conexiones, autentificación del origen de datos y un servicio opcional anti-repetición.

- El Encapsulating Security Payload (ESP) provee confidencialidad (encriptación), y confidencialidad limitada al flujo de tráfico. También da integridad sin conexiones, autentificación de origen de datos, y servicio anti-repetición.

- Ambos protocolos AH y ESP, son herramientas de control de acceso. Se basan en la distribución de claves criptográficas y la administración del flujo de tráfico presente entre los protocolos de seguridad.

3.6.5.2. Modos de utilización.

El IPSec se utiliza para autenticar y encriptar paquetes en el modo de transporte y en el modo de encapsulamiento. En el primero, un segmento del paquete IP se autentica y encripta, en el segundo, la autentificación y encriptación ocurre en todo el paquete IP.

Mientras el IPSec en modo de transporte ha probado ser muy útil, el modo de encapsulamiento IPSec, proporciona mayor protección contra continuos ataques y monitoreo de tráfico que pueden ocurrir en el Internet.

Estos protocolos pueden ser aplicados solos o en combinación para proporcionar un grupo de servicios de seguridad. En modo transporte los protocolos proveen protección primaria para los protocolos de capas superiores; en modo de túnel estos protocolos se utilizan para encapsular paquetes IP.

IPSec permite al usuario (o administrador del sistema) controlar el nivel de seguridad que ofrecen. Por ejemplo, alguien puede crear un solo túnel para acarrear todo el tráfico entre dos gateways de seguridad o se puede crear un túnel encriptado de forma separada para cada conexión TCP entre cada par de Hosts que se están comunicando a través de los gateways.

La administración del IPSec incorpora facilidades que especifican:

- Cuáles son los servicios de seguridad que van a utilizarse y en que combinaciones.
- Los niveles a los cuales se debe aplicar protección y seguridad (Políticas de Seguridad).
- Los algoritmos de encriptación que van utilizarse para efectos de seguridad (Algoritmos de Encriptación).

El desafío de conocer cuál es el mejor método para intercambiar y administrar claves de codificación para la encriptación de la información ha sido intensamente cuestionado y el esquema ISAKMP/Oakley (ahora llamado IKE (Internet Key Exchange)) está siendo revisado para ser aceptado como un estándar IETF.

Como estos servicios de seguridad comparten valores secretos llamados claves criptográficas, IPSec confía en un grupo de mecanismos separados, para poner las claves en su lugar. (Las claves son utilizadas para servicios de autentificación y servicios de encriptación).

Se especifica una aproximación basada en claves públicas para administración de claves automáticas, pero también se utilizadan otras técnicas de distribución automática de claves. Por ejemplo sistemas basados en KDC tales como Kerberos y otros sistemas de claves públicas como SKIP también podrían ser empleados.

IPSec permite al emisor (o un gateway de seguridad en sí) autentificar o encriptar cada paquete IP o aplicar ambas operaciones. IPSec se construye sobre un número de tecnologías criptográficas estandarizadas que proveen confidencialidad, integridad de datos, y autentificación, que son:

- Intercambio de claves Diffie-Hellman, que entrega claves secretas entre pares semejantes, sobre una red pública de datos.

- Codificación de claves públicas para señalizar intercambio Diffie-Hellman, que garantiza la identidad de las dos partes y previene ataques tipo man-in-the-middle o intromisión de terceros.

- DES y otros algoritmos de encriptación de datos de gran capacidad.

- Algoritmos codificados hash (HMAC, MD5, SHA).

- Certificados digitales para validar claves públicas.

Existen dos maneras de intercambiar y administrar claves dentro de la arquitectura del IPSec: la codificación manual y el intercambio de claves en Internet (Internet Key Exchange IKE) para una administración automática de claves. Estos dos métodos son requerimientos obligatorios del IPSec. Mientras el intercambio manual de claves puede ser conveniente para una VPN con un pequeño número de enlaces, las VPNs que cubren un gran número de sitios o soportan algunos usuarios remotos se benefician de una administración automatizada de claves.

El IPSec se considera la mejor solución para ambientes IP, debido a que incluye fuertes medidas de seguridad -encriptación, autentificación, y administración de claves- en su estructura estándar. IPSec, diseñado para trabajar únicamente con paquetes IP, PPTP y L2TP, se utiliza en ambientes multiprotocolos como los que utilizan NETBEUI, IPX y AppleTalk.

3.653. Donde puede ser implementado IPSec.

IPSec se implementa en un Host o en conjunto de ellos con un router o firewall, para crear un gateway de seguridad. A continuación, ejemplos comunes son dados:

- Integración IPSec dentro de la implementación nativa IP. Requiere acceso al código fuente IP y es aplicable a ambos Hosts y gateways de seguridad.

- Implementación “Bump in the stack” (BITS), donde IPSec se ubica debajo de una implementación de una pila de protocolos existente, entre el IP nativo y los drivers de una red local. El acceso al código fuente para la pila IP no es requerido, haciendo de esta implementación la más apropiada para sistemas legales. Generalmente se utiliza en Hosts.

- Un procesador criptográfico se presenta de manera común en diseños de sistemas de seguridad para redes y lo utilizan militares y algunos sistemas comerciales. Esta implementación se conoce como Bump in the Wire (BITW) y se diseña para servir a un Host, gateway o ambos. Generalmente el equipo BITW es direccionable bajo IP. Cuando lo soporta un único Host, es similar a una implementación BITS, pero para dar soporte a un router o un firewall, debe operar como un gateway de seguridad.

3.6.5.4. Asociaciones seguras.

El concepto de asociaciones de seguridad (SA) es fundamental para el IPSec. Tanto AH como ESP hacen uso de SAs. Una de las principales funciones de IKE es el establecimiento y mantenimiento de asociaciones de seguridad. Todas las implementaciones de AH o ESP deben soportar el concepto de asociaciones de seguridad.

3.655. Definición y cobertura.

Una asociación segura es una conexión simple que dispone de servicios de seguridad para el tráfico acarreado por ella. Los servicios de seguridad son provistos por un SA por el uso de AH o ESP, pero no ambos. Si tanto los protocolos de protección AH como ESP son aplicados a una cadena de tráfico, entonces, dos o más SAs son creados para esta cadena de tráfico. Para asegurar una comunicación bidireccional entre dos Hosts, dos gateways de seguridad, son necesarias dos asociaciones seguras (una en cada lado).

Una asociación segura se identifica únicamente por los tres parámetros siguientes: Security Parameter Index (SPI), una dirección IP destino y un identificador del protocolo de seguridad sea AH o ESP.

Los mecanismos de administración IPSec SA actualmente se utilizan solamente para direcciones unicast.

3.6.5.6. Tipos de asociaciones seguras SAs.

Se definen dos tipos de SA: Modo transporte y modo túnel.

AS Modo transporte: Es una asociación segura entre dos hosts. La cabecera del protocolo de seguridad en modo transporte aparece inmediatamente después de la cabecera IP y de algunas opciones adicionales, y antes de cualquier protocolo de capa superior (por ejemplo TCP, UDP).

En el caso del ESP, un modo transporte provee servicios de seguridad solamente para las capas superiores de protocolos no para las cabeceras IP, ni para alguna extensión de las cabeceras precedentes a la cabecera ESP.

En el caso de AH, la protección es extendida hacia ciertas partes de la cabecera IP, partes de cabeceras de extensión, y opciones seleccionadas.

AS Modo Túnel: Un modo túnel es una AS aplicada a un túnel IP. Una SA entre dos gateways de seguridad siempre es un túnel, así como una AS entre un host y un gateway de seguridad.

Para los casos por ej. Comandos SNMP, el gateway de seguridad funciona como un Host, entonces está permitido el modo transporte, es decir en este caso el gateway de seguridad no debería estar funcionando como gateway sino como un host sin transmitir tráfico.

Para una asociación de seguridad modo túnel, hay una cabecera IP externa que especifica el procesamiento de destino, mas una cabecera interna que especifica el último destino para el paquete. La cabecera del protocolo de seguridad aparece después de la cabecera IP externa, y antes de la cabecera IP interna.

Si es empleado AH en modo de túnel, algunas partes de la cabecera IP externa está provista de protección, así como todos los paquetes encapsulados.

Si es empleado el ESP, la protección es provista solamente para los paquetes encapsulados, no para la cabecera externa.

En suma:

a) Un host puede soportar ambos modos, tanto túnel como transporte.
b) Un gateway de seguridad soporta únicamente modo de túnel. Si este soporta el modo transporte, entonces debería ser utilizado solamente cuando un gateway de seguridad que está actuando como un host, por ejemplo para la administración de una red.

3.6.5.7. Funcionamiento de las asociaciones seguras.

El grupo de servicios de seguridad ofrecidos por una *SA* depende de los protocolos de seguridad seleccionados, el modo SA, los puntos finales del SA, y de la elección de servicios opcionales dentro del protocolo.

Por ejemplo AH proporciona autentificación de origen de datos, e integridad sin conexiones para datagramas IP. AH es un protocolo mas apropiado para utilizar cuando no es requerida la encritptación o no es permitida debido a restricciones gubernamentales. AH también proporciona autentificación para determinadas partes de la cabecera IP.

ESP de manera opcional proporciona confidencialidad para tráfico (la fortaleza de los servicios de confidencialidad depende en parte de los algoritmos de encriptación empleados). ESP también puede proveer autentificación. Si la autentificación es negociada por un ESP SA el receptor también puede elegir, reforzar un servicio anti-replay. La cobertura de la autentificación ofrecida por ESP es menor que la que proporciona AH, la cabecera IP externa no es protegida. Si solamente los protocolos de la capa superior necesitan ser autentificados entonces la autentificación ESP es la mejor elección y la mas eficiente.

Se debe recalcar que aunque la confidencialidad y autentificación son opcionales, los dos no pueden ser omitidos. Al menos uno de ellos debe ser seleccionado. Si el servicio de confidencialidad es seleccionado, entonces un ESP (modo túnel) SA entre dos gateway de seguridad puede ofrecer confidencialidad para una parte del flujo de tráfico.

El uso del modo túnel permite a la cabecera interna IP ser encriptada, ocultando así las identidades del tráfico entre fuente y destino.

El uso del ESP payload padding también puede ser utilizado para esconder el tamaño de los paquetes, ocultando de esta manera las características externas del tráfico.

Similares servicios de confidencialidad son necesarios con un usuario móvil en un acceso dial-up estableciendo un SA ESP a un firewall de una a red corporativa (que está actuando como un gateway de seguridad).

3.6.5.8. Combinando asociaciones de seguridad.

Los datagramas IP transmitidos sobre un SA tienen sistemas de protección por exactamente un protocolo de seguridad, sea AH o ESP, pero no ambos. Algunas veces una política de seguridad puede necesitar una combinación de los servicios de seguridad para determinados datagramas IP, en estos casos es necesario emplear múltiples SAs.

Capítulo 4.

4. Análisis y Diseño del Proyecto.

4.1. ¿Quiénes son SECOHI?.

Segundo Corrales e Hijos, SECOHI, es una empresa dedicada a la venta de repuestos de maquinaria pesada como Mercedes Benz, Man, Volvo al por mayor y menor. Abarca el mercado de los transportistas: tractores, vehículos de carga pesada, trailers, vehículos de transporte de mercaderías en general.

Para captar el mercado nacional, la empresa cuenta con seis agencias ubicadas en Latacunga (Matriz), Quito, Cuenca, Guayaquil, Ambato e Ibarra. Desde la matriz (agencia Latacunga) se realiza la administración de la totalidad de la empresa así como el control de inventario, compra y despacho de mercadería. Consciente de las necesidades de los transportistas ofrece la entrega de sus pedidos con precisión, esmero y prontitud donde el cliente lo requiera, ofreciendo para ello facilidades de crédito y una correcta atención personalizada.

4.2. Situación actual de la empresa.

Las oficinas sucursales de SECOHI, como muestra la figura 4.1, no se encuentran integradas de manera permanente a través de una intranet. Cada una de ellas cuenta con una red LAN provista de un servidor Windows NT y de 4 a 10 computadoras dependiendo de la agencia. Adicionalmente cada sucursal está equipada con un modem, que permite conectar cada agencia a un ISP local haciendo una llamada telefónica para accesar como un cliente dial-up.

La actualización de precios y cotizaciones de pedidos entre sucursales, se realiza diariamente a través del intercambio de e-mails a primeras horas de la mañana y tarde. Cada intercambio de información consta del envío y recepción de correo electrónico así como de las respectivas confirmaciones de los e-mails recibidos entre sucursales, desde las sucursales a la Matriz y viceversa.

4.3. Necesidad de interconexión.

El sistema que maneja SECOHI para comunicar sus oficinas se ha convertido en una solución muy precaria que origina inconvenientes y malestares por los siguientes motivos:

- No existe interconexión permanente entre todas las sucursales. Sólo están enlazadas durante el tiempo que estén conectados a Internet (vía mail).

- Es un cliente dial-up, su comunicación depende de una línea telefónica. Si se interrumpe el servicio telefónico 0 no se logra accesar al Internet por congestión de usuarios quedan incomunicados. Establecer la conexión bajo estas condiciones no garantiza un tiempo de transferencia de información sin interrupciones y genera un retardo creciente y molesto para el personal de SECOHI y sus clientes. Cuando Internet no les funciona envían información físicamente en diskettes utilizando para ello transportes interprovinciales. Ello pone en riesgo la confidencialidad de la misma, aumenta el retardo y reduce la velocidad de respuesta a sus clientes.

- La velocidad efectiva de comunicación es lenta y lo es más el tiempo para transferencia y recuperación de información lo que repercute directamente en el nivel de ventas. Los clientes de hoy exigen precios convenientes y respuestas rápidas a sus necesidades, factores claves para el desarrollo y permanencia en el mercado de cualquier empresa.

- Lo referido afecta también al correcto desempeño de empleados porque se ven obligados a repetir actividades una y otra vez, principalmente la

confirmación vía telefónica de que todos los archivos han llegado completos.

Pero SECOHI, es una empresa que está en la búsqueda de sistemas de comercialización basados en transparencia y competitividad a fin de satisfacer a plenitud los requerimientos de calidad y garantía del producto, y ofrecer a sus clientes un servicio eficiente, personalizado e inmediato para consolidarse como un ente competente que se adapta a las condiciones cambiantes del mundo actual. Es por ello que, considerando las altas metas planteadas, y a sabiendas que la condición de permanencia en el mercado es integrar sus sucursales distribuidas en forma estratégica en las principales ciudades del país, nuestro grupo de trabajo plantea una propuesta basada en los adelantos tecnológicos de los que el Ecuador está formando parte en el comenzar de este nuevo milenio.

Esta solución no solo es económicamente acertada a corto plazo, sino también a largo plazo, a pesar de que el Internet en nuestro país está en su etepa inicial. Cuando se masifique este último, futuro próximo, habrá mayor competencia a nivel de precio, velocidad y calidad del acceso a la red.

4.4. Beneficios de una intranet.

- Acceso a la base de datos existente en la matriz y demás oficinas sucursales en forma segura y sin retrasos en los envíos y recepción de mails con sus respectivas confirmaciones.

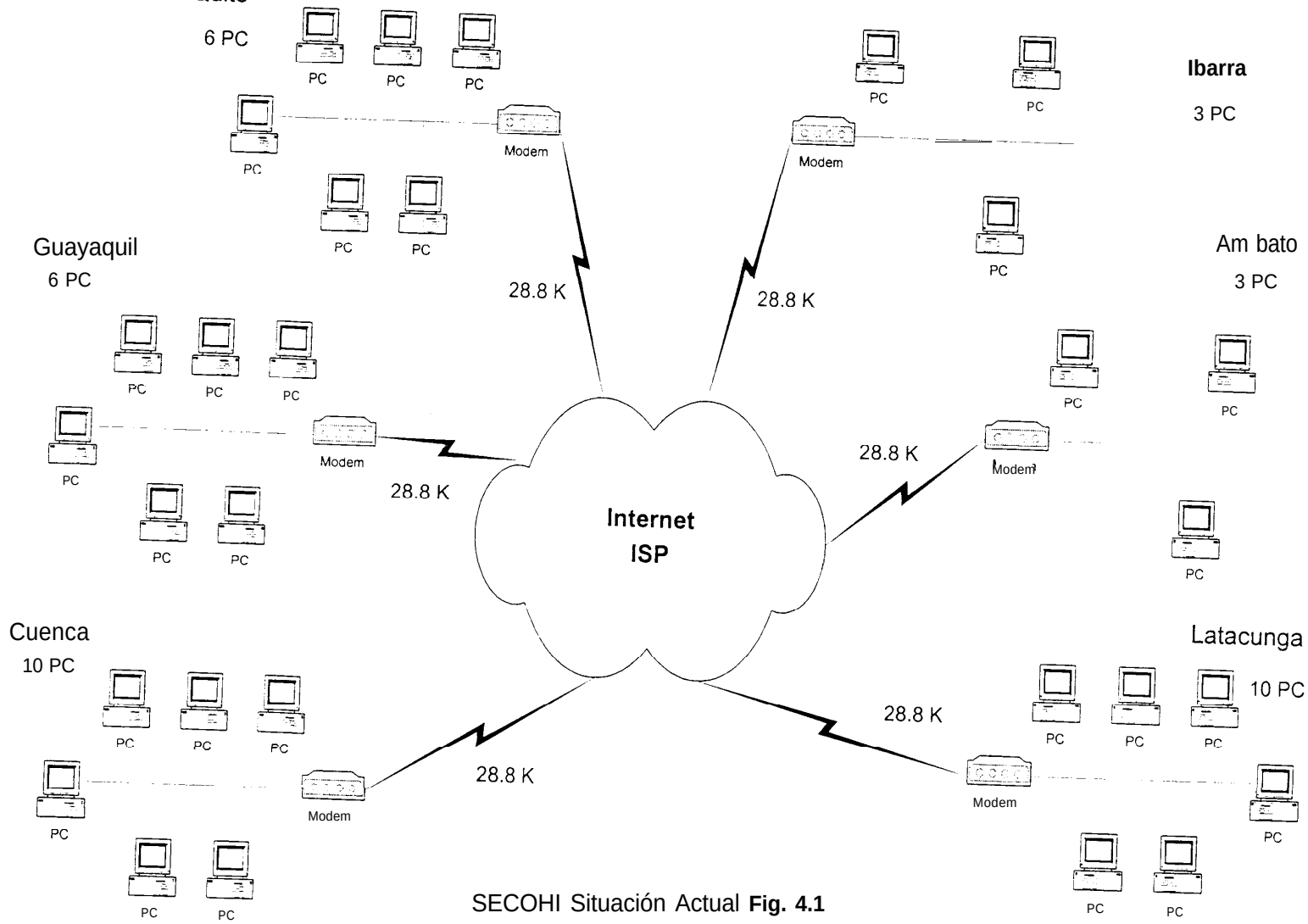
- Es fácil implementar un sistema de control del stock de mercancías.
- Es fácil implementar un sistema de control de asistencia del personal.
- Es fácil implementar un sistema que maneje los requerimientos de la matriz, resto de sucursales y usuarios remotos.
- Es fácil establecer un sistema de servicio al cliente.
- Es fácil implementar un sistema de facturación e información actualizada.

4.5. Solución de interconexión para SECOHI.

Ya expuesta la necesidad de interconexión de las oficinas SECOHI, vamos a proponer la solución que consolide la intranet:

- Tecnología VPN.

Nota: En el anexo G encontrarán dos soluciones adicionales, explicadas a breves rasgos con una tabla en la que se analizan los costos que conlleva implementarlas. Estas son: Contratación de backbone Frame Relay de empresa proveedora y contratación de enlaces satelitales. En el anexo H, se puede encontrar cuadros comparativos de costos a corto, mediano y largo plazo, en los que las VPNs destacan como la solución más económica.



SECOHI Situación Actual **Fig. 4.1**

4.5.1. Tecnología VPN.

4.5.1 .l . Análisis técnico.

A continuación se expone en detalle el diseño de la intranet para SECOHI utilizando tecnología VPN.

4.5.1.1.1 Ubicación geográfica de las sucursales de SECOHI.

Una vez claro el funcionamiento de SECOHI, y la opinión del cliente: consideraciones particulares y necesidades, lo primero es determinar la ubicación exacta de las sucursales. En la tabla 4.1. se expone un listado con las direcciones de las agencias.

Estas direcciones denotan una ubicación urbana y además, un enlace entre la oficina sucursal y el ISP a través del proveedor de última milla de tipo urbano, lo que permite conservar los costos de estos enlaces.

Tabla 4.1. Direcciones de las sucursales SECOHI.

Sucursal	Dirección
Latacunga (matriz)	Eloy Alfaro y Galarza
Ambato	Avda. Amazonas y Calandrias
Cuenca	Aeropuerto España y Gil Ramírez Dávalos
Ibarra	Avda. Cristóbal Troya 1059
Guayaquil	Avda. de las Américas frente al Aeropuerto
Quito	Avda. Maldonado 10038 al Norte de la ciudad

4.5.1 .1.2. Dimensionamiento de la red.

Para los enlaces entre las sucursales Guayaquil, Quito, Cuenca, Latacunga y el ISP respectivo, se contrata un ancho de banda para accesar a Internet de 32K de CIR con 64K de Burst. Esto asegura el ancho de banda de 32K cuando los demás clientes conectados al puerto del ruteador asignado estén transmitiendo, sino se aprovecha el enlace de 64K. Esta decisión toma en cuenta las posibilidades de expansión futura de estas sucursales y tiene la ventaja de disponer de mayor ancho de banda para transmitir en determinados momentos. Para los enlaces de las sucursales de Ambato e Ibarra es suficiente contratar un enlace de 32K/32K según con los requerimientos actuales.

Por las características técnicas del ruteador y consideraciones de carácter práctico proporcionadas por el proveedor del equipo, conocemos que se puede manejar una LAN de 10 PCs sin inconvenientes a través de un enlace de 32K hacia el Internet.

Para llegar a esta conclusión se consideró la capacidad de procesamiento y la memoria flash del Cisco 1720, teniendo presente que la encriptación al utilizar la opción 3 DES, consume aproximadamente el 25 % de los recursos del ruteador.

Tabla 4.2. Dimensionamiento del enlace de cada sucursal con su ISP local.

Sucursal	**Número de PCs**	**Enlace CIR/Burst**
Ambato	LAN NT- 3PC	32/32 K.
Cuenca	LAN NT-IOPC	32/64 K.
Guayaquil	LAN NT- 6PC	32/64 K.
Ibarra	LAN NT- 3PC	32/32 K.
Latacunga	LAN NT- 10 PC	32/64 K.
Quito	LAN NT- 6PC	32/64 K.

4.51 .1.3. Asignación de direcciones IP.

Debido a que la red de SECOHI requiere de la privacidad de una Intranet, se consideran las direcciones IP reservadas con dicho propósito específico. Siguiendo entonces con este esquema, se asigna a cada sucursal un segmento de red que la identifique (Ver tabla 4.3).

Tabla 4.3. Segmentos de direcciones no válidas para identificar cada LAN.

LAN	Direcciones de Red IP no válidas
Latacunga	192.168.1 .O
Quito	192.168.2.0
Cuenca	192.168.3.0
Guayaquil	192.168.4.0
Ambato	192.168.5.0
Ibarra	192.168.6.0

El proveedor de Internet, por su parte, asigna la dirección de subred que se muestra en la tabla 4.4.

Tabla 4.4. Dirección de subred y máscara asignada por ISP.

Dirección de subred	Máscara
216.219.56.160	**255.255.255.248**

Al contraponer la dirección de subred con la máscara en notación binaria, es fácil notar que disponemos de las tres últimas posiciones para conjugar la dirección de la red SECOHI, 6 direcciones válidas de Internet para cada LAN, y una dirección broadcast.

Tabla 4.5. Dirección de subred y máscara en notación binaria.

Dirección de subred	11011000 11011011 00111000 10100000
Máscara	11111111 11111111 11111111 11111000

En resumen, las direcciones se distribuyen tal muestra las tablas 4.6 y 4.7.

Tabla 4.6. Distribución de direcciones asignadas.

Dirección de red	216.219.56.160
Direcciones válidas en Internet	216.219.56.161 – 216.219.56.166
Dirección de broadcast	216.219.56.167

Tabla 4.7. Direcciones IP válidas asignadas a cada LAN.

LAN	**Direcciones IP válidas**
Am bato	216.219.56.165
Cuenca	216.219.56.163
Guayaquil	216.219.56.164
I barra	216.219.56.166
Latacunga	216.219.56.161
Quito	216.219.56.162

Estas direcciones se ubicarán en cada ruteador que conforma la VPN, de manera que cualquier requerimiento realizado por una PC dentro de la LAN utilice una de estas direcciones para enviar los datos encriptados a través del Internet.

En cada ruteador, se establece la tabla de traducción NAT que identifica cada sucursal con la dirección IP válida asignada al ruteador respectivo para salir al Internet. Para los usuarios remotos el ISP proporciona direcciones adicionales.

El número de IPs públicas se ubican en las tablas de NAT. Esto asegura la salida al Internet cuando una PC que pertenezca a la LAN haga un requerimiento.

4.5.1.1.4. Transmisión de información en una red VPN.

Suponga que se transmiten datos entre la PC1 de la sucursal Guayaquil, con IP 192.168.4.5, y la PC2 de la LAN Latacunga (matriz), con IP 192.168.1.8.

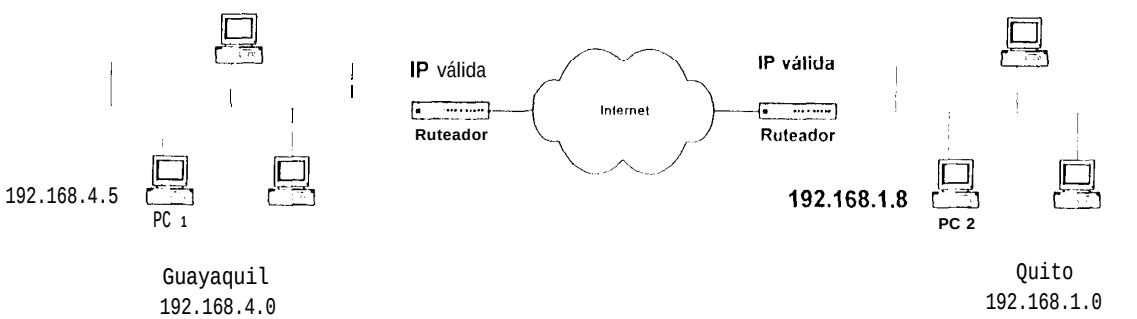


Figura 4.2. Transmisión de un paquete entre dos sucursales.

El paquete enviado por la PC1 al ruteador contiene, en forma general, la dirección IP origen, la destino y los datos. Vea la figura 4.3.

Figura 4.3. Paquete enviado por la PC1 al ruteador.

Cuando el requerimiento arriba al ruteador, las tablas de NAT realizan la traducción correspondiente, que depende del número de direcciones IP válidas asignadas.

Cuando se hayan definidas algunas direcciones IPS válidas, el ruteador asigna una de ellas al requerimiento de la PC1 para salir al Internet.

Si la IP pública es solo una para algunas máquinas de la LAN, caso que corresponde a nuestro diseño, entonces todas utilizan la misma IP para salir al Internet. Lo que diferencia la transmisión entre PCs es el puerto TCP que se le asigna aleatoriamente a cada transmisión.

Este rango de puertos TCP disponibles se los define con anterioridad, para este ejemplo van de 6000 a 7000.

Luego de usar las tablas NAT, el paquete sale del ruteador con el formato abreviado de la figura 4.4.

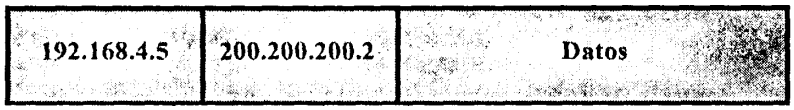


Figura 4.4. Direcciones IP del paquete que sale del ruteador.

Vamos a utilizar el protocolo IPSec para establecer los túneles encriptados entre los gateways de seguridad (ruteadores existentes). Por ello, habilitamos en el protocolo de seguridad el establecimiento de asociaciones seguras en modo túnel debido a que entre dos gateways de seguridad es necesario que exista siempre una asociación de seguridad de este tipo.

Configuramos al IPSec para utilizar los servicios de confidencialidad ESP debido a que este permite la utilización de un algoritmo de encriptación para la confidencialidad del tráfico. Provee también servicios de autentificación. Este servicio es negociado por un SA ESP. La cabecera externa IP no es protegida. Como se necesita autentificación solo para las capas superiores entonces la autentificación ESP es una buena elección. Utilizando entonces el modo túnel se puede encriptar la cabecera IP interna, ocultando de esta manera las identidades de la fuente y destino del tráfico. Si seleccionamos el ESP payload entonces podemos esconder el tamaño de los paquetes, de manera que se esconde también las características externas del tráfico.

Es necesario definir todos estos parámetros al realizar la configuración de los equipos, tanto para la comunicación entre gateways así como para el acceso de un usuario móvil que se conecta a la LAN estableciendo un SA ESP en modo túnel hacia un gateway corporativo.

Entonces, el paquete enviado por la LAN pasa por el ruteador, este a su vez se encarga de encriptarlo y verifica en la tabla establecida de asociaciones seguras los permisos necesarios para que el usuario en mención pueda acceder al equipo cuya dirección IP es la del destino del paquete. Solo si esto es posible, se establece una asociación segura y luego un túnel IPSec entre el origen y destino, por donde se envía el resto de la información.

Entonces el paquete quedaría aproximadamente de la siguiente manera:

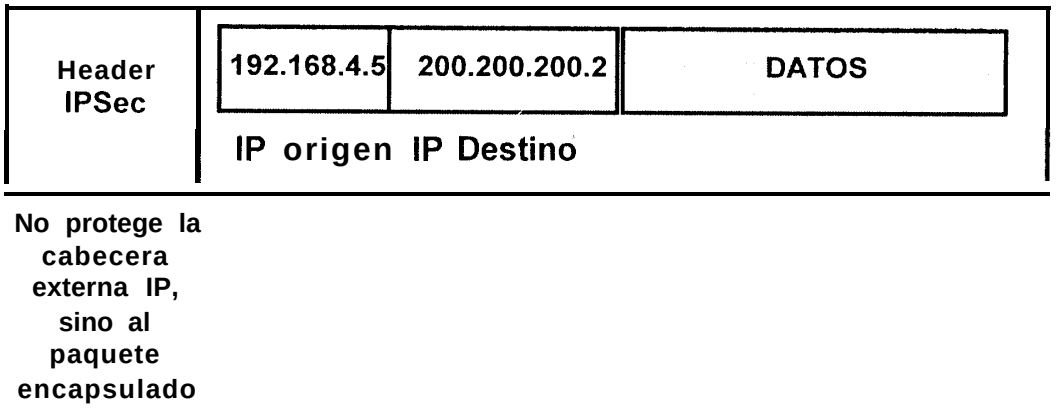


Figura 4.5. Paquete a enviarse.

Y pasa a encapsularse en el protocolo Frame Relay, y luego a través de la nube del proveedor de última milla llega al puerto de acceso al Internet, en el ISP, donde el paquete queda desencapsulado de Frame Relay para posteriormente ser enrutado al Internet.

Con un puerto TCP origen 6001 (que se encuentra dentro del rango definido) y un puerto destino por ejemplo 5000. Al terminar la transmisión de archivos entre sucursales, la relación entre la IP de la PC1 (origen) y el puerto TCP asignado se mantiene presente en el ruteador por aproximadamente 1 minuto, valor configurable por supuesto, para posibles envíos posteriores.

Adicionalmente en los ruteadores de nuestro ISP se deben establecer rutas estáticas entre cada uno de ellos y los ruteadores de nuestra red VPN, de manera tal que todo el tráfico de LAN dirigido a SECOHI se enrute de forma directa. De igual manera en cada ruteador de la VPN se debe especificar las correspondientes rutas estáticas hacia los ruteadores del ISP ingresando en la tabla de ruteo una línea con el siguiente formato.

Ejemplo: Sucursal Guayaquil.

0.0.0.0 (Toda dirección IP) 192.168.8.1 (Dirección WAN del puerto de acceso del ISP)

0.0.0.0 (Con cualquier máscara) 255.255.255.128 (Máscara del ruteador)

Es decir que todo requerimiento hacia cualquier dirección IP y con cualquier máscara se enruta por la dirección de enlace WAN (no válida) a través del proveedor de enlace última milla, hacia el puerto de acceso del ISP.

Las direcciones WAN asignadas al enlace de cada sucursal con el ISP se muestran en la tabla 4.8.

Tabla 4.8. Asignación de direcciones WAN a cada sucursal.

Sucursal	ISP	SECOHI
Latacunga	192.168.9.1	192.168.9.2
Quito	192.168.9.3	192.168.9.4
Cuenca	192.168.9.5	192.168.9.6
Guayaquil	192.168.9.7	192.168.9.8
Ambato	192.168.9.9	192.168.9.10
Ibarra	192.168.9.11	192.168.9.12

El enlace **última milla en las ciudades de Quito, Cuenca, Guayaquil y Ambato** se dará a través de la nube Frame Relay de un provedor local que llamaremos (A). Y el enlace de las sucursales Ibarra y Latacunga tendrá como proveedor, uno local llamado (B). Ambos accesos permiten llegar al ISP ubicado en Quito, Guayaquil y Cuenca.

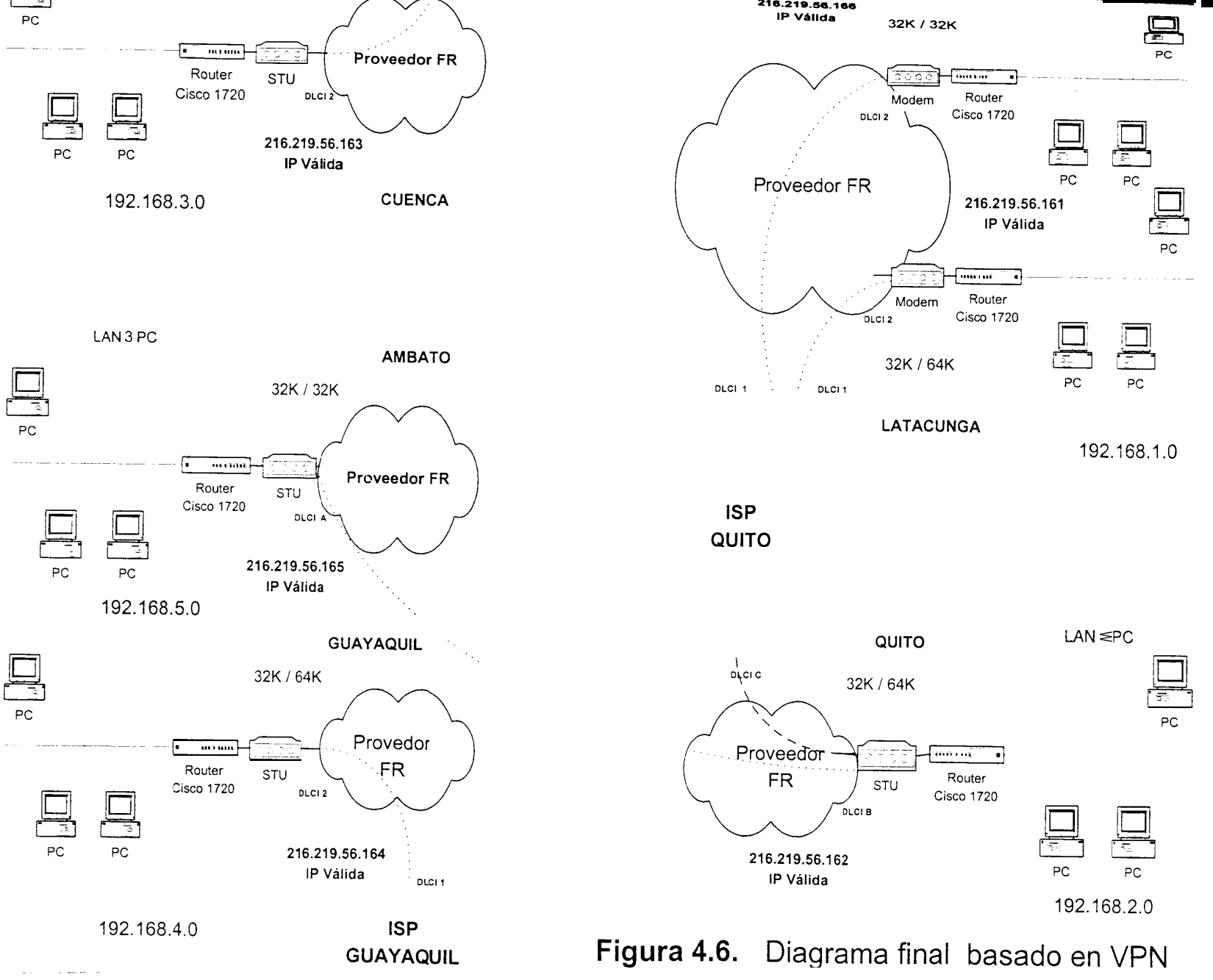


Figura 4.6. Diagrama final basado en VPN

4.5.1 .1.5. Implementación del acceso para usuarios remotos.

Básicamente, cuando un usuario remoto requiere conectarse a la intranet, éste debe accesar a un NAS (Network access ser-ver) de un ISP. El NAS se encarga de establecer un túnel encriptado hacia la red de la empresa. Además, permite a los usuarios conectarse a múltiples redes creando diferentes túneles.

Aquí diferenciamos dos tipos de acceso de usuarios remotos. El primero, que se muestra en la figura 4.7, se caracteriza por no encriptar la conexión entre el cliente remoto y el ISP y confiar en la seguridad de la Red de Telefonía Pública. En el segundo, figura 4.8, el cliente establece una conexión PPP con el NAS del ISP, luego, verifica la identidad del usuario y crea un túnel encriptado sobre la red Telefónica Pública. Para utilizar este segundo tipo de acceso se requiere que se instale el software "Cisco Secure VPN Client" en el NAS y la portátil desde la cual se quiere accesar.

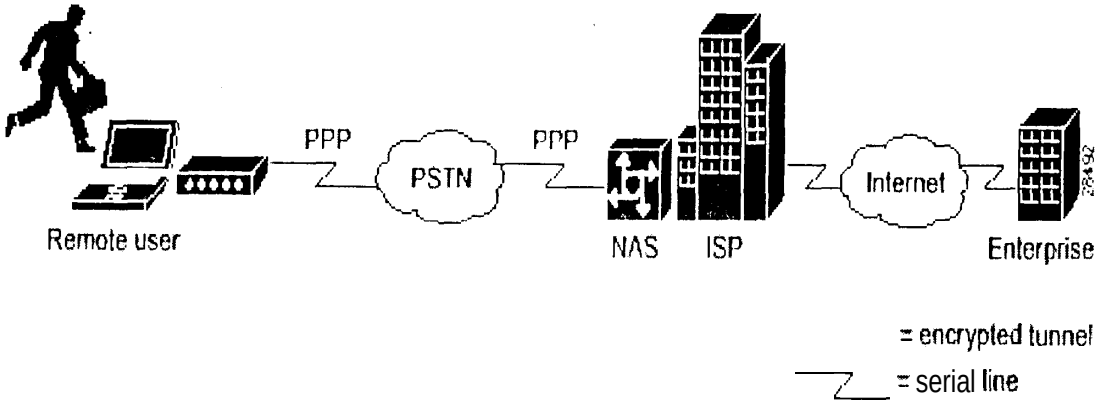


Figura 4.7. Alternativa A de acceso remoto de usuarios.

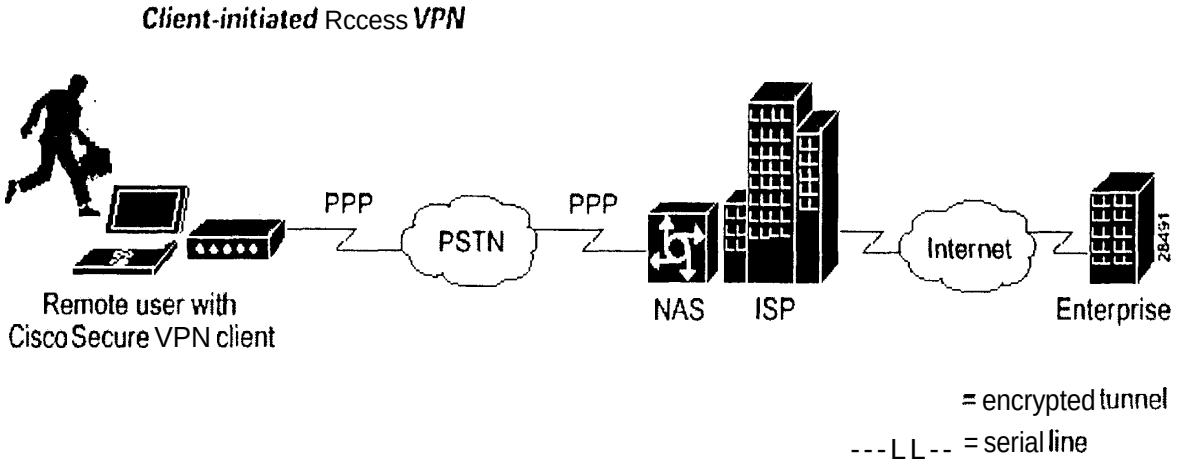


Figura 4.8. Alternativa B de acceso remoto de usuarios

Para el acceso de usuarios remotos a la red SECOHI utilizaremos la alternativa B que requiere de la instalación del software "Cisco Secure VPN Client" (Ver anexo D) en la PC del usuario remoto. La VPN en sí, transmite datos encriptados en forma segura sobre una red Pública. El software Cisco Secure VPN Cliente, entonces, establece túneles encriptados entre el cliente y un ruteador (empresa) utilizando direccionamiento IP estático o dinámico.

Además, Cisco Secure VPN Client con direccionamiento estático, da la opción de generar claves pre-compartidas para un túnel seguro entre el cliente y el ruteador CISCO. Las claves Pre-Compartidas son simples de implementar a pesar de no ofrecer tanta escalabilidad como los Certificados Digitales. Por esta razón, se recomiendan para redes pequeñas (hasta 10 clientes).

Para el caso de nuestro diseño, hemos escogido esta configuración debido al reducido tamaño de las sucursales y accesos remotos que maneja la red.

En la siguiente tabla se muestran los pro y contras de las claves precompartidas y los certificados digitales.

Tabla 4.9. Claves Pre-Compartidas Vs. Certificados Digitales.

Pre-shared Keys		Digital Certificates	
PROS	CONS	PROS	CONS
Claves precompartidas son comunes en redes pequeñas de hasta 10 clientes.	La red en menos escalable que con el otro sistema, los ruteadores deben ser reconfigurados con cada cliente adicional.	La red es más escalable, que con el otro sistema. Se pueden configurar un número ilimitado de clientes.	Los Certificados Digitales, pueden volverse complejos.
No es necesario Involucrar a una autoridad de Certificados CA.		Los Certificados Digitales permiten la autentificación de equipos y sobre todo una manera de autentificación más segura.	Es necesaria una Autoridad de Certificados externa.

4.5.1.1.5.1. Requerimientos para la instalación del software CISCO Secure VPN Client.

Para la instalación exitosa de este software que permite la creación de túneles encriptados desde el usuario remoto hasta el router de la compañía se necesita que tanto la PC del usuario como el NAS gocen de ciertas características que se detallan a continuación.

- Requerimientos de la PC del usuario remoto.
- Requerimientos del NAS (Network Access Ser-ver).

4.51 .1.5.1 .1. Requerimientos de la PC del usuario remoto.

La PC del usuario remoto debe reunir las siguientes características:

Computadora PC- Compatible – Procesador Pentium o equivalente.

Sistema Operativo- Uno de los siguientes:

- Microsoft Windows 98.
- Microsoft Windows 95.
- Microsoft Windows NT 4.0 (con Service Pack 3 o 4).

RAM Mínima- Depende del sistema operativo utilizado.

- 16MB RAM para Windows 95.
- 32 MB RAM para Windows 98.
- 32 MB RAM para Windows NT 4.0.

Espacio disponible en Disco Duro- Aproximadamente 9MB.

Para Instalación del Software- Drive CD-ROM.

Requerimientos de Interoperabilidad Cisco IOS Release 12.0(4)XE o últimos releases.

Protocolo de comunicaciones- TCP IP Nativo de Microsoft.

Conexiones Dial-up Módem, interno o externo, sin encriptación, o dialer nativo PPP.

Conexiones de Red- Ethernet.

4.51 .1.5.1.2. Requerimientos del NAS.

En el NAS, es necesario instalar y operar los ruteadores CISCO para la interoperabilidad del CISCO Secure VPN Client:

- Un ruteador CISCO serie 1700 (Recomendada para redes pequeñas).
- Que corra el Software image de CISCO Release 12.0(4)XE o últimos releases, incluyendo *Release* 12.0 (5) *T.*

451.2. Análisis financiero.

La tabla siguiente resume los costos de implementar una Intranet soportada en tecnología VPN alquilando los equipos requeridos para nuestro caso particular de estudio, SECOHI.

Tabla 4.10. Costo de Intranet VPN, alquilando los routers.

Tecnología VPN			
Acceso a Internet	Instalación* **	Servicio*	Costo mensual*
Sucursal GYE-ISP GYE	180.00	300.00	480.00
Sucursal UIO-ISP UIO	180.00	300.00	480.00
Sucursal Cuenca-ISP Cuenca	180.00	300.00	480.00
Sucursal Latacunga-ISP UIO	180.00	300.00	480.00
Subtotal Acceso a Internet			1,920.00
Acceso última milla	Derecho de inscripción* **	Servicio*	Costo mensual*
Guayaquil	51.60	120.00	171.60
Quito	51.60	120.00	171.60
Cuenca	51.60	120.00	171.60
Ambato - Quito	103.20	192.00	295.20
Ibarra - Latacunga	103.20	192.00	295.20
Latacunga - Quito	51.60	120.00	171.60
Subtotal última milla			1,276.80
Alquiler de equipos	Cantidad	Precio unitario*	Costo mensual*
Modems 9.2 a 128 Kbps	6.00	45.00	270.00
Router Cisco 1720	6.00	300.00	1,800.00
Subtotal alquiler equipos			2,070.00
**Software ** **	Cantidad	Precio unitario*	Total*
VPN client - usuarios remotos	1.00	870.00	870.00
Subtotal software			870.00
Total del primer mes			6,136.80
*Valor en dólares **Este valor se cancela una sola vez			
Costo mensual a partir del 2do mes			4134
Costo 1er año			$51,610.80
Costo a partir del 2do año			$49,608

Sin embargo, también se considera la opción compra de equipos para tener el servicio. La tabla siguiente resume los costos.

Tabla 4.11. Costo de implementación de intranet VPN comprando routers.

Alternativa considerando la compra de los Ruteadores	
Router CISCO 1720	1195
Tarieta Serial (1 Puerto WIC-1T)	400
Cable	100
Memoria FLASH	400
Memoria DRAM	**700**
	2795 Cada Router
Por 6 ruteadores **Total**	**$16,770**
Costo del enlace última milla y acceso a Internet	$4,336.80
Costo de los ruteadores	$16,770
Costo del primer mes	$21,107
Costo mensual de acceso a Internet	$2,334
Costo ler año	$46,781
Costo a partir del 2do año	$28,008

451.3. Ventajas de las redes VPN.

- Interoperabilidad entre distintos estándares de seguridad. En una economía actual toda empresa debe mantener una presencia extendida en un entorno económico cada vez más globalizado, para poder interactuar con múltiples empresas a nivel mundial.

- Tecnología menos costosa por utilizar enlaces existentes que brindan servicio de Internet, que como se sabe, es una red que se expande a nivel mundial, y, por este motivo, su crecimiento en nuestro país mejora la

cobertura a nivel nacional de cualquier intranet que quiera ser soportada sobre él.

- Flexibilidad y mayor rapidez en la integración de nuevas sucursales debido a que solo se requiere que se adquieran los equipos que se necesiten y se contrate el ancho de banda del acceso al Internet a través de un ISP. Importante es recalcar que la integración de esta sucursal no depende prioritariamente de la ubicación geográfica en sí.

- Los puntos remotos pueden llegar a conectarse a los proveedores del canal de comunicación (ISP) mediante sistemas como la red telefónica básica o la red digital de servicios Integrados, además de otros canales de coste fijo y mayor capacidad como enlaces Frame Relay, lineas dedicadas, etc. Lo que nos permite mezclar diferentes formas de acceso de acuerdo a las necesidades de cada sucursal o usuario remoto.

451.4. Desventajas de las redes VPN.

- Mala imagen del servicio de Internet, tanto por la seguridad de la información que viaja en él, como la de los enlaces administrados por los ISPs.

- Falta de un nuevo marco regulatorio en nuevas tecnologías, que den facilidades y garantías al usuario.

- Desconfianza en la confidencialidad de los datos, debida a los piratas del Internet.

Capítulo 5.

5. Conclusiones y recomendaciones.

Las redes privadas virtuales VPNs son una tecnología concebida para el ahorro de recursos, debido a que se basa en la utilización de infraestructura ya existente, el Internet, sin dejar de lado en ningún momento el aspecto de la confidencialidad de los datos que maneja. Entonces, se cumple a cabalidad el objetivo planteado al inicio del proyecto porque es factible utilizar una red de uso público como un medio para establecer enlaces privados seguros y disminuir así los costos de los mismos con enormes beneficios para la empresa que lo implemente.

- Se demuestra la necesidad de una interconexión permanente a través de VPNs para la mejor administración de cualquier empresa, más aún si los precios de sus productos están sujetos a cambios y las ventas son representativas en intervalos menores a un día, como es el caso de SECOHI.

Nuestro proyecto se fundamenta principalmente en el ahorro de recursos al realizar la implementación de una Intranet. Esto a su vez permitirá a las empresas que actualmente no cuentan con una red privada el considerar esta alternativa para de esta manera integrar todas sus sucursales, con las conocidas ventajas que una intranet trae consigo.

- La integración permanente de sus redes LAN's y la consecuente conexión a una única base de datos mejorará notablemente la calidad de servicio de la empresa en cuanto a atención al cliente, ya que la información de la empresa se actualizará instantáneamente y tendrá una mejor integridad,

En muchas ocasiones se presenta el hecho de la poca apertura a nueva tecnología. Pero desde todo punto de vista consideramos que es necesario formar parte de los avances tecnológicos para poder beneficiarnos de una tecnología moderna y actual.

Al momento de la investigación se puede concluir que las herramientas existentes sobre VPN están mejorando muy rápidamente, por lo que el diseño debe caracterizarse por su flexibilidad a nuevos cambios sin que esto implique gastos representativos, pero sí mejorando notablemente los servicios obtenidos.

- El desarrollo de esta nueva tecnología en nuestro país no está muy difundido, ni explotado por lo que es un excelente campo de trabajo.

- En los estudios financieros se demostró que la utilización de una VPN versus crear una red privada tradicional, ya sea sobre Frame Relay o enlaces satelitales dedicados, es mucho más conveniente en cuanto a costos. Por ejemplo, en los Estados Unidos la diferencia de costos presenta una relación de 10 a 1'.

En cuanto a la seguridad de la información a través de una red pública (Internet), gracias a los nuevos protocolos y técnicas de seguridad se llega a un grado alto de confiabilidad.

Es importante considerar las siguientes recomendaciones:

- Utilizar un software que permita monitorear el tráfico cursado a través del enlace al ISP y de esta manera comparar con los informes que el proveedor periódicamente entregue. Esto es necesario para tener la certeza de que el ancho de banda contratado es realmente el acordado al inicio. Se puede conseguir una versión de un software bastante útil al contactarse con el proveedor de los equipos.

Infonetics Research (The networking Information Source).
Check Point Software Technologies Ltd.

- Es necesario hacer un seguimiento a las horas de mayor tráfico para determinar momentos en los que se produzca congestión, y de esta manera poder preveer posibles ampliaciones del ancho de banda contratado.

- Utilizar la técnica de Claves Pre-Compartidas (CISCO) para la asignación de usuarios puesto que el tamaño de la red no justifica el uso de un servidor para otro tipo de asignaciones de claves, como certificados digitales, el costo de este tipo de implementaciones se justificaría en el caso de que la red crezca considerablemente. Los equipos utilizados en nuestro diseño son completamente flexibles a un upgrade de este tipo.

- En el caso de que nuestro cliente necesite la integración a la Intranet de una sucursal situada en el exterior, que es una necesidad a corto plazo, esta tecnología nos permite hacerlo con un mínimo de inversión adicional.

ANEXO A.

1. DES (Data Encryption Standard).

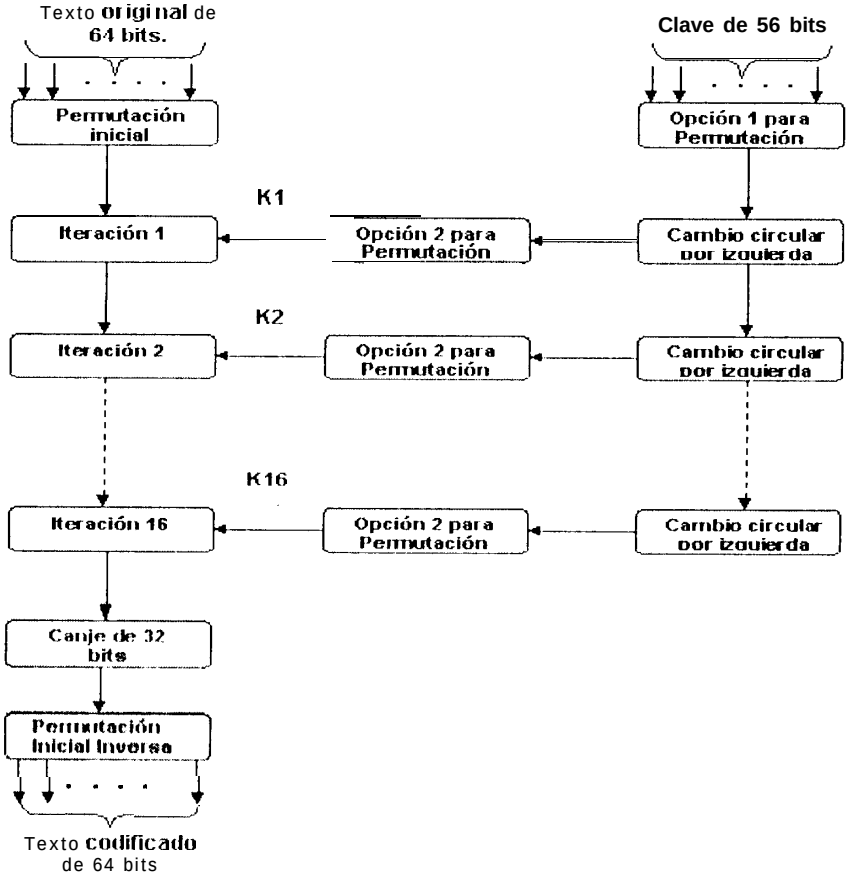


Figura A.1. Descripción general del DES.

El esquema de encriptación más utilizado se conoce como DES. Fue adoptado en 1977 por el NABU (National Bureau Standards), ahora el NIST (National Institute of Standars and Technology). La Figura A.l ilustra el esquema general de la encriptación DES.

Como la mayoría de estos esquemas, tiene dos entradas hacia la función de encriptación: el texto a ser encriptado y la clave. En este caso, el texto original debe tener 64 bits de longitud y la clave de 56 bits de longitud.

El procesamiento del texto original tiene 3 fases:

- Fase I: El bloque de texto de 64 bits pasa a través de una permutación inicial que reacondiciona el orden de los bits para producir una *entrada permutada(IP).*

- Fase II: La IP realiza 16 iteraciones de la misma función. La salida de la última iteración consiste de 64 bits, resultados de la función sobre la entrada del texto original y la clave. Las mitades izquierda y derecha de la salida son cambiadas de posición para producir el *preoutput.*

- Fase III: El preoutput pasa a través de una permutación (IP^{-1}), que es el inverso de la función de permutación inicial para producir un texto codificado de 64-bits.

La parte derecha del texto original, mostrado en la Figura A.l, señala la manera en que se usa la clave de 56 bits. En un principio, ésta pasa a través de una función de permutación y por cada iteración, se genera una clave (Ki) de la combinación de una entrada circular por la izquierda y una permutación. La función de permutación es la misma para cada iteración, pero una subclave diferente se produce por el cambio repetido de los bits de la clave. La Figura A.2 examina detenidamente dicho algoritrno para una iteración.

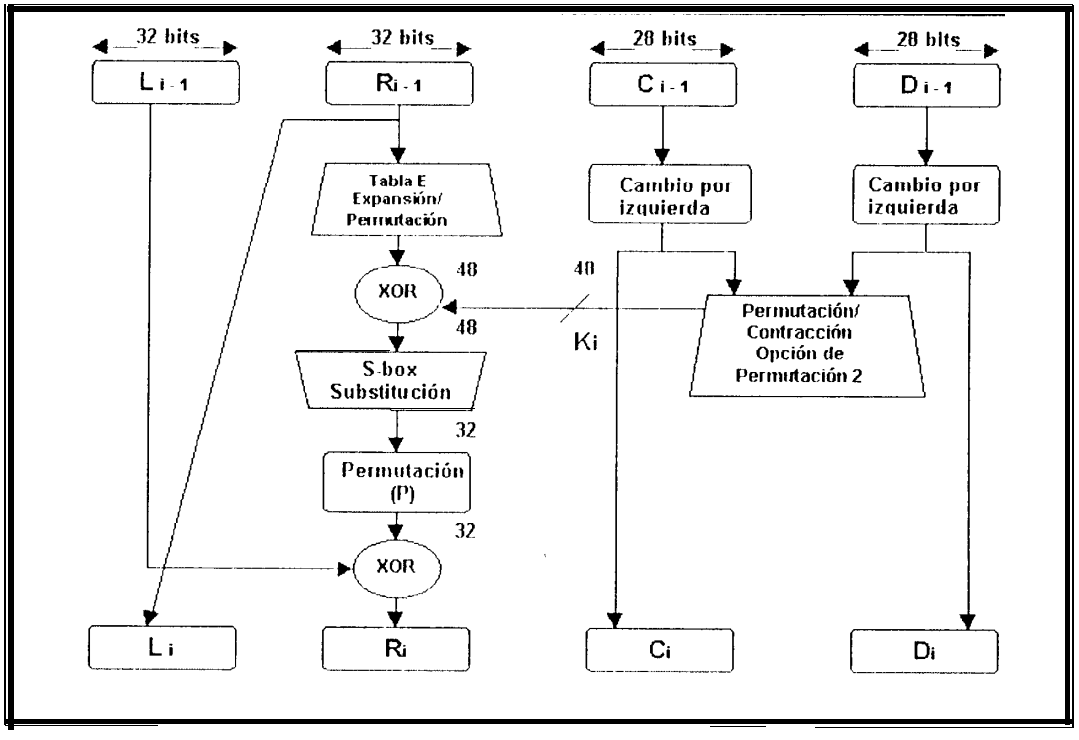


Figura A.2. Iteración única del algoritmo DES.

La entrada permutada de 64 bits iteraciona 16 veces, produciendo un valor intermedio de 64 bits a la conclusión de cada iteración. Las mitades derecha e izquierda de cada valor intermedio de 64 bits son consideradas como cantidades separadas 32 bits, llamadas L (izquierda) y R (derecha). La totalidad del proceso ocurrido en cada iteración puede ser resumido en las siguientes ecuaciones:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

Donde $\oplus$ denota la función lógica XOR.

Debido a esto la salida del lado izquierdo de una iteración L_i es simplemente igual a la entrada del lado derecho de la iteración R_{i-1}. La salida del lado derecho R_i es la operación or exclusivo de Li-1 y una función compleja f de R_{i-1} y K_i. Esta función compleja involucra ambas operaciones, como permutación y substitución. La operación de sustitución, es representada como tablas llamadas “S-boxes”, las que simplemente ubica cada combinación de 48 bits entrantes en un patrón particular de 32 bits.

Retornando a la Figura A.1, vemos que la clave de 56 bits, utilizada como entrada del algoritmo primero, es objeto de una permutación. La clave resultante de 56 bits se maneja como dos cantidades de 28 bits cada una, Co y

Do. En cada iteración se producen en C y D un cambio circular izquierdo de 1 o de 2 bits.

Estos valores cambiantes sirven como entrada para la siguiente iteración. También 'son utilizados como entrada para otra función de permutación, la que produce una salida de 48 bits que sirve luego como entrada para la función f **(Ri-1,** Ki).

El proceso de desencriptación del DES utiliza el mismo proceso de encriptación. Las reglas son: Utilizar el texto codificado como una entrada al algoritmo DES, designando las claves K_i en orden inverso. Esto significa que se usa K_{16} en la primera iteración, K_{15}, en la segunda, y así sucesivamente hasta que K_1 se use en la iteración décimo sexta.

2. Eficacia del DES.

Desde su adopción como estándar Federal, ha mantenido su posición por los niveles de seguridad que provee gracias a la naturaleza del algoritmo y el tamaño de la clave.

Durante algunos años, despertó un gran interés debido a la posibilidad de explotar las características del algoritmo DES para realizar análisis criptográfico. El enfoque principal se centra en 8 tablas de sustitución, o "S-boxes" que se

usan en cada iteración. Como el criterio del diseño para estas cajas, y en efecto para el algoritmo completo, nunca se han hechos públicos, existen sospechas de que dichas cajas se construyen de manera tal que el análisis criptográfico es posible para un atacante que conoce sus debilidades. A pesar de los avances en técnicas criptoanalíticas, la fortaleza principal del algoritmo DES se ha hecho más evidente. El interés más importante en la actualidad es el tamaño de la clave. Con una clave de longitud de 56 bits hay 2 exp 56 claves posibles, que aproximadamente son 7.7 X 10 exp 16 claves. Por este motivo un ataque tipo fuerza – bruta no es muy práctico. Asumiendo que se ha descubierto la mitad de una clave, una máquina que realiza una encriptación DES por microsegundo tomaría cientos de años en romper el código. Sin embargo el asumir que la máquina puede realizar una encriptación por microsegundo es una idea demasiado conservadora.

Existen análisis en la actualidad que demuestran que existen técnicas que permiten realizar búsquedas de mas de 50 millones de claves por segundo, aunque se debe considerar que el costo de estos equipo es directamente proporcional a la velocidad de procesamiento, podríamos hablar de valores mayores a $10.000.000.

3. Triple DES.

Esquema de encriptación propuesto en Julio de 1979 por W. Hellman Tuchman que presentó “No-Shortcut Solutions to DES IEEE Spectrum”. Se estandarizó para aplicaciones financieras. Utiliza dos claves y tres ejecuciones del algoritmo DES. Ver Figura A.3.

Su funcionamiento comprende una secuencia encriptar-desencriptar-encriptar (EDE).

$$C = E_{k1}(D_{k2} (E_{k1}(P)))$$

No hay un significado criptográfico para utilizar la desencriptación en la segunda etapa, pero sí la ventaja de permitir a usuarios Triple DES desencriptar datos encriptados por usuarios DES.

$$C = E_{k1}(D_{k1}(E_{k1}(P))) = E_{k1}(P)$$

Aunque solo se utilizan dos claves, se requiere emplear tres veces el algoritmo DES.

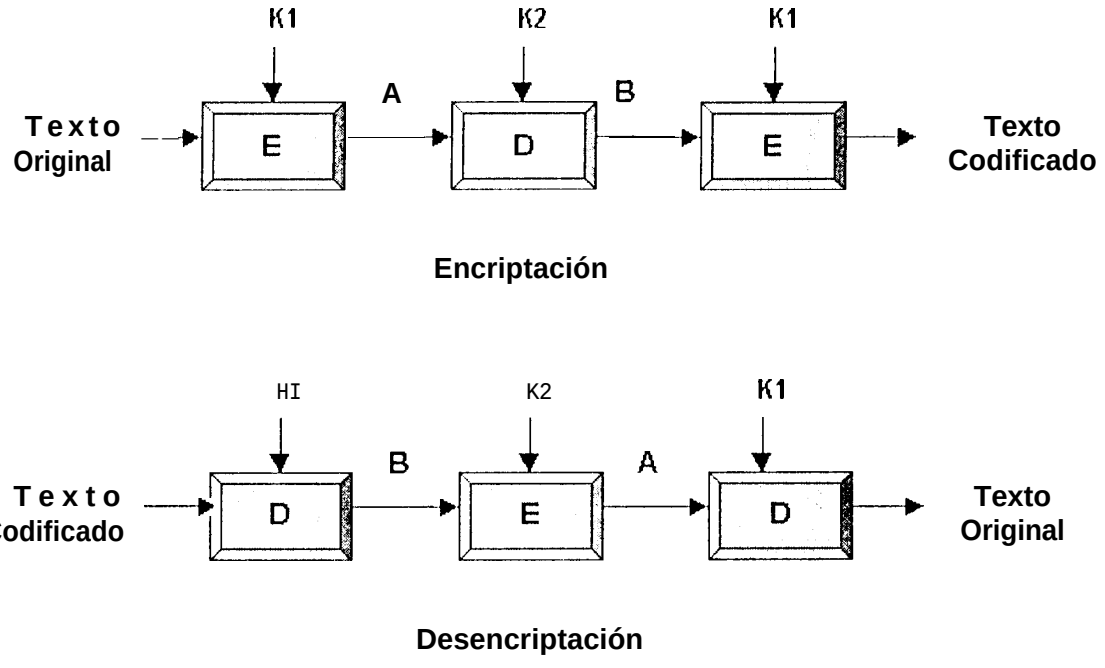


Figura A.3. Triple DES.

Existe una técnica simple conocida como meet-in-the-middle attack, que reduce un sistema doble DES con dos claves hacia la fortaleza ordinaria de una encriptación DES. Con tres iteraciones realizadas por la función DES, la longitud efectiva es 112 bits.

ANEXO B.

1. Configuración de una línea dedicada.

Los parámetros primordiales para configurar el ruteador son:

- Parámetros Globales.
- Seguridades.
- Configurando la Interface la interface Fast Ethernet.
- Interface Serial.
- Parámetros de Ruteo Dinámico.
- El acceso al ruteador a través de una linea de comandos.

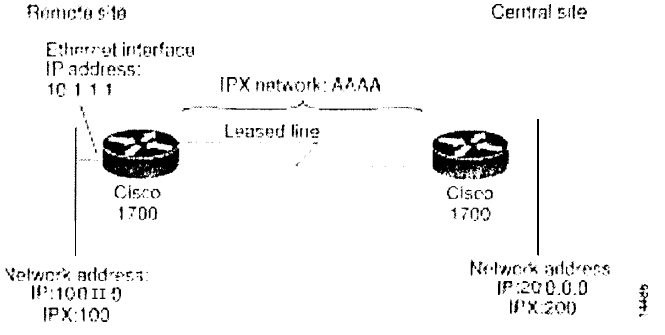


Figura B.1. Configuración de una línea dedicada.

2. Configuración de parámetros globales.

Esta tabla se utiliza para configurar parámetros generales del ruteador.

Tabla B.1. Configurando el ruteador.

Step	Task	Router Prompt	Command
1	Enter configuration mode.	Router#	**configure terminal**
2	Configure the router to show the date and time of all debug messages. This command is optional, but recommended if you use debug commands to troubleshoot your configuration.	Router(config)#	service timestamps debug datetime msec
3	Configure the router to show the date and time of all log messages. This command is optional, but recommended if you use the verification steps described in this guide. This feature is enabled for all the example command output shown in this guide.	Router(config)#	service timestamps log datetime msec
4	Configure the router to use subnet zero for interface addresses and routing updates.	Router(config)#	ip subnet-zero
5	Disable the IP Domain Name System (DNS)-based host name-to-address translation on the router.	Router(config)#	no ip domain-lookup
6	Enable IPX routing and configure the router with an IPX address.	Router(config)#	**Ipx routing** *0000.0caa.1111*

3. Configuración de seguridades.

La tabla a continuación configura medidas de seguridad en el ruteador.

Tabla B.2. Configurando seguridades en el ruteador.

Step	Task	Router Prompt	Command
1	Specify a password to prevent unauthorized access to the router.	Router(config)#	**Enable password** *<1700user>*
2	Configure the router with a host name, which is used in prompts and default configuration file narnes. For PPP authentication, the host name entered with this command must match the username of the central-site router.	Router(config)#	

4. Configuración de la Interfase Fast Ethernet.

La siguiente tabla configura la Interface Fast Ethernet que conecta el rutsador a la red local.

Tabla 8.3. Configurando la Interface Fast Ethernet.

Step	Task	Router Prompt	Command
1	Enter configuration mode for the Fast Ethernet interface.	1700(config)#	**interface fastethernet0**
2	Configure this interface with an IP address and a subnet mask. This interface must have an IP address assigned in order for the serial interface to be configured for IP *unnumbered* routing.	1700(config-if)#	**ip address** *10.1.1.1 255.0.0.0*
3	Enable IPX routing on this interface, assign the IPX network number, and configure the interface for IPX SAP encapsulation.	1700(config-if)#	**ipx network 100 encapsulation sap**
4	Configure a secondary IPX network on this interface that uses the default Netware encapsulation.	1700(config-if)#	**ipx network** *100* **encapsulation novell-ether secondary**
5	Enable the interface and the configuration changes you have just made on the interface.	1700(config-if)#	no shutdown
6	Exit configuration mode for this interface.	1700(config-if)#	**exit**

5. Configuración de la Interfase Serial.

Esta tabla permite configurar la interface serial, que conecta el ruteador al ruteador de la oficina Matriz.

Tabla B.4. Configurando la interface serial.

Step	Task	Router Prompt	Command
1	Enter configuration mode for the serial interface.	1700(config)#	**interface serial0**
2	Add a description of this interface to help you remember what is attached to it.	1700(config-if)#	**Description** *leased line to headquarters*
3	Enable IP routing on this interface without assigning an IP address.	1700(config if)#	**ip unnumbered FastEth0**
4	Enable IPX routing on this interface and assign an IPX network number.	1700(config-if)#	*ipx network* **AAAA**
5	Configure this interface for PPP encapsulation.	1700(config-if)#	**Encapsulation PPP**
6	Enable this interface and the configuration changes you have just made on the interface.	1700(config-if)#	no shutdown
7	Exit configuration mode for this interface.	1700(config-if)#	**Exit**

6. Configurando parámetros de ruteo dinámico.

Seteando los parámetros de esta tabla se configura el ruteo dinámico.

Tabla B.5. Configurando parámetros de ruteo dinámico.

Step	Task	Router Prompt	Command
1	Enable RIP routing on the router and enter router configuration mode.	1700(config)#	**router rip**
2	Specify the router to use RIP version 2.	1700(config-router)#	**version 2**
3	Enable Enhanced IGRP for this network.	1700(config-router)#	**network** *10.0.0.0*
4	Disable automatic summarization of subnet routes into network-level routes.	1700(config-router)#	**no auto-summary**
5	Configure the router to forward packets addressed to a subnet of a network with no network default route.	1700(config-router)#	**ip classless**
6	Exit router configuration mode.	1700(config-router)#	exit

7. Configuración de accesos al ruteador a través de líneas de comandos.

Tabla B.6. Configuración de accesos al routeador por líneas de comando.

Step	Task	Router Prompt	Command
1	Specify the console terminal line and enter line configuration mode.	1700(config)#	**Line console 0**
2	Set the interval that the EXEC command interpreter waits until user input is detected.	1700(config-line)#	**Exec-timeout 5**
3	Specify a virtual terminal for remote console access	1700(config-line)#	**line vty 0 4**
4	Specify a password on the line.	1700(config-line)#	**password** *<lineaccess>*
5	Enable password checking at terminal session login.	1700(config-line)#	**login**
6	Exit configuration mode.	1700(config-line)#	**end**

8. Verificando la configuración.

El buen funcionamiento lo determina la configuración de la interfase serial.

Paso **1:** Desde el modo de comandos privileged EXEC se ingresa el siguiente comando de Interface serial.

show interface serial 0

Paso 2: Para confirmar la interface serial, el mensaje que aparece a la salida del comando anterior es “Serial 0 is up, line protocol is up”.

```
1700# show interface ser0
Serial0 is up, line protocol is up
Hardware is PowerQUICC Serial
Description: leased line to headquarters
Interface is unnumhered. Using address of FastEthernet0 (10.1.1.1)
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Closed
```

Paso 3: Si se observa el mensaje mostrado, se ingresa nuevamente a la confguración por “global configuration mode”.

9. Troubleshooting Leased Line Problems.

La siguiente tabla describe problemas, posibles causas y, acciones sugeridas que se presentan comunmente con líneas dedicadas.

Tabla 8.7. Problemas comunes, causas y soluciones.

Line State	Possible Cause	Suggested Actions
Serial x is down, line protocol is down.	The router is not sensing a carrier detect (CD) signal due to one of the following reasons: . Telephone company problem, such as the line is down or not connected to the DSU/CSU. . Faulty or incorrect cabling of the router. . Local DSU/CSU hardware failure. . L ocal router hardware failure.	Following are some steps you can take to isolate the problem: . Check the LEDs on the external DSU/CSU for CD activity. • Refer to the Cisco ***1700*** *Router* Hardware *Installation Guide* to confirm that your router is correctly installed using the correct cables. . Contact the telephone company. • Connect the leased line to another port, if possible. If the connection come up, there is a hardware failure. Contact your Cisco reseller.

Serial x is up, line protocol is down.	Possible causes for this line state are . Local or remote router misconfigured. . The remote router is not sending keepalive packets. . Problem with the leased line. . The serial clock transmit external is not set on the DSU/CSU. . Local or remote DSU/CSU hardware failure. . Router hardware failure.	Following are some steps you can take to isolate the problem: • Perform DSU/CSU loopback tests. During local loopback, enter the **show interface ser0** command. If the line protocol is shown as up, there might be **a** problem with the telephone cornpany, or the rernote router is down. . Refer to the Cisco 1700 *Router Hardware Installation Guide* to confirm that your router is correctly installed using the correct cables. . Connect the leased line to another port, if possible. If the connection come up, there is a hardware failure. Contact your Cisco reseller.
Serial x is up, line protocol is up (looped).	The possible cause is that a loop exists in the circuit. The sequence number in the keepalive packet changes to a random number when a loop is first detected. If the same random nurnber is returned over the line, a loop exists.	Following are some steps you can take to isolate the problem: . Use the **write terminal** privileged EXEC command to display any instances of the loopback command. If the router has been configured with the loopback command, enter the no loopback command to remove the loop. . Check to see if the DSU/CSU is configured in manual loopback rnode. If it is, disable manual loopback. . Reset the DSU/CSU. . If you are unable to isolate the problem, contact the telephone company for help with troubleshooting.
Serial x is administratively down, line protocol is up.	The possible causes for this state are . The serial interface has been disabled with the **shutdown interface** configuration command. . Different interfaces on the router are using the same IP address.	Following are some steps you can take to isolate the problem: . Use the **show configuration** privileged EXEC command to display the serial port configuration. If "shutdown" is displayed after "interface Serial0," use the **no shutdown** interface configuration command to enable the interface. . Use the **show interface** privileged EXEC command to display the IP addresses for all router interfaces. Use the **ip address** interface configuration command to assign unique IP addresses to the router interfaces.

10. Chequeando la configuración.

- Verificar la conectividad hacia el Central Site-Router.
- Verificar el status de la interface serial.
- Verificar la configuración del enlace asincrónico. Confirming Connectivity to the Central-Site Router.

Paso 1: Ingrese desde el modo de comando privilegiado EXEC, el comando **ping** seguido por la dirección IP del central-site router.

Note The modem might need time to synchronize with the central-site modem. You might have to enter the **ping** command several times before you get a response.

```
1700# ping 192.168.37.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.37.40, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/43/48
ms
1700#
*Mar 1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
*Mar 1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
*Mar 1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Accessl,
changed state to up
*Mar 1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Accessl, changed state to up
*Mar 1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

Paso 2: Tome en cuenta el porcentaje de “Success rate..." (línea en negritas en el ejemplo anterior). Un valor de 60% (3/5) o mayor significa que el ruteador esta transfiriendo datos exitosamente hacia el central-site router.

Paso 3: La configuración continua re-ingresando al modo de configuración global.

II. Confirmando el estatus de la interfase serial.

Paso 1: Desde el modo de comando privilegiado EXEC, ingrese el comando **show interface serial 0 .**

Paso 2: Verifica que las lineas mostradas en negritas en el ejemplo siguiente aparezcan en la salida del comando.

```
1700# show interface serial0
Serial0 is up, line protocol is up
Hardware is PQUICC Serial in async mode (TTY1)
Internet address is 12.0.0.2/8
MTU 1500 bytes, BW 19 Kbit, DLY 100000 usec, rely 255/255, load
1/255
Encapsulation PPP, loopback not set, keepalive not set
DTR is pulsed for 5 seconds on reset
LCP Open
Listen: CDPCP
Open: IPCP
Last input 00:00:01, output 00:00:01, output hang never
Last clearing of "show interface" counters never
Input queue: 0/10/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
20 packets input, 1605 bytes, 0 nobuffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
4 input errors, 0 CRC, 4 frame, 0 overrun, 0 ignored, 0 abort
23 packets output, 2403 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

Paso 3: La configuración continua re-ingresando **al modo de configuración global.**

12. Confirmando la configuración de la línea asíncrona.

Paso 1: Dese el modo de comando privilegiado EXEC ingresar el comando show line 1.

La dirección IP **en el mensaje** "Line is **running" mostrada debe ser la dirección IP de la Interface WAN hacia el router central-** site.

```
1700# show line 1
Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns
A 1 TTY 19200/19200 - - - -- - 2 4 0/0

Line 1, Location: "", Type: ""
Length: 24 lines, Width : 80 columns
Baud rate (TX/RX) is 19200/19200, no parity, 1 ntopbits, 8 databits
Status: Ready, Active, Async Interface Active, HW PPP Support Active
Capabilities: Line is permanent async interface
Modem state: Ready
Line is running PPP for address 192.168.39.40
0 output packets queued, 0 input packets.
Async Escape map is 00000000000000000101000000000000
Modem hardware state: CTS DSR DTR RTS
Special Chars: Escape Hold Stop Star-t Disconnect Activation
^^x none - - none
```

13. **Configurando enlace backup (Marcado del ruteador).**

El ruteador se configura para saber cómo y cuándo marcar hacia el central-site router.

Tabla B.8. Configurando el marcado del ruteadorr.

Step	Task	Router Prompt	Command
1	Enter configuration mode for the serial interface.	1700(config)#	**interface Serial0**
2	Define a dialer map for snapshot routing.	1700(config)#	**dialer map snapshot** *1* **name** *HQ*
3	Configure a dialer map to send IP data over the modem line to the central-site router.	1700(config)#	dialer map ip 192.168.39.40 name *HQ* modem-script dialout *5552053*
4	Configure a dialer map to send IPX data over the modem line to the central-site router.	1700(config)#	dialer map ipx *9876.0000.0c06.ecc6* modem-script dialout *5552053*
5	Configure a route to IPX services, such as servers and printers, on the central-site network.	1700(config)#	ipx sap *4 HQ* server *AA 1234.0000.0000.000 1 2*
6	Exit configuration mode for this interface.	1700(config-if)#	**exit**

ANEXO C.

Datos técnicos de los equipos a utilizarse en la implementación del diseño.

1. CISCO 1720.

El ruteador CISCO 1720 de acceso modular provee una solución flexible e integrada para pequeñas oficinas sucursales y negocios de tamaño medio a pequeño que desean tener accesos tipo Intranet y Extranet hacia el Internet. Para que el diseño realizado tenga la posibilidad de realizar futuras ampliaciones desde un negocio de tamaño pequeño como una pequeña oficina sucursal hasta una sucursal de mayor capacidad, se debe diseñar la red con las siguientes características:

- Flexibilidad o adaptabilidad a los nuevos requerimientos que surjan en un futuro.
- Posibilidad de incorporar nuevos servicios WAN.
- Integrar múltiples funciones de red para simplificar las operaciones de desarrollo y administración.

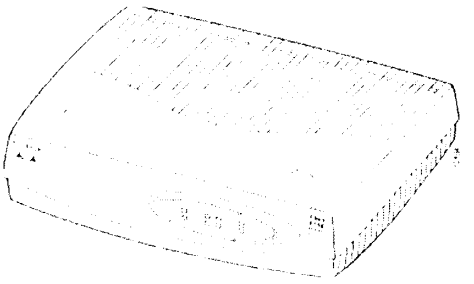


Figura C.1. CISCO 1720.

El Cisco 1720 ofrece los siguientes componentes:

- Un puerto con reconocimiento automático 10/100 Fast Ethernet LAN.
- Dos slots de tarjetas modulares que soportan un amplio arreglo de interfaces WAN.
- Un puerto de consola.
- Procesador RISC para encriptación de alto rendimiento.
- **Un slot de expansión interna para un módulo de encriptación basado en** hardware para VPN que permite mayores velocidades de transmisión.

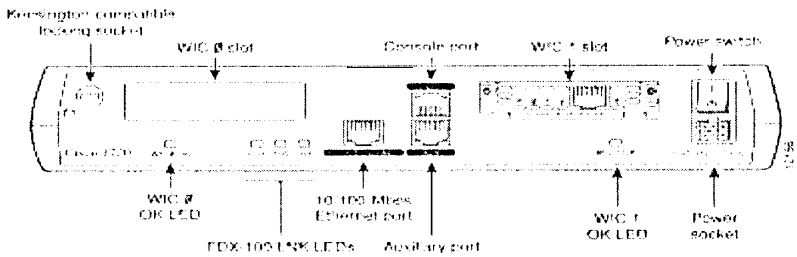


Figura C.2. Parte Posterior del CISCO 1720.

Adicionalmente soporta cualquier combinación de dos tarjetas de interface WAN siguientes:

- ISDN (Integrated Service Digital Network).
- Serial Asincrónica.
- Serial Sincrónica.
- Líneas Dedicadas.
- Frame Relay.
- Switch 56.
- x.25
- SMDS (Switched Multimegabit Data Service).

1.1. Memoria del ruteador.

El ruteador CISCO 1720 tiene los siguientes tipos de memoria.

- DRAM (Dinamic ramdom-access memory) Memoria de almacenamiento principal del ruteador, contiene información de configuración dinámica. El ruteador guarda una copia de trabajo del Software CISCO IOS, y la información de configuración dinárnica así como la información de la tabla de ruteo. Viene por default 16 MB expandible a 4, 8, 12, 32, 48 MB.

- NVRAM (Non-volatil random-access-memory) Contiene una copia de backup de la configuración presente en el ruteador. Si el suministro de energía se ve interrumpido por alguna razón, la copia de backup permite al ruteador volver a operación sin necesidad de reconfigurar el equipo.

- Memoria Flash Memoria de clase especial que, puede borrarse o programarse, contiene una copia del Software CISCO IOS. Su estructura permite almacenar múltiples copias de Software CISCO IOS. Hace posible cargar un nuevo nivel de sistema operativo en cada ruteador de la red y, cuando sea conveniente, actualizar toda la red a un nuevo nivel. La memoria flash es almacenada en módulos mini-flash. Viene por default 4MB expandible a 4, 8, 16 MB. Procesador: Motorola MPC860T PowerQUICC a 50 MHz.

1.2. **Especificaciones técnicas del equipo.**

Las siguientes tablas resumen las especificaciones técnicas para el CISCO 1720.

Tabla C.1. Especificaciones técnicas del equipo.

Descripción	Especificaciones
Puerto de Consola	RJ-45
Puerto Auxiliar	RJ-45
Puerto Ethernet	**RJ-45**
Dimensiones H x W x D	3.1 x ll .2 x 8.7 in. (7.85 x 28.4 x 22.1 cm)
Peso Con dos tarjetas de interface WAN	2.6 lbs. (1.18 kg.) 2.9 lbs. (1.32 kg.)
Suministro de Energía Externa On-board	Universal AC/DC switching --- Voltajes +5V, +12V, y -12V Voltajes de 3.3V y -5V
Consumo de Potencia	15W
(Especificaciones de Operación. Temperatura de Operación. Temperatura de almacenamiento. Niveles de Humedad	32 to 104° F (0° to 40°C) -4 to 149° F (-20° to 65°C) 10 to 85%, sin condensación.

Tabla C.2. Paquetes de seguridad para ruteadores Cisco 1700.

Paquete	Requerimientos
Firewall Package	Cisco 1700 Series IOS IP Firewall Software 16 to 20 MB DRAM Upgrade[1]
VPN Package	Cisco 1700 Series IOS IP Plus Firewall IPSec 3DES Software 16 to 32 MB DRAM Upgrade[1] 4 to 8 MB Flash Upgrade[1]
VPN Package including VPN Module	VPN Module for the Cisco 1700 Series Routers Cisco 1700 Series IOS IP Plus Firewall IPSec 3DES Software 16 to 32 MB DRAM Upgrade[1] 4 to 8 MB Flash Upgrade[1]

1. Satisface requerimientos de memoria para 12.1(1)T

1.3. Características del software CISCO IOS.

El ruteador Cisco 1720 con software Cisco IOS habilita un desarrollo VPN práctico a un costo razonable y de amplia escala. Este software soporta un amplio grupo de opciones básicas y avanzadas de seguridad de redes que incluyen listas de control de acceso (ACLs), autentificación de usuarios, autorización (como PAP/CHAP, TACACS+ y RADIUS) y encriptación de datos.

El firewall integrado Cisco IOS protege la LAN interna de ataques con control dinámico de acceso mientras el encapsulamiento IPSec con DES y encriptación 3DES provee estándares con miras a controlar el viaje de los datos a través de

una red pública, considerando aspectos como privacidad, integridad y autentificación de datos. L2F y L2TP, combinados con IPSec y encriptación, proporcionan una solución multiprotocolo (como IP, IPX, Appletalk y más) para acceso remoto a la VPN. Los usuarios móviles marcan a un POP de un ISP local y los datos son encapsulados (por ejemplo dentro de un segundo protocolo como lo es el L2TP) de regreso al ruteador Cisco 1720.

El módulo VPN opcional para la serie 1700 optimiza la plataforma para VPNs, encaja en un slot interno del Cisco 1720 y encripta los datos utilizando algoritmos DES y 3DES a velocidades confortables para una conexión serial full - dúplex T1/E1 (4 Mbits por segundo (Mbps) para paquetes de 1514 bytes). El módulo, junto a la plataforma, soporta cerca de 100 túneles encriptados (400 asociaciones de seguridad) para sesiones simultáneas con usuarios móviles u otros sites.

En nuestro diseño necesitamos instalar la siguiente opción de software en el router:

IP Plus IPSec 3 DES (SI 7CK2- 12.0.5T)

Con los siguientes requerimientos de memoria:

Memoria Flash: 4MB.

Memoria RAM: 20 MB.

El equipo viene con 16 MB de memoria RAM fijos por default en el equipo. Existe la posibilidad de realizar un upgrade a 20MB sin necesidad de instalar tarjetas adicionales. El código es el siguiente: MEM1 700 - 1 6U20D. La memoria Flash, si cumple con los requerimientos necesarios.

1.4. Protocolos que soporta.

Autentificación de usuarios.

- PAP/CHAP
- RADIUS
- TACACS+
- Token para verificar identidad de usuario.

1.5. Encapsulamiento IPSec, GRE, L2F, L2TP.

- Opciones de métodos de encapsulamiento basados en estándares para crear VPNs para tráfico IP y tráfico no IP.
- Permite utilizar cualquier estándar basado en IPSec o cliente L2TP para interoperar con tecnologías de encapsulamiento Cisco IOS.

1.6. Equipos CISCO necesarios para el diseño.

Para el diseño que proponemos son necesarios los siguientes equipos:

- Router Cisco 1720 1 0/100 Base T Modular Router w / 2 WAN slots
- Tarjeta Serial de interface WAN / 1 puerto (WIC – 1T).
- Un Upgrade de la Memoria DRAM de fábrica de 16MB a 20MB (MEM 1700 - 16U20D)
- Cable RS-232,DTE,Male, 10 Feet Para WIC – 1T (CAE3 – 232MT)

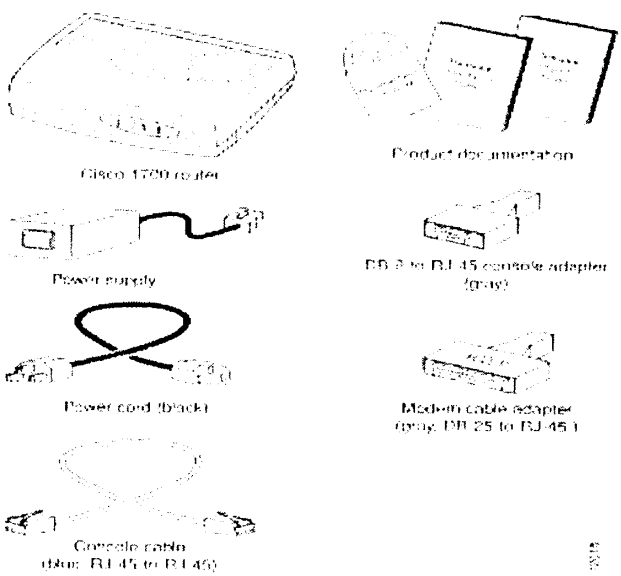


Figura C.3. Set CISCO 1720.

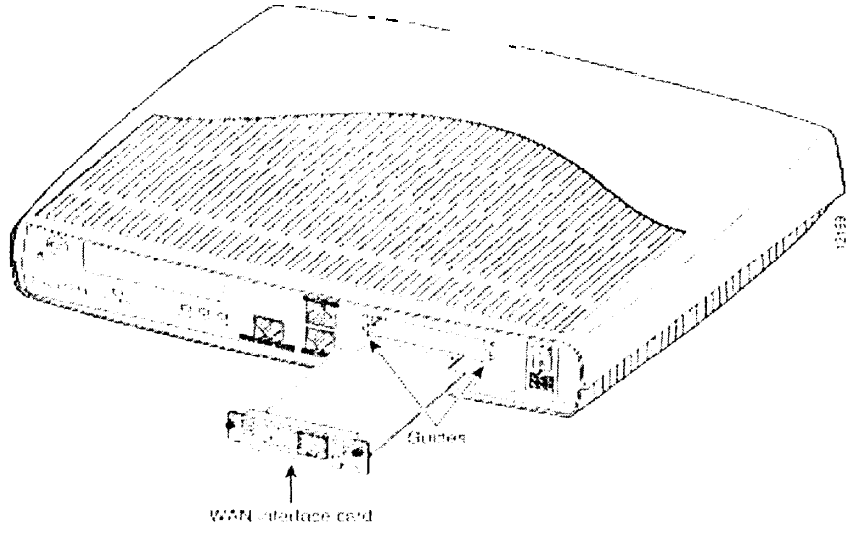


Figura C.4. Tarjeta de interfase WAN.

2. STU-160 baseband modetn.

El STU-160 baseband NTU (Network Terminal Unit) es un equipo diseñado para líneas dedicadas de enlaces de datos que utilizan circuitos físicos de 2-cables para velocidades que van desde 1,2 Kbit/s a 128 Kbit/s.

La unidad está equipada con 2 interfaces DTE independientes con una máxima velocidad de transmisión disponible de 128 Kbit/s.

Estas dos interfaces DTE están provistas de un conector hembra tipo D de 25 pines o de un conector rectangular hembra de 34 pines. Los conectores D son equipados con dos tornillos de seguridad de tipo UNC 4-40. El conector rectangular de 34 pines posee dos tornillos de seguridad tipo UNC 6-32.

Existen otras interfaces disponibles como: V.35, V.36, X.21, V.24/V.28 y 64 Kbit/s G.703, que pueden cambiarse sin necesidad de abrir el equipo.

El STU es un módem, que se utiliza con el Martis DXX Digital Multiplexing y el sistema Cross-Connect. En el otro lado del nodo Martis DXX el STU-160 es conectado a una unidad IUM localizada en el nodo Básico.

2.1. Información técnica.

DTE data rates: 1.2, 2.4, 4.8, 7.2, 9.6, 14.4, 19.2, 38.4, 4-8, 56, 64 y 128 Kbit/s

DTE rate adaptation. V. ll 0 / V. 110

Interfaces: **Adapter**	**IF Type**
VMI 370	V.35 sync (conector D-25 pines, ISO21 10)
VHI 371	V.36 sync (conector D-25 pines, ISO2110)
VHI 371	**X.21** sync (conector D-25 pines, ISO21 10)

Las interfaces V.36 y X.21 son implementadas con el mismo adaptador de interface (VHI 371). Las interfaces utilizan diferentes cables.

VLI 372	V.24 / V.28 sync / async (conector D-25 pines, iso 2110)

GMI 373	G.703 (64 Kbit/s, codir) (conector D-25 pines, iso 2110)
VMI 377	V.35 sync (conector de 34 pines, lSO2593)
XMI 378	X.21 sync (conector D-15 pines, ISO 4903)
EHI 392	LAN Bridge (Ethernet 10Base-2 y 10Base-T) (+MEM 393)

Voltaje de entrada: 230Vac,+6 / -15 %(hacia el adaptador AC/AC)

Frecuencia: 47... 63 Hz.

Consumo de Potencia: Menos de 10 VA con cualquiera de las unidades de Interface.

Indicador de Encendido: Led Verde.

Dimensiones: Ancho: 240 mm.

Profundidad: 290 mm.

Altura: 53 mm.

Peso: 2 Kg..

3. Newbridge 2703 Mainstreet.

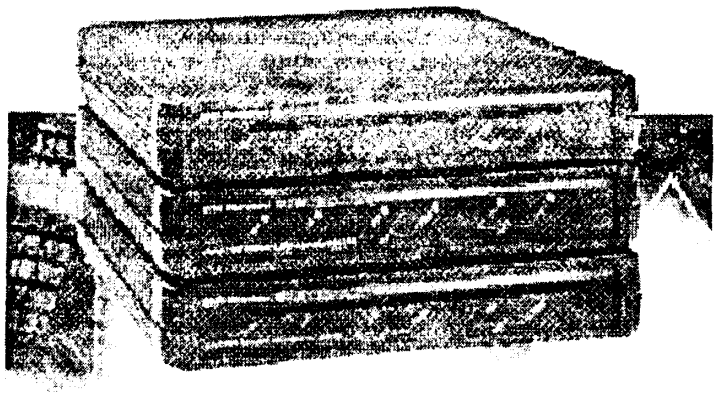


Figura C.5. NTU.

Es un Data Termination Unit (DTU) de ALCATEL que forma parte integral de una solución integrada de banda ancha, configurable de forma remota y con capacidad avanzada que le permite trabajar con enlaces xDSL que permite aprovechando al máximo las facilidades de los enlaces de cobre.

La familia de DTUs 2700 Mainstreet comprende rangos de operación extendidos que operan a distancias superiores a 7.2Km (4.5 Mi).

Las diferentes opciones incluyen el envío asincrónico de datos vía V.24 e incrementan las velocidades con interfaces V.35 y conexiones de redes

redundantes. La familia de DTUs aprovecha al máximo el ancho de banda y ofrece flexibilidad y administración a un mínimo costo.

Velocidad Máxima: 128Kbps.

Interface del puerto: **v.35 + v.35**

Soporta 6 circuitos por slot.

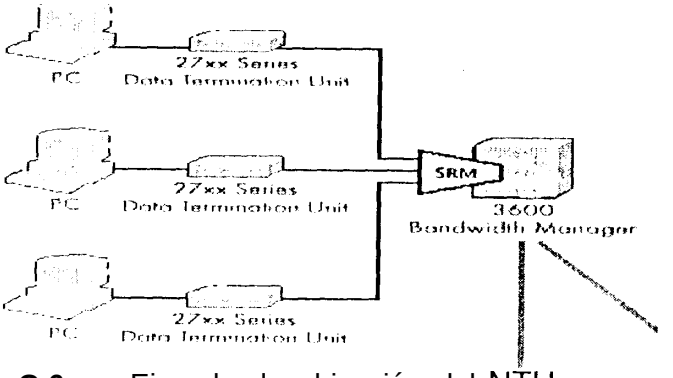


Figura C.6. Ejemplo de ubicación del NTU en una Red.

3.1. Especificaciones técnicas.

Puertos: Dual V.35.

Conectores: **v.35**

Interface Física: CCITT V.35 ISO 2593

Modo de operación: DTE/DCE

Soporta control de señales:	2.2(RTS, CTS, ALB, RDL, DCD, DSR, DTR, DTR, RI.)
Carácter de longitud variable:	9, 10, 11 (start, data, parity, stop bits).
Adaptaciones de velocidad:	CCITT V.110
Line Connections:	superior a 5.4 Km (3.4 Mi) utilizando cable 26 AWG
Conector:	RJ-45

Transmisión utilizando técnicas de supresión de ecos.

3.2. Especificaciones del sistema.

Software de sincronización seleccionable.

Software de data rate seleccionable.

Estadísticas de eficiencia de datos.

Autodiagnóstico automático.

Varios modos de reloj.

Dimensiones:	
Alto:	3.76 cm.
Ancho:	19.41 cm.
Profundidad:	26.67 cm.
Peso:	0.85 Kg.
Velocidades Sincrónicas:	hasta 128 Kb/s.
Velocidades Asincrónicas:	hasta 57.6 Kb/s.
Fuente de poder:	115VAC 60 Hz.
	230 V. AC 50 Hz.

Anexo D.

1. Conexiones.

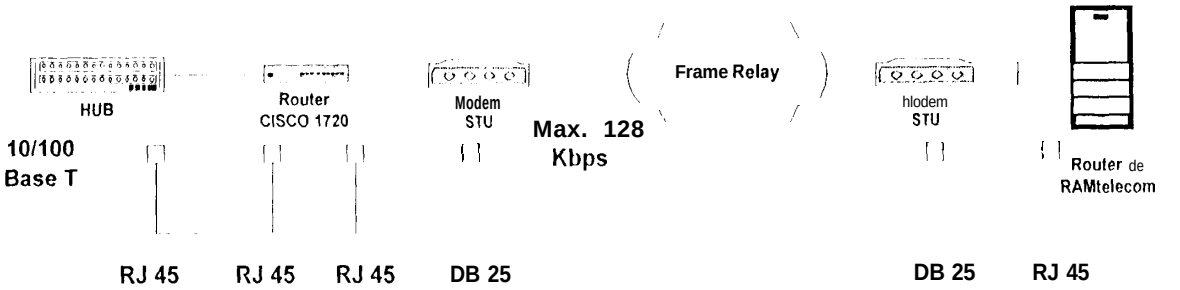


Figura D.1. Interconexión de los equipos utilizados en el diseño.

Como conexiones explicaremos las interfaces que se utilizan entre los enlaces Hub - Ruteador, Ruteador - Modern y Modem - Ruteador ISP.

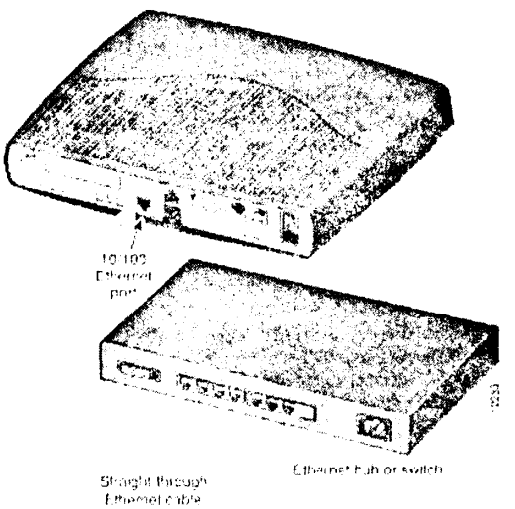


Figura D.2. Conexión del ruteador al hub.

El cable utilizado para conectar el router al Hub o concentrador local de LAN es una interfase punto a punto que en los extremos tiene conectores RJ-45 con el pinout de la Tabla D.l .

Tabla D.1. Pinout para conectores RJ 45 punto a punto.

# PIN	Descripción	Color
1	TX +	Blanco/Naranja
2	TX -	Naranja
3	RX +	Blanco/Verde
4		Azul
5		Blanco/Azul
6	RX -	Verde
7		Blanco/Café
8		Café

Entre el ruteador del ISP y el STU que utiliza el Proveedor de enlace última milla A, existe un cable de conexión punto a punto con interface V.35 y conectores DB-60 en el puerto del ruteador hacia un conector DB-25 male hacia el STU. El mismo cable se utiliza para la conexión con el DSU/CSU del Proveedor B última milla.

Tabla D.2. Pinout para conector DB-60 a DB-25.

EIA/TIA 232 DTE Cable Pinout (DB-60 to DB-25)

60 Pin	Signal	Description	Direction	25 Pin	Signal
J1-50 J1-51 J1-52	MODE_0 GND MODE_DCE	Shorting group	-	-	-
J1-46	Shield GND	Single	-	J2-1	Shield GND
J1-41 Shield	TxD/RxD -	Twisted pair no. 5	-->| -	J2-2 Shield	TxD -
J1-36 Shield	RxD/TxD -	Twisted pair no. 9	<--	-	J2-3 Shield	RxD -
J1-42 Shield	RTS/CTS -	Twisted pair no. 4	-->| -	J2-4 Shield	RTS -
J1-35 Shield	CTS/RTS -	Twisted pair no. 10	<--	-	J2-5 Shield	CTS -
J1-34 Shield	DSR/DTR -	Twisted pair no. 11	<--	-	J2-6 Shield	DSR -
J-45 Shield	Circuit GND -	Twisted pair no. 1	-	-	J2-7 Shield	Circuit GND -
J1-33 Shield	DCD/LL -	Twisted pair no. 12	<--	-	J2-8 Shield	DCD -
J1-37 Shield	TxC/NIL -	Twisted pair no. 8	<--	-	J2-15 Shield	TxC -
J1-38 Shield	RxC/TxCE -	Twisted pair no. 7	<--	-	J2-17 Shield	RxC -
J1-44 Shield	LL/DCD -	Twisted pair no. 2	-->| -	J2-18 Shield	LTST -
J1-43 Shield	DTR/DSR -	Twisted pair no. 3	-->| -	J2-20 Shield	DTR -
J1-39 Shield	TxCE/TxC -	Twisted pair no. 6	-->| -	J2-24 Shield	TxCE -

Arrows indicate signal direction: --> indicates DTE to DCE, and <-- indicates DCE to DTE.

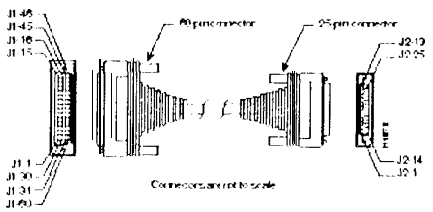


Figura D.3. Conectores DB60 y DB25.

ANEXO E.

Características del software CISCO utilizado en el diseño.

1. El Cisco Secure VPN Client.

Componente software que permite a un usuario final crear un túnel encriptado, utilizando IPSec y/o IKE hacia un sitio remoto para establecer una comunicación tipo extranet.

La tecnología de encriptación IP Security Protocol (IPSec), es parte de IETF, es ampliamente aceptada a nivel Industrial. Internet Key Exchange (IKE) es un protocolo híbrido con herramientas como el Oakley Key Exchange y el Skeme Key Exchange dentro del Internet Security Association and Key Management Protocol (ISAKMP), protocolos antes nombrados con herramientas utilizadas por IKE.

IPSec puede ser configurado sin IKE aunque el lo mejora y le proporciona presentaciones adicionales, flexibilidad y facilidad de configuración. Los ruteadores CISCO establecen, utilizando el IPSec, túneles encriptados entre ruteadores CISCO. El Software Cisco Secure VPN Client permite realizar las siguientes operaciones desde la comodidad de un escritorio.

- Generar una llave Pública/Privada.
- Obtener un Certificado Digital.
- Establecer una Política de Seguridades.

Crea una comunicación segura Cliente - Servidor sobre una red de capa 3 IP, tal como lo es el Internet.

En esta alternativa que se presenta al ruteador con el CISCO IOS IPSec habilitado, que va a actuar como un servidor, mientras el software CISCO Secure VPN Client realiza las tareas del Cliente.

1 .I. Interoperabilidad con ruteadores CISCO.

Es necesario utilizar ruteadores CISCO basados en VPN, aunque el software también puede interoperar con cualquier ruteador CISCO que soporte IPSec.
Para un óptimo funcionamiento, se recomiendan los siguientes modelos de ruteadores CISCO:

- Cisco 7100 VPN ruteador para empresas grandes.
- Cisco 2600 o serie Cisco 3600 para empresas de tamaño mediano.
- Cisco 1720 VPN ruteadores para empresas pequeñas.

1.2. Configuraciones que soporta.

Cisco soporta la utilización de Cisco Secure VPN Client con el IPSec y los protocolos de seguridad IKE. Para interoperabilidad entre el ruteador y el software, CISCO soporta las siguientes configuraciones:

- Direccionamiento IP Estático o Dinámico para el cliente con Claves Pre-Compartidas.
- Direccionamiento IP Estático o Dinámico para el cliente con Certificados Digitales.
- Direccionamiento IP Dinámico de Clientes con el Modo IKE de configuración.

ANEXO F

1. Descripción de los enlaces de última milla.

Las características más relevantes consideradas al elegir un enlace de última milla específico son:

- Velocidad de transmisión que permite alcanzar.
- Distancia que existe entre los puntos que se comunican.
- Nivel de ruido e interferencias.

Se pueden diferenciar dos grupos de enlaces última milla:

- Medios alámbricos.
- Medios inalámbricos.

1.1. Medios alám bricos.

1 .1.1 . Enlace dedicado.

Se trata de dos hilos de cobre aislados y trenzados entre sí, y en la mayoría de los casos cubiertos por una malla protectora. Los hilos trenzados reducen las interferencias electromagnéticas con respecto a los pares cercanos (dos pares paralelos constituyen una antena simple, un par trenzado, no).

Se utilizan para transmisión analógica y digital. Su ancho de banda depende de la sección de cobre usado y de la distancia que recorre.

Es el tipo de cableado más económico y utilizado, en especial en la red telefónica. Su velocidad de transmisión depende del tipo de cable de par trenzado empleado, el cual se clasifica por EIA/TIA en tres categorías:

- **Categoría 1:** Hilo telefónico trenzado de calidad de voz no adecuado para transmisiones de datos. Velocidad de transmisión inferior a 1 Mbits/seg.
- **Categoría** 2: Cable de par trenzado sin apantallar. Su velocidad de transmisión es de hasta 4 Mbits/seg.
- **Categoría** 3: Velocidad de transmisión de 10 Mbits/seg. Con este tipo de cables se implementa las redes Ethernet 10-Base-T

- **Categoría** 4: La velocidad de transmisión llega a 16 bits/seg.

- **Categoría** 5: Puede transmitir datos hasta 100 Mbits/seg.

Tiene una longitud máxima limitada y, a pesar de los aspectos negativos, es una opción a tener en cuenta debido a que ya se encuentra instalado en muchos edificios como cable telefónico y esto permite utilizarlo sin necesidad de obra.

La mayoría de las mangueras de cable de par trenzado contiene más de un par de hilos por lo que es posible encontrar mangueras ya instaladas con algún par de hilos sin utilizarse. Además resulta fácil de combinar con otros tipos de cables para la extensión de redes.

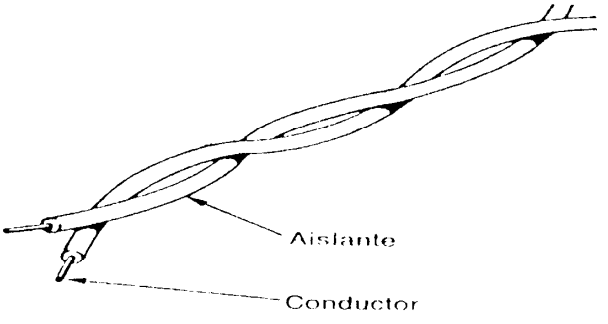


Figura F.1. Cable de par trenzado.

1.1.2. Enlace de fibra óptica.

Una fibra óptica es un medio de transmisión de la luz que consiste básicamente en dos cilindros coaxiales de vidrios transparentes y de diámetros muy pequeños. El cilindro interior se denomina núcleo y el exterior se denomina envoltura, siendo el índice de refracción del núcleo algo mayor que el de la envoltura.

En la superficie de separación entre el núcleo y la envoltura se produce el fenómeno de reflexión total de la luz, al pasar éste de un medio a otro que tiene un índice de refracción más pequeño. Corno consecuencia de esta estructura óptica todos los rayos de luz que se reflejan totalmente en dicha superficie se transmiten guiados a lo largo del núcleo de la fibra.

Este conjunto está envuelto por una capa protectora. La velocidad de transmisión es muy alta, 10 Mb/seg siendo en algunas instalaciones especiales de hasta 500 Mb/seg, y no resulta afectado por interferencias.

Los cables de fibra óptica ofrecen muchas ventajas respecto de los cables eléctricos para transmitir datos:

- Mayor velocidad de transmisión. Las señales recorren los cables de fibra óptica a la velocidad de la luz (c = 3 X 10^9 m/s), mientras que las señales eléctricas recorren los cables a una velocidad entre el 50 y el 80 por cien de ésta, según el tipo de cable.

- Mayor capacidad de transmisión. Pueden lograrse velocidades por encima de 1 Gbit/s.

- Inmunidad total ante interferencias electromagnéticas. La fibra óptica no produce ningún tipo de interferencia electromagnética y no se ve afectada por rayos o por pulsos electromagnéticos nucleares (NEMP) que acompañan a las explosiones nucleares.

- No existen problemas de retorno de tierra, crosstalk o reflexiones como ocurre en las líneas de transmisión eléctricas.

- La atenuación aumenta con la distancia más lentamente que en el caso de los cables eléctricos, lo que permite mayores distancias entre repetidores.

- Se consiguen tasas de error típicas del orden de 1 en 10^9 frente a las tasas del orden de 1 en 10^6 que alcanzan los cables coaxiales. Esto permite aumentar la velocidad eficaz de transmisión de datos, reduciendo el número

de retransmisiones o la cantidad de información redundante necesaria para detectar y corregir lo errores de transmisión.

- No existe riesgo de cortocircuito o daños de origen eléctrico.
- Los cables de fibra óptica pesan la décima parte que los cables de corte apantallados. Esta es una consideración de importancia en barcos y aviones.
- Los cables de fibra óptica son generalmente de menor diámetro, más flexibles y más fáciles de instalar que los cables eléctricos.
- Los cables de fibra óptica son apropiados para utilizar en una amplia gama de temperaturas.
- Es más difícil realizar escuchas sobre cables de fibra óptica que sobre cables eléctricos. Es necesario cortar la fibra para detectar los datos transmitidos. Las escuchas sobre fibra óptica pueden detectarse fácilmente utilizando un reflectómetro en el dominio del tiempo o midiendo las pérdidas de señal.
- Se puede incrementar la capacidad de transmisión de datos añadiendo nuevos canales que utilicen longitudes de onda distintas de las ya empleadas.

- La fibra óptica presenta una mayor resistencia a los ambientes y líquidos corrosivos que los cables eléctricos.

- Las materias primas para fabricar vidrio son abundantes y se espera que los costos se reduzcan a un nivel similar al de los cables metálicos.

- La vida media operacional y el tiempo medio entre fallos de un cable de fibra óptica son superiores a los de un cable eléctrico.

- Los costos de instalación y mantenimiento para grandes y medias distancias son menores que los que se derivan de las íktalaciones de cables eléctricos.

La mayor desventaja es que no se puede “pinchar” fácilmente este cable para conectar un nuevo nodo a la red. Las transmisiones de la señal a grandes distancias se encuentran sujetas a atenuación lo que limita la longitud del cable. Los segmentos pueden ser de hasta 2000 metros.

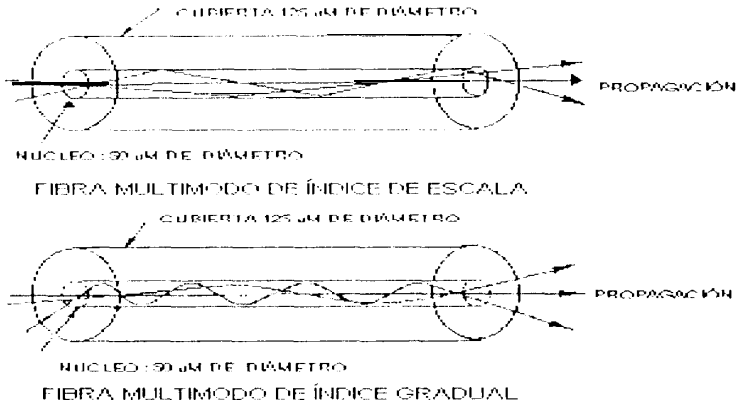


Figura F.2. Propagación multimodo en una fibra óptica de índice de escala y de índice gradual.

1.2. Medios inalámbricos.

1.2.1. Señales de radio.

Consiste en la emisión/recepción de una señal de radio, por lo tanto el emisor y el receptor deben sintonizar la misma frecuencia. La emisión puede traspasar muros y no es necesario la visión directa de emisor y receptor.

La velocidad de transmisión suele ser baja: 4800 Kbits/seg. Se debe tener cuidado con las interferencias de otras señales.

Anexo G.

Tecnologías alternativas para VPNs.

1. Contratación de Backbone Frame Relay de empresa proveedora.

Es factible interconectar cada una de las sucursales SECOHI mediante la contratación del Backbone de una empresa proveedora a la que denominaremos (C), la misma que debe poseer una red de microondas que enlace las ciudades más importantes del país y ofrezca servicios de transmisión de datos, Internet y telefonía móvil usando dicha red.

1 .1 . Características técnicas.

El backbone de la empresa proveedora (C) está conformado por microondas de diferente capacidad. Para tecnología PDH, las capacidades típicas son 4E1, 8E1 y 16E1 y, para tecnología SDH, 64 El. Cada enlace El maneja un flujo de 2048 Kbps dividido en 30 time slot de 64 Kbps y puede manejar voz y datos. Adicionalmente, posee 2 time slot mas: uno para sincronizar la trama y otro para señalizarla. En total, un enlace El posee 32 time slot de 64 Kbps cada uno.

Las necesidades de los usuarios determinan se enlacen varias microondas, creando así carriers de datos de una ciudad a otra. Cuando se transmiten

datos surge el requerimiento de un equipo complementario que maneja flujos de datos a nivel de time slot, tal cual lo hacen las microondas a nivel de El.

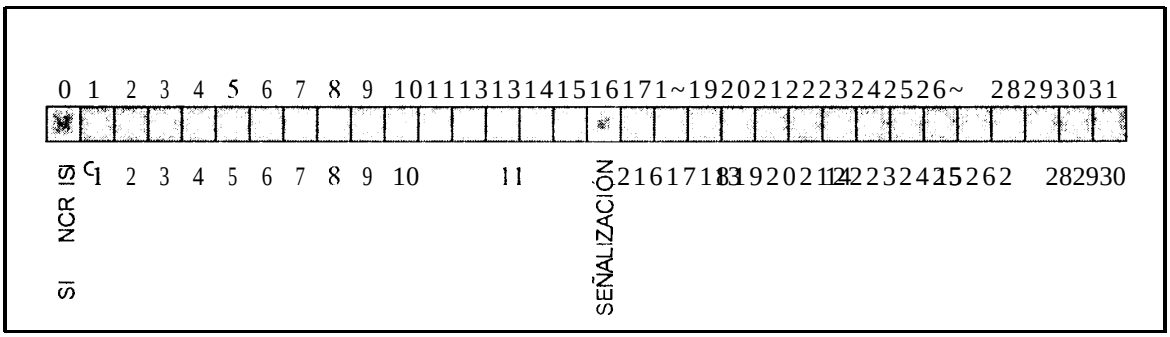


Figura G.1. Time slots de una El.

El equipo usado por el proveedor, Newbridge 9600, permite multiplexar, demultiplexar, configurar conexiones (entre microondas) y otras aplicaciones adicionales. Este dispositivo permite además configurar la distribución de time slot e interconectar El según la capacidad de transmisión solicitada por el usuario.

El manejo de los canales distribuidos se hace por medio de puertos V.35 (tarjeta V.35) y DTU (tarjeta DNIC), que establecen conexiones con los enlaces de última milla (V. Anexo E).

La figura G.2 muestra un detalle del bacltbone de la empresa proveedora (C).

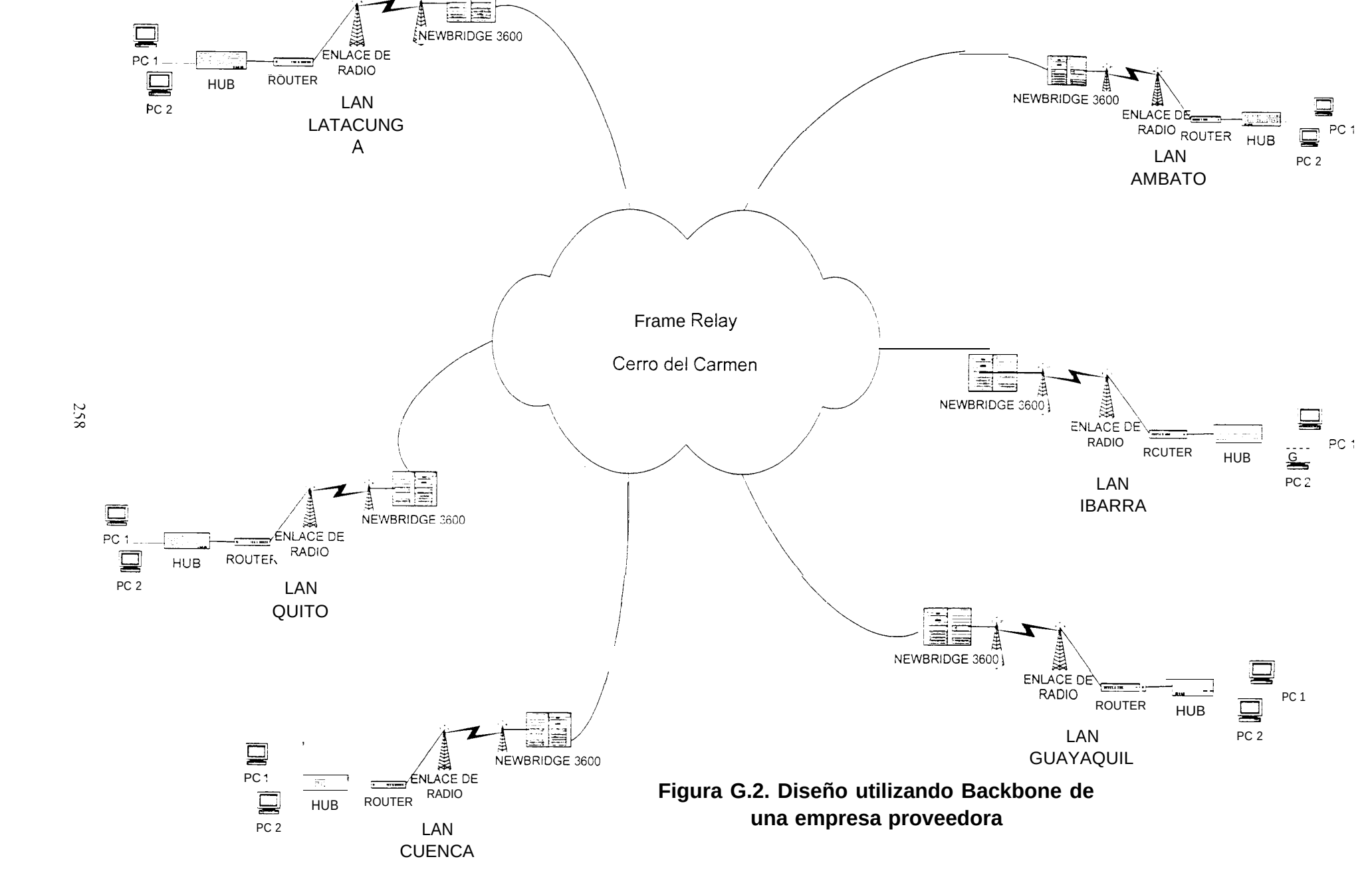


Figura G.2. Diseño utilizando Backbone de una empresa proveedora

1.2. Análisis financiero.

En el siguiente cuadro se resumen los costos de alquiler una Intranet soportada en un backbone de empresa proveedora. Note que necesita una alta inversión inicial.

Tabla G.1. Costo de alquiler de intranet soportada en un backbone.

Alquiler del Backbone de una Empresa Proveedora			
Tipo de servicio	Cantidad	Valor unitario*	Total*
Creación PVC**	11 .00	**400.001**	**4.400.001**
Utilización del puerto físico	**6.00**	**300.00**	1,800.00
Arrendamiento de routers	**6.00**	**250.00**	1,500.00
Ultima milla (Renta)	**6.00**	**300.00**	1,800.00
Costo acceso a Internet (UIO + GYE)	**2.00**	**400.00**	**800.00**
Total primer mes			**10,300.00**
*Valor en dólares			
**Este pago sólo se realiza el primer mes			
Costo mensual a partir del 2do mes			**5,900.00**
Costo del ler año			**$200**
Costo a partir del 2do año			**$70.800**

1.3. Ventajas del backbone.

- Sistema de gestión que controla toda la red.
- El canal no es compartido de esta manera se garantiza el uso de la totalidad del ancho de banda contratado.
- **Brinda mayores servicios con el desarrollo de nuevas tecnologías.**

1.4. Desventajas del backbone.

- Mayor costo por contratar un medio dedicado.
- En caso de ampliaciones, mayor dificultad de integrar una nueva sucursal.
- Eficiencia del servicio depende de la compañía privada.

2. Enlaces satelitales.

Los enlaces satelitales se utilizan cuando se requiere una alta confidencialidad en la información que se transmite.

2.1. Características técnicas.

Existen tres modalidades de estos enlaces disponibles en nuestro medio:

- Modalidad SCPC, que consta básicamente de un Clear Channel donde al cliente se le asigna una portadora dedicada de un ancho de banda fijo preestablecido, lo que significa que el usuario va a disponer de la totalidad del ancho de banda contratado.
- Modalidad VSAT que proporciona un sistema compartido por múltiples usuarios.

- En el caso de un enlace tipo DAMA, basado en la demanda del cliente, se asigna al usuario una portadora que permite el uso del ancho de banda por demanda, es decir que el cliente usará el ancho de banda que requiera en un determinado momento.

2.2. Análisis financiero.

Considerando la opción de establecer la Intranet basada en enlaces satelitales como solución para el caso SECOHI se necesita asumir los costos de alquiler que muestra la tabla a continuación.

Tabla G.2. Costo de intranet sobre enlaces satelitales.

Alternativa con enlaces Satelitales.	
Costo de Alquiler de equipos (Arriendo de los equipos) (Estación Base Satelital, y Torre)	$1,250
Costo del Servicio enlace Clear Channel 64K	$1,250
Costo de Instalación por enlace 64K	$2,500
Total parcial	**$5,000**
Por 6 sucursales **Total**	$30,000
Costo de compra de los ruteadores	$16,700
Costo del primer mes	$46,700
Costo mensual	$31,700
Costo del Primer año	**$395.400**
Costo del Segundo año	$380,400

2.3. Ventaja de los enlaces satelitales.

Una de las mayores ventajas al trabajar con enlaces satelitales es la amplia cobertura a nivel mundial con que se cuenta, puesto que se puede implementar una estación satelital para llegar a lugares de difícil acceso, sean estos, islas, región oriental, desiertos, donde no hay la posiblilidad de otras soluciones.

Otra ventaja es la alta confidcncialidad de los datos que se transmiten por este sistema, como también la posibilidad del usuario de administrar el ancho de banda alquilado a su convieniencia.

2.4. Desventajas de los enlaces satelitales.

Como desventaja podemos citar el retardo de aproximadamente 500 ms que se presenta en cada salto satelital, situación que hay que considerar en el caso de aplicaciones que demandan un menor retardo para funcionar óptimamente como por ejemplo, voz sobre IP.

3. Elección.

Ya expuestos aspectos técnicos, financieros, ventajas y desventajas de las diferentes alternativas que consolidan la intranet, consideramos como mejor opción la que usa tecnología VPN y compra los routers:

- Con respecto a la confidencialidad, los métodos de encriptación que emplea la hacen una red segura.

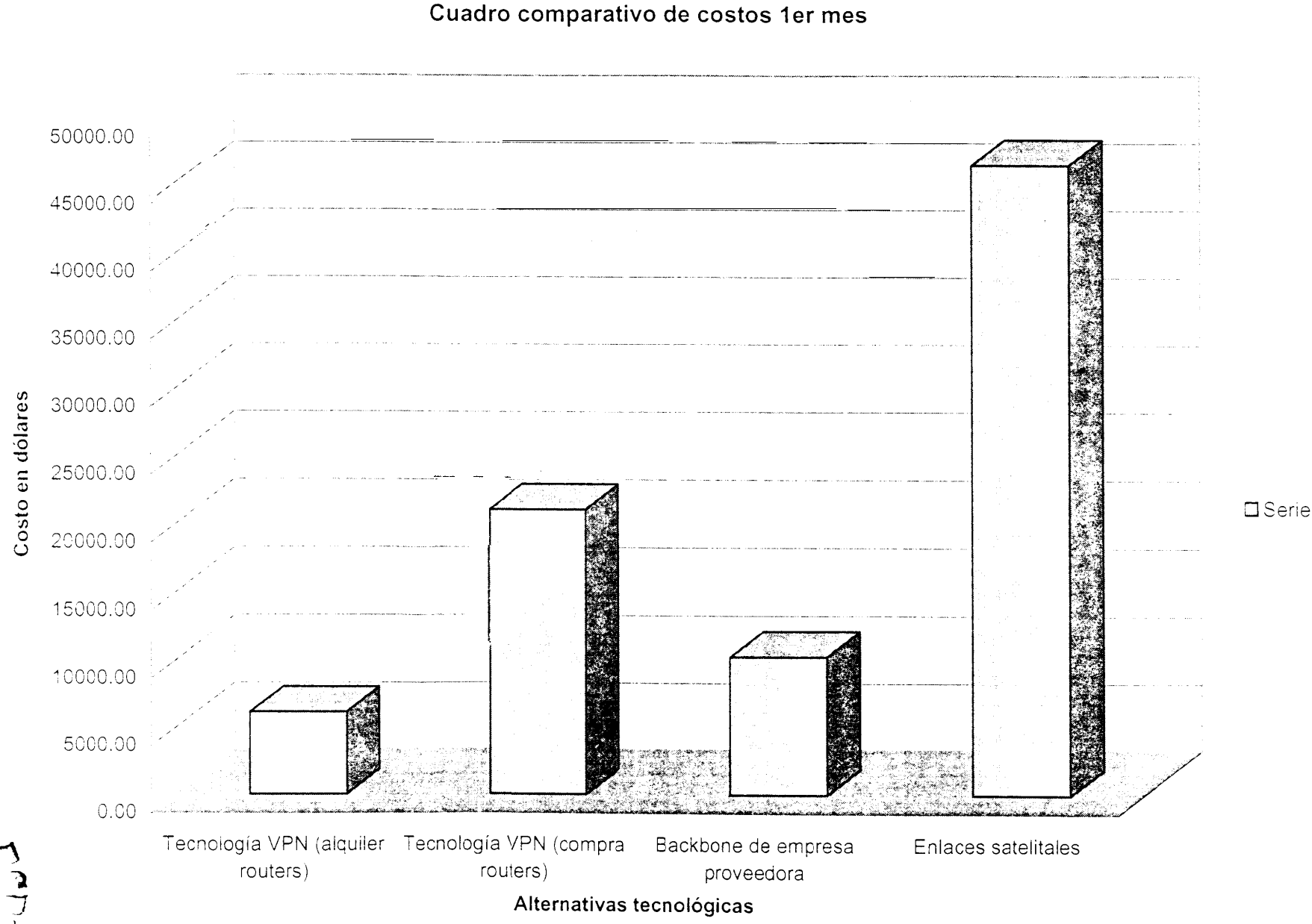
- El sistema VPN es una alternativa económica a corto y largo plazo (Referirse all anexo de comparación de costos).

- Rapidez y mínima inversión en caso de integración de nuevas sucursales, ya que se utiliza la infraestuctura ya existente del Internet.

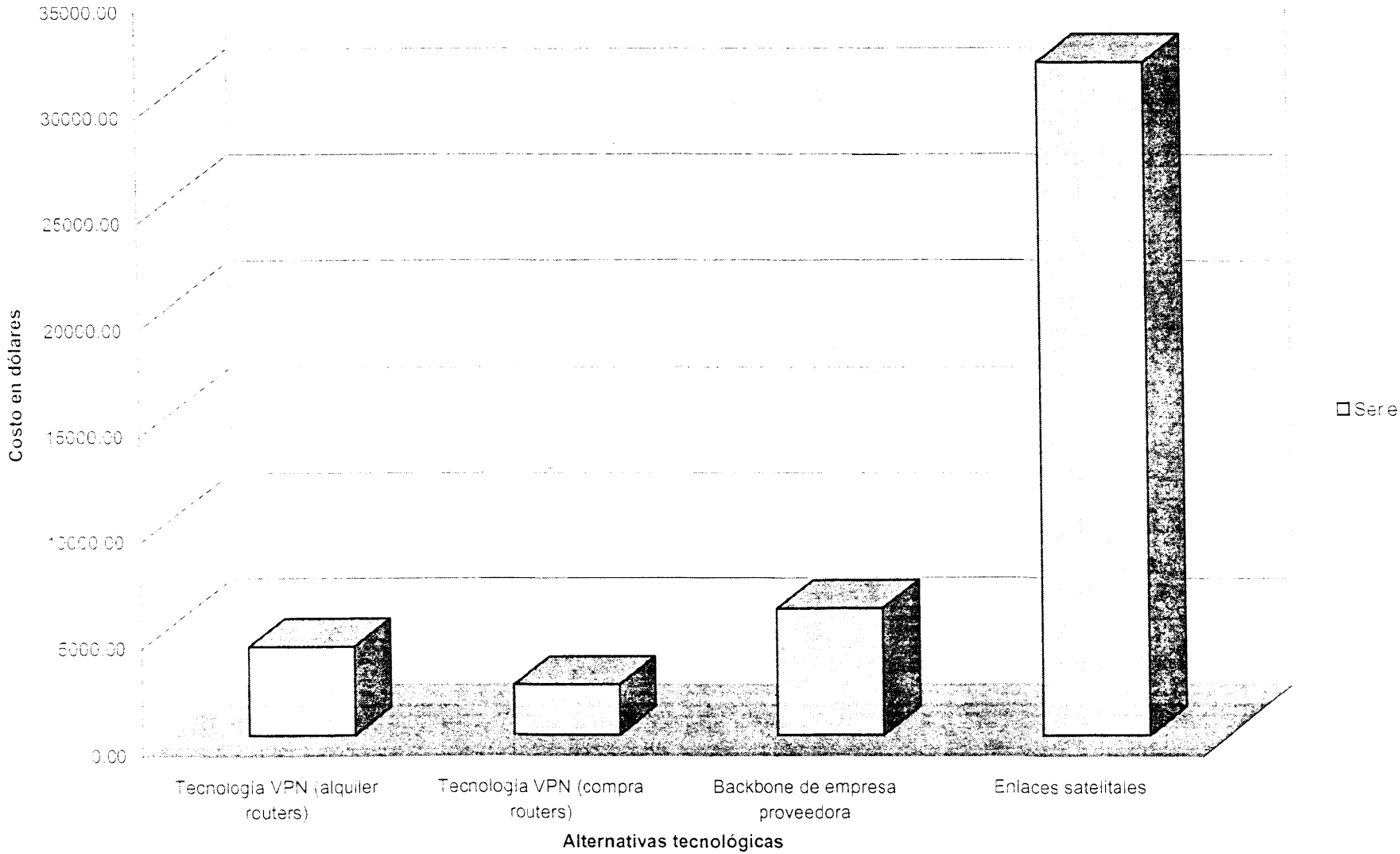
- Es factible usuarios remotos desde cualquier lugar donde haya Internet.

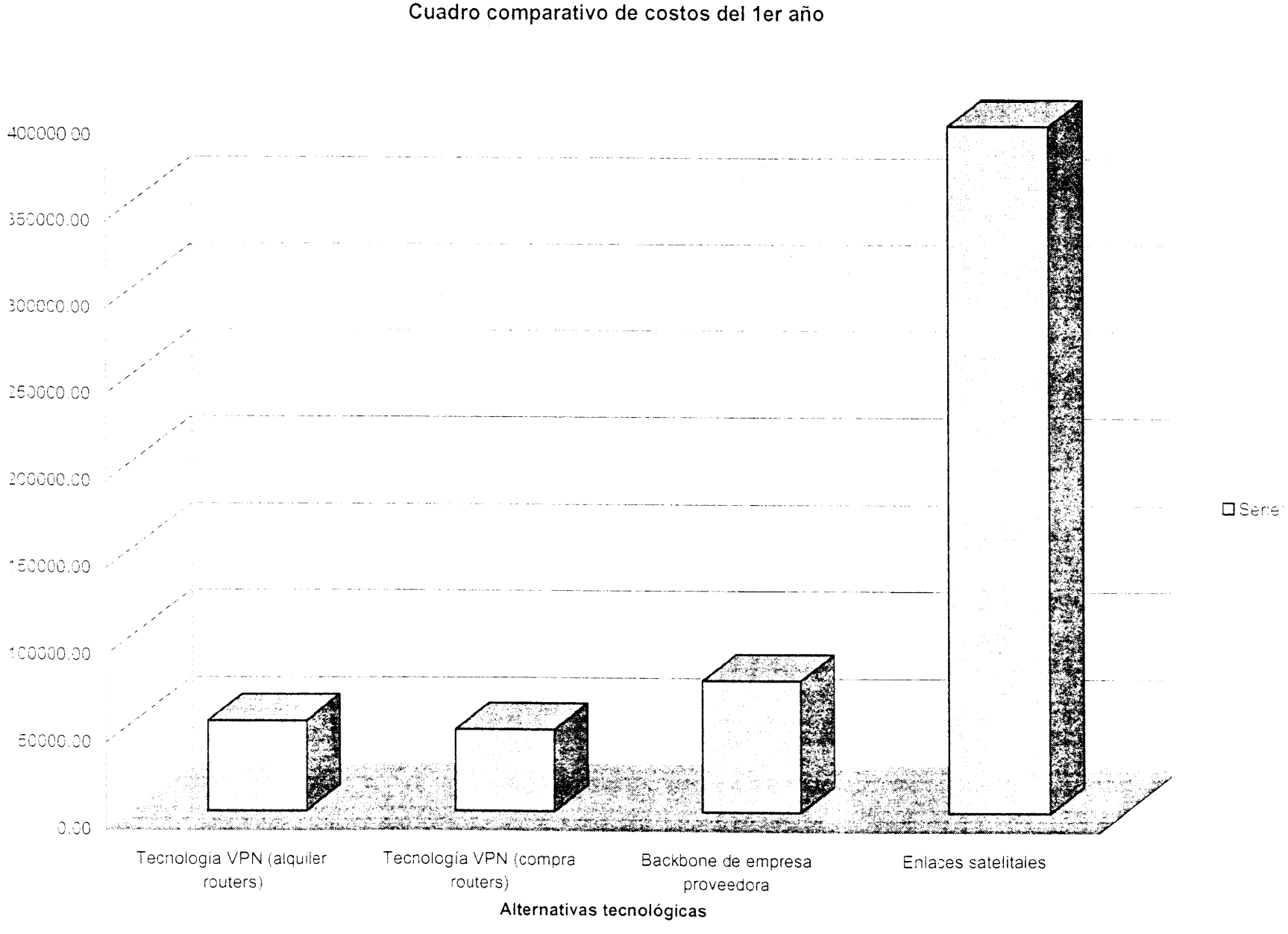
La alternativa con enlaces satelitales aplicada a SECOHI, cuyas sucursales se ubican en zonas urbanas de fácil acceso, no se justifica tanto por el elevado costo de la inversión que demanda como por el retardo adicional que producirían los saltos satelitales sumados al del proveedor de Internet.

La alternativa de alquiler de backbone de empresa proveedora es buena pero su costo es más elevado en relación al de las VPN y presenta limitaciones en cuanto a la integración de nuevas sucursales, por depender de las perspectivas de crecimiento de la empresa proveedora del backbone.

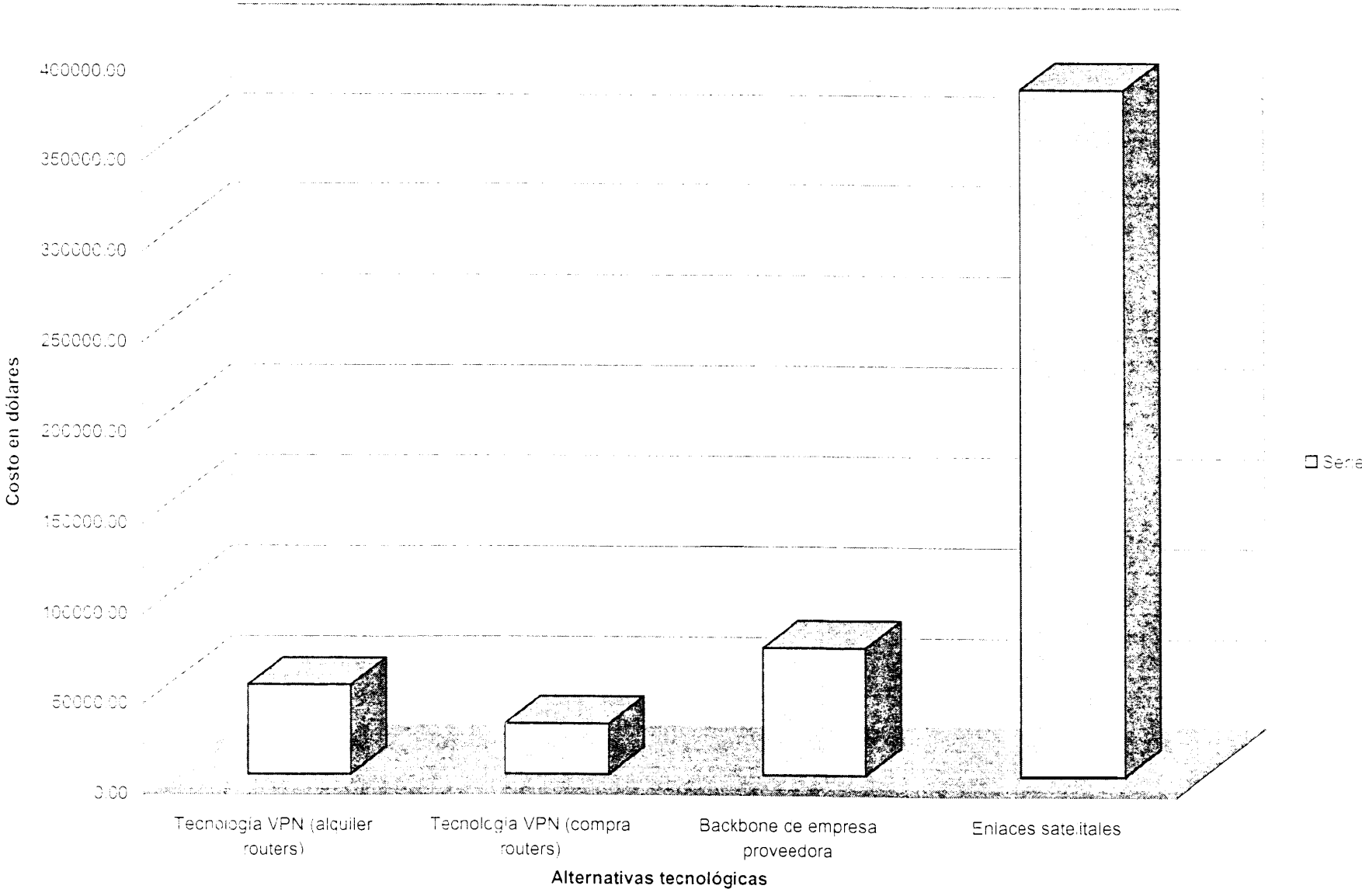

Cuadro comparativo de costos 1er mes
50000.00
45000.00
40000.00
35000.00
30000.00
25000.00
20000.00
15000.00
10000.00
5000.00
0.00
Costo en dólares
Tecnología VPN (alquiler routers)
Tecnología VPN (compra routers)
Backbone de empresa proveedora
Enlaces satelitales
Alternativas tecnológicas
Serie

Cuadro comparativo de costos a partir del 2do mes




Cuadro comparativo de costos del 1er año
400000.00
350000.00
300000.00
250000.00
200000.00
150000.00
100000.00
50000.00
0.00
Tecnología VPN (alquiler routers)
Tecnología VPN (compra routers)
Backbone de empresa proveedora
Enlaces satelitales
Alternativas tecnológicas
Serie1

Cuadro comparativo de costos a partir del 2do año



BIBLIOGRAFIA.

"Intranets, Mejorando la Comunicación interna para apoyar su estrategia empresarial" Ing Guillermo Jacobi MAE, Nicaragua. Universidad de Costa Rica proyecto de la Red telemática Institucional

" TCP/IP Arquitectura, protocolos e Implementación con IPV6 y seguridad de IP", por Dr. Sidnie Feit.

"Data and Computer Communications", por William Stallings.

"Computer Networks" por Andrew S. Tanenbaum.

"Soporte Técnico Microsoft España". Redes Privadas Virtuales.

"Managed VPN Services: Marketing Opportunity and Paths for Implementation" por VPNet.

"Virtual Private Networks" por VPNet.

"Virtual Private Networks (VPNs) Tutorial" por Nortel Networks.

"Interconexión de Redes Privadas Virtuales" por Daxnet.

"Benefits of Using VPN Technology" por Technologic, Inc.

"Redefining the Virtual Private Network" por Check Point Software Technologies Ltd.

"CISCO 1720 Manual", de CISCO.

"STU-1 60 Baseband Modem Operating Booklet" por Tellabs, MartisDXX.

RFC IPSec.

Direcciones de Internet:

http://www.red.ucr.ac.cr

http:// www.tellabs.fi

http:// www.tlogic.com

http://www.aui.es/biblio/libros.

http://www.daxnet.com

http://www.iec.org

http://www.infonetics.com

http://www.vpnet.com

http://www.microsoft.com

http://www.cisco.com