UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REDES PRIVADAS VIRTUALES - VPN

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

LUIS ALEXANDER SÁNCHEZ MENDOZA

PROMOCIÓN
2002 - II

LIMA – PERÚ
2006

REDES PRIVADAS VIRTUALES - VPN

Dedico este trabajo a:

Dios, quien es fuente de mis fuerzas y es quien me da la vida para continuar en este mundo.

Mis padres, quienes son los que me alientan y apoyan para continuar superándome en este largo caminar.

Mis hermanos, por el apoyo incondicional y ser la alegría de mi vida

Mi asesor por indicarme el camino para la presentación de este informe.

SUMARIO

En este informe de suficiencia mostraremos la definición, requerimientos para la implementación y aplicación de una Red Privada Virtual (**VPN** – *Virtual Private Networks*). Así mismo, se dará el concepto y requerimientos de un *tunneling* VPN. Se definirá los tipos de VPN según el RFC 2764 y según el alcance del VPN para la organización. También se verá las características de cada tipo de VPN. Daremos las clasificaciones de VPN que son el modelo superpuesto y modelo par a par. Para el *tunneling* se ha desarrollado protocolos que serán definidos en este informe, se mostrarán las características de cada uno de ellos pero no se abordara en detalle en cada uno de ellos. El VPN es uno de los servicios que los proveedores como Telmex S.A. brinda a sus clientes; se mostrará un Proyecto Integral de Comunicaciones de la Red Extranet Financiera para el Banco de Central de Reserva del Perú, la cual en la actualidad Telmex le está brindando el servicio de transporte usando VPN a través del *backbone* ATM de Telmex, en esta parte se verá la solución, propuesta y las respectivas pruebas del proyecto.

INDICE

INDICE DE GRAFICAS

INDICE DE TABLAS

INTRODUCCION

Introducción

A medida que la computadora fue siendo incorporada a las empresas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa.

Una red se extiende sobre un área geográfica amplia, como en un país o un continente; y esta tiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones).

En los últimos años, las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto, dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

Se ha demostrado en la actualidad que las redes reducen los gastos de tiempo y dinero de las empresas, esto ha significado una gran ventaja para las organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también, es cierto que estas redes remotas han despertado la curiosidad de algunas personas, que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo, la seguridad de las redes es de suma importancia, es por eso que se escucha hablar tanto de los famosos firewalls y los VPNs.

Las primeras redes de computadoras fueron implementadas con dos tecnologías fundamentales: líneas dedicadas (*leased lines*), para una conectividad permanente, y conexiones conmutadas (*dial-up lines*), para requerimientos de conectividad ocasional. Estas redes iniciales brindaban a los usuarios una alta seguridad (para tener acceso a datos transportados sobre líneas dedicadas hay que tener equipamiento para estos fines y acceso

físico a dichas líneas), pero no brindaban una buena relación costo-beneficio por dos razones fundamentales:

- El promedio de tráfico entre dos sitios cualesquiera de una red varía basado en muchos factores, entre ellos, el momento del día, de la semana, del mes, etcétera.
- Los usuarios finales requieren de respuestas rápidas, lo que exige de altos anchos de banda entre los sitios de red. Pero el ancho de banda de una línea dedicada sólo es usado una parte del tiempo, cuando el usuario está activo.

Estas dos razones iniciales llevaron a la industria del transporte de datos y a los proveedores de servicio a desarrollar e implementar esquemas de redes de conmutación de paquetes, con principios de multiplexación estadística que brindan a los clientes servicios equivalentes a líneas dedicadas.

En este documento se discute solamente la implementación de VPNs a través de *backbone* IP, sea redes IP privadas o el Internet público. Los modelos y los mecanismos descritos aquí se aplican en *backbones* IPV4 e IPV6. Este documento no discute específicamente los métodos para construir VPNs usando mapeo sobre el *backbone* conmutado, por ejemplo, VPNs construido usando Emulación de LAN sobre ATM (**LANE** - *LAN Emulation*) o Multiprotocolo sobre ATM (**MPOA** – *Multiprotocol Over ATM*), protocolos que funcionan sobre *backbone* ATM. En el *backbone* IP son construidos usando tales protocolos, interconectando *routers* sobre el *backbone* conmutado, los VPNs discutidos funcionan por encima de esta red IP, y por lo tanto no utilizan directamente los mecanismos nativos del *backbone*. Los VPNs nativos se restringen al alcance del *backbone*, mientras que los VPNs basados en IP puede extenderse al alcance de la accesibilidad IP. Los protocolos VPNs nativos están claramente fuera del alcance del IETF, y se pueden abordar por los organismos tales como el forum ATM.

Problemática

Una problemática que se presenta es como interconectar dos o más redes implementadas, dándose como una solución es a través de la PSTN pero la desventaja es el costo de la llamada, ya que su costo sería por minuto conectado, además si el punto extremo no es local sería una llamada de larga distancia, a parte que no contaría con la calidad y velocidad adecuada; y otra solución sería una red privada, pero para esto se tendría que tender cable, ya sea de cobre o fibra óptica, de un punto a otro, en esta opción

el costo es muy elevado porque si se necesita enlazar la oficina central con una sucursal que se encuentra a cientos de kilómetros de distancia, el costo sería la renta mensual por kilómetro, sin importar el uso.

Al realizar la transmisión de datos en un medio inseguro (Internet) esto puede conllevar a la intercepción y a la suplantación de la comunicación.

Las expectativas de comunicación actuales no siempre pueden cubrirse debido a la problemática para su gestión, explotación y coste que llevan implícitas.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

Justificación

Una de las principales preocupaciones de las organizaciones es cómo administrar el conocimiento e inteligencia de sus negocios, cómo darse a conocer en mercados globales, y cómo unir su cadena de valor para hacer más eficientes sus operaciones.

Las Redes Privadas Virtuales (**VPN** - *Virtual Private Networks*) son una alternativa a la conexión WAN mediante líneas telefónicas y al Servicio de Acceso Remoto (**RAS** – *Remote Access Service*), bajando los costos de éstos y brindando los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones.

En la actualidad, tanto las empresas como los organismos oficiales y otras entidades presentan una estructura distribuida, disponiendo de sedes en puntos distantes. La llegada del Internet abre las puertas a la comunicación entre estos puntos. Las Redes Privadas Virtuales proporcionan soluciones para que dicha comunicación sea fiable y segura. La implantación de una Red Privada Virtual, permite:

- Establecimiento de comunicaciones seguras entre distintos puntos de una red mediante la utilización de canales públicos (Internet).
- Conseguir una comunicación transparente entre los usuarios de todas las delegaciones.
- Acceso a los recursos del Intranet desde cualquier punto de Internet manteniendo los niveles de seguridad adecuados.

VPN ofrece una manera más práctica y económica, para que el personal viajero (por ejemplo, ejecutivos de ventas) se puedan conectar en forma segura a la red corporativa. VPN también es atractiva para conectar en forma segura la sede principal de una organización con sus sucursales remotas.

A continuación se mostrará en el capitulo I Fundamentos Teóricos donde se tratará acerca de la definición, requerimientos de una implementación y aplicación de una VPN y conceptos de *tunneling*.

Luego en el capítulo II se tratará acerca de los tipos, clasificaciones y protocolos de una VPN que son usados y desarrollados hasta el momento, en los cuales se mostrará la operación de los mismos, acerca de los tipos de VPN se tratará según el **RFC 2764** y según el alcance del VPN para la organización, y clasificaremos las VPN según modelos superpuesto y par a par.

Posteriormente explicaremos en el capitulo III un proyecto de un servicio VPN brindado por Telmex en el cual veremos la propuesta del proyecto, la implementación y prueba de servicios desarrollada para el Banco Central de Reserva del Perú en el 2002. Asimismo en el Capitulo IV se darán las ventajas e inconvenientes de la tecnología VPN, y también se expondrá las conclusiones y por ultimo se mostrará un glosario donde se explicará los términos usados en este informe.

CAPITULO I
FUNDAMENTOS TEORICOS

1.1 Definición

Una Red Privada Virtual es un mecanismo de comunicación que permite conectar una o más redes privadas mediante una red pública, de forma que estas redes parezcan sólo una (Virtual) y mantenga la privacidad.

Tomar en cuenta que las redes Frame Relay o ATM del proveedor de servicios de telecomunicaciones también son compartidas, aunque no son tan "públicas".

Una Red Privada Virtual se construye a base de conexiones realizadas sobre una infraestructura compartida con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada real. El objetivo de las VPNs es contener aplicaciones de intra/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" porque el usuario "cree" que posee los enlaces. Las IP VPN (**RFC 2764**) son soluciones de comunicación VPN basadas en el protocolo de red IP.

La esencia del VPN reside en que el tráfico privado viaja protegido como si se tratara de una red dedicada, por eso se habla de una red "privada virtual", ya que no es una red "privada real".

1.2 Requerimientos de implementación y aplicación VPN

1.2.1 Requerimientos generales para una VPN

Es creciente el interés en el uso de VPNs como una de la manera más efectiva en la construcción y despliegue de una red de comunicación privada para comunicar múltiples sitios con una aproximación a las redes privadas existentes.

Existen redes privadas que se pueden categorizar generalmente en dos tipos: WANs dedicado que permanentemente conectan múltiples sitios, y las redes conmutadas (*dial networks*), que permite conexión en demanda a través de la Red Publica de Conmutación Telefónica (**PSTN** - *Public Swicthed Telephone Network*) para uno o mas lugares en la red privada.

WANs son típicamente implementados usando líneas dedicadas o circuitos dedicados, por ejemplo conexión Frame Relay o ATM entre múltiples sitios. *Routers* o *switches* del **CPE** (*Customer Premises Equipment*), de diferentes sitios, se conectan con estas instalaciones dedicadas y permiten conectividad a través de la red. Dado el coste de tales instalaciones dedicadas y la complejidad de la configuración de los dispositivos del CPE, generalmente las redes no son totalmente enmalladas, pero en lugar de ello tienen cierta forma de una topología jerárquica. Por ejemplo una oficina remota puede ser conectada directamente a la oficina regional más cercana, la oficina regional conectada conjuntamente con algunos desde mallas completas o parciales.

Redes conmutadas privadas (*Private dial netwoks*) son usadas para permitir que los usuarios remotos se conecten en la red de la empresa, usando enlaces de la PSTN o la Red Digital de Servicios Integrados (**ISDN** - *Integrade Service Digital Network*). Típicamente, esto se hace con el despliegue del Servidor de Acceso de Red (**NAS** - *Network Access Server*), en una o más lugares centrales. Los usuarios marcan un NAS, que interactúa con los servidores de Autenticación, Autorización y Contabilidad (**AAA** - *Authentication, Authorization and Accounting*), para verificar la identidad del usuario y para brindar de servicio al usuario que es autorizado.

En épocas recientes, más negocios han encontrado la necesidad de conexiones de alta velocidad a través del Internet para sus redes corporativas privadas, existe un interés significativo en el despliegue del CPE basado en VPNs que funcionan a través del Internet. Esto ha sido típicamente conducido por la tasación insensible a la ubicuidad y a la distancia de los servicios actuales del Internet, que puede resultar un costo significativamente bajo en comparación a los dos tipos de redes privadas.

La noción de usar el Internet para las comunicaciones privadas no es nueva, y muchas técnicas, tales como el Desborde de Ruta Controlada (*controlled route leaking*) se han utilizado para este propósito. Sin embargo, recientemente se tienen los mecanismos IP apropiados y necesarios para encontrar los requisitos del cliente debido a las VPNs. Estos requisitos incluyen lo siguiente:

- Transporte no transparente de paquetes:

El tráfico llevado dentro de un VPN no puede tener relación con el tráfico del *backbone* IP, porque el tráfico es multiprotocolo, o porque la red IP del cliente puede utilizar direcciones IP sin relación al *backbone* IP, en el cual se transporta el tráfico. En detalle, la red IP del cliente puede utilizar direcciones privadas IP no-únicas.

- Seguridad de datos:

En general los clientes que usan VPNs requieren seguridad de datos. Hay diversos modelos de confianza que son aplicables al uso de VPNs. Un caso es aquel cuando el cliente no confía en el proveedor de servicio para proporcionar seguridad y en lugar de eso se implementa una VPN usando los dispositivos del CPE que ofrecen funcionalidad de firewall y son conectados usando seguridad de túnel. En este caso el proveedor de servicio es utilizado solamente para el transporte de paquetes IP.

Un caso alternativo es aquel cuando el cliente confía en el proveedor de servicio para proporcionar un servicio de administración segura de VPN. Esto es similar a la confianza involucrada cuando el cliente utiliza un servicio de *switch* público como Frame Relay o ATM , en el cual el cliente confía en que los paquetes no serán inyectados en la red de una manera no autorizada, fisgoneada, modificada en el tránsito, o sujeto a análisis de tráfico por personas no autorizadas.

En este caso, la responsabilidad del proveedor de servicio es brindar la operabilidad de firewall y el servicio de transporte seguro de paquetes. Diversos niveles de seguridad pueden ser necesarios dentro del *backbone* del proveedor, dependiendo del despliegue usado. Si el tráfico de VPN es contenido dentro de un solo *backbone* IP de un proveedor, entonces los mecanismos de seguridad, tales como lo entregado por la suite de protocolo de Seguridad IP (**IPSec** - *IP Security*) **[1]**, pueden no ser necesarios para los túneles entre los nodos del *backbone*. Si el tráfico de VPN atraviesa redes o equipos de administración múltiple, entonces los mecanismos de seguridad pueden ser convenientes. Si esta percepción acerca de las redes es o no es correcta, debe ser considerado en la implementación del VPN.

- Garantía de calidad de servicio

Además de asegurar la privacidad de la comunicación, existen técnicas de redes privadas, que son construidos sobre mecanismo de capa física o de enlace, que también ofrecen varios tipos de garantía de calidad de servicio. En particular, las líneas dedicadas y las conmutadas ofrecen garantías de ancho de banda y de latencia, mientras que las tecnologías de conexión dedicada como Frame Relay y ATM tienen mecanismos con garantías similares. Como el IP basado en VPNs llega a ser ampliamente extendido, será la demanda del mercado para tener garantías similares que asegura la transparencia de aplicaciones de extremo a extremo. Mientras que la capacidad del IP basado en VPN ofrece tales garantías, lo cual dependerá de la capacidad del *backbone* IP; una estructura de VPN se debe dirigir de manera por la cual los sistemas de VPN pueden utilizar tales capacidades, y como ello evoluciona.

- Mecanismo de *tunneling*

Los dos primeros requisitos mencionados dan a entender que los VPNs deben ser implementados a través de un mecanismo de *tunneling* IP, donde los formatos de paquete y/o dirección usados dentro del VPN están sin relación a ése usado para encaminar el túnel de los paquetes a través del *backbone* IP. Tales túneles, dependiendo de su forma, pueden proporcionar un nivel de seguridad de datos, o esto también se puede incrementar usando otros mecanismos (como ejemplo, IPSec).

Además, se discute más adelante, que tales mecanismos de *tunneling* también pueden ser trazados dentro del desarrollo del mecanismo de administración de tráfico IP. Allí ya se definen una gran cantidad de mecanismos de *tunneling* IP. Algunos de estos satisfacen las aplicaciones VPN.

1.2.2 CPE y redes basadas en VPN

La mayoría de implementaciones actuales de VPN se basa en el CPE. Las capacidades del VPN se están integrando en una variedad amplia de dispositivos de CPE, extendiéndose desde los firewalls a los *routers* de borde de la WAN, y a los dispositivos especializados de terminación VPN. Tales equipos pueden ser comprados y desplegados

por los clientes, o puede ser desplegado (y ser a menudo administrado remotamente) por los proveedores de servicio en un modelo de *outsourcing*.

Hay un interés significativo en las "redes basadas en VPNs", donde la operación del VPN es dada en *outsourcing* a un Proveedor de Servicio de Internet (**ISP** - *Internet Service Provider*). El interés en la solución de *outsourcing* es para los clientes que intentan reducir costos de soporte y para el ISPs que busca nuevas fuentes de ingreso. El soporte de VPNs en la red permite el uso de mecanismos particulares que pueden conducir a soluciones VPN altamente eficientes y rentables, con equipos y operaciones comunes y costeadas por una gran cantidad de clientes.

La mayoría de los mecanismos discutidos mas adelante pueden ser aplicados a cada CPE o redes basadas en VPNs. No obstante, los mecanismos particulares son probablemente pruebas de aplicaciones más recientes; dado que las herramientas de influencia (por ejemplo, *piggybacking on routing protocols*) son accesibles solamente en el ISPs y los cuáles son pocos probables de ser puestos a disposición de cualquier cliente, o aún ser albergado en el propio ISP y en el CPE debido a los problemas de coordinar la administración del CPE suministrado por el ISP y el cliente.

A continuación se mostrará los diversos productos Cisco con la finalidad de familiarizarse con ellos, por que en el proyecto que se muestra en el capitulo III se utilizará los equipos Cisco para dar la solución al proyecto del Banco Central de Reserva del Perú.

1.2.2.1 Aplicación VPN a través de productos Cisco

Se presenta una problemática en la administración y despliegue del VPN, como se muestra en figura 1.1, debido a lo siguiente:

Variedad de dispositivos CPE y clientes.

Lugares remotos no tienen soporte en el lugar que se encuentra.

Túneles VPN sobre conexiones WAN estático y/o dinámico

Direcciones IP dinámicas y/o estáticas

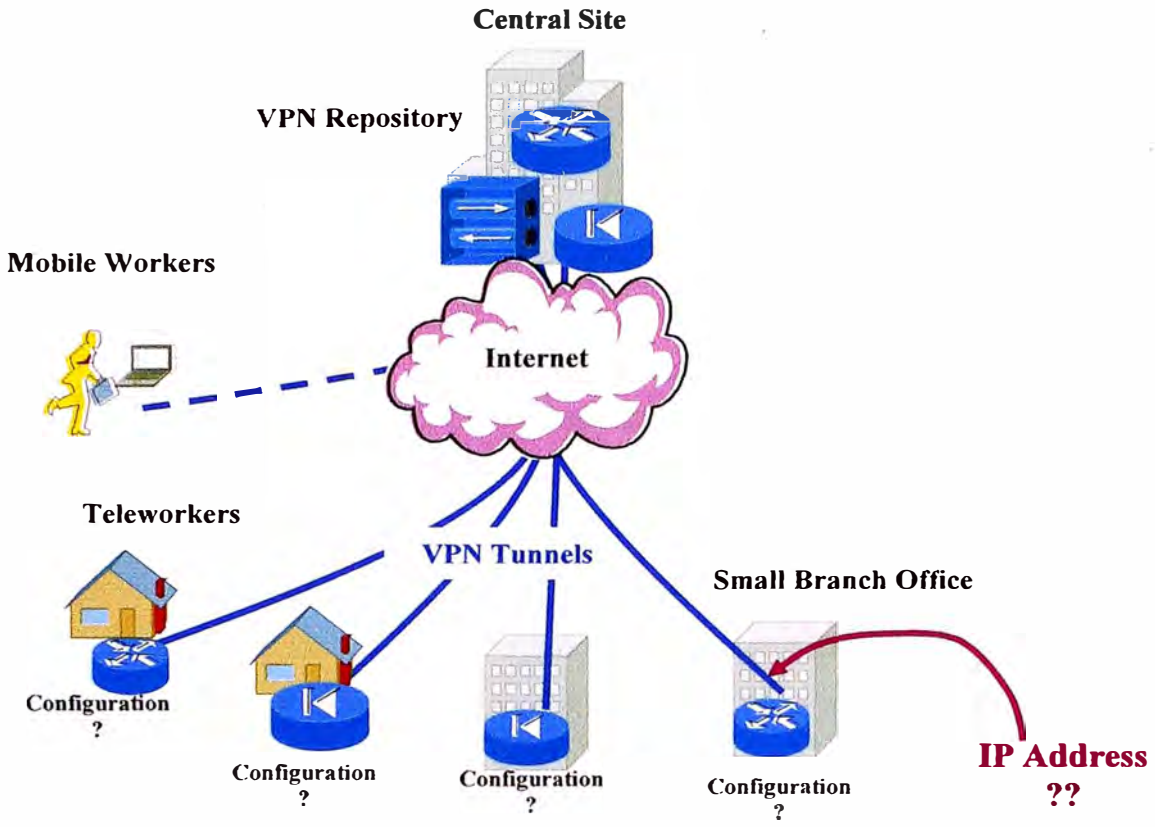

Figura 1.1: Problemática presentada

Cisco ofrece una variedad de plataformas y aplicaciones, que son diseñadas para implementar VPN. A través del desarrollo y adquisición de productos, Cisco tiene una variedad de componentes de hardware y software disponible que permite a los negocios de todo tamaño una rápida y fácil implementación de VPNs usando IPSec u otros protocolos.

Cisco puede proveer hardware y software para cubrir casi todos los posibles requerimientos de VPN. Desde un *router* a un firewall, para aplicaciones de internet, concentradores VPN (*VPN concentrador*) y *clients*, para aplicaciones de acceso remoto. Esta sección introduce algunas de las características claves de los productos VPN de Cisco.

Cisco ha dado una solución para la VPN, influenciando en el trabajo unificado del usuario, por lo tanto ha desarrollado dispositivos de CPE que los clasifica de la siguiente manera:

- *Router* VPN Cisco.
- Firewalls PIX Cisco.
- Concentrador 3000 VPN Cisco.

VPN Clients

- VPN *Client* Cisco
- Hardware de VPN 3002 *Client* Cisco
- *Easy* VPN Cisco

A. *Router* VPN Cisco

Los *routers* VPN Cisco son las mejores opciones para construir VPNs intranet o VPNs extranet de *site to site*. Estos *router* usan Software IOS Cisco y puede ser usado para *multicast*, encaminamiento y multiprotocolo a través del VPN. Estos dispositivos permiten calidad de servicio (**QoS** - *Quality of Service*) y opciones de personalización de firewall lo cual lo convierte en robustos firewalls. Algunos *routers* también tienen integrado DSL y cable modem para proveer acceso VPN a oficinas pequeñas o oficinas de casa (**SOHO** – *Small Office/Home Office*).

Algunos *routers* para VPN pueden equiparse con módulos especiales para manipular procesamiento de cifrado para túneles VPN. Estos módulos de memoria y ciclos de CPU pueden ser usados para conmutación de paquetes, la cual es la función primaria del *router*.

Estos *routers* VPN ofrecen un amplio rango de protocolos VPN. La tabla 1.1 muestra algunas características de los *routers* Cisco que están disponibles para la aplicación de identificación y servicio VPN, y donde estos debería ser probablemente mas aplicado.

Site	Modelo	Funcionamiento VPN	Características
SOHO VPN de acceso Remoto VPN extranet	Router ADSL 827H Cisco	384 Kbps hasta 50 túneles	Configuración estable Modem ADSL integrado Soporte para remoto Ez VPN
SOHO VPN de acceso Remoto VPN extranet	Router Cable uBR905 Cisco	6 Mbps hasta 50 túneles	Configuración estable Modem Cable integrado 4 puertos 10Base T hub Soporte para remoto y servidor Ez VPN
SOHO VPN de acceso Remoto VPN extranet	Router 806 boradband Cisco	384 Kbps hasta 50 túneles	Configuración estable Modem *boardband* instalado por atrás Intenface 10 Base T Ethernet WAN 4 puertos 10 Base T LAN hub Soporte para remoto Ez VPN
SOHO VPN de acceso Remoto VPN extranet	Router 1710 Cisco	3 Mbps hasta 100 túneles	Configuración estable Puerto 10/100 Fast Ethernet Puerto 10Base T Ethernet Soporte para remoto y servidor Ez VPN
Oficina pequeña remota VPN de acceso Remoto VPN intranet VPN extranet	Ruter Serie 1700 Cisco	4 Mbps hasta 100 túneles con módulos VPN	Configuración modular Soporte para modulo VPN Soporte para remoto y servidor EzVPN
Branch office VPN intranet VPN extranet	Router Serie 2600 Cisco	14 Mbps hasta 800 túneles con módulos VPN	Configuración modular Soporte para modulo VPN Soporte para servidor EzVPN
Large branch office VPN intranet VPN extranet	Router Serie 3600 Cisco	40 Mbps hasta 800 túneles con módulos VPN	Configuración modular Soporte para módulo VPN Soporte para servidor EzVPN
Lugar de hub central VPN intranet VPN extranet	Router Serie 7100 Cisco	145 Mbps hasta 5000 túneles con módulos de aceleración VPN (VAM)	Configuración modular Soporta VAM Soporte para servidor EzVPN
Lugar de hub central VPN intranet VPN extranet	Router Serie 7100 Cisco	145 Mbps hasta 5000 túneles con VAM	Configuración modular Soporta VAM Soporte para servidor EzVPN

Tabla 1.1: *Routers* VPN Cisco

B. Firewall PIX Cisco

Los componentes de hardware que proveen VPNs es la serie de Firewall PIX Cisco. Las características del Firewall PIX tienen como propósito construir sistemas operativos y proveer un amplio rango de seguridad y servicio de red. Junto con el VPN-IPSec, el Firewall PIX también puede proveer VPN-PPTP y VPN-L2TP desde clientes Microsoft Windows.

A continuación se mostrará algunas de las características que serán contenidos en estos dispositivos:

- La Traducción de Direcciones de Red (**NAT** - *Network Addrress Translation*) y la Traducción de Direcciones de Puertos (**PAT** - *Port Address Translation*), satisfacen y filtran URL, RADIUS (**RADIUS** - *Remote Authentication Dial-In User Service*) y TACACS+ (**TACACS+** - *Terminal Access Controller Access Control System Pluss*) que contiene AAA.
- El Protocolo de Configuración de *Host* Dinámico (**DHCP** - *Dynamic Host Configuration Protocol*)
- X.509
- Infraestructura de Llaves Publicas (**PKI** - *Public Key Infraestructure*)

Algunos de los Firewall PIX pueden aceptar módulos VPN para manejar el CPU y la memoria del proceso de cifrado IPSec. El Firewall PIX Cisco posee un rango de sistemas operativos como VPN *Clients* así como también hardware de VPN 3002 *Client* de Cisco. La tabla 1.2 bosqueja las series de Firewalls PIX, identificando su capacidad de VPN.

Site	Modelo	Funcionamiento VPN
SOHO VPN de acceso remoto VPN intranet VPN Extranet	Firewall PIX 501 Cisco	3 Mbps Hasta 5 pares simultáneos de VPN
Remote office/branch office (ROBO) VPN de acceso remoto VPN intranet VPN Extranet	Firewall PIX 506E Cisco	16 Mbps Hasta 25 pares simultáneos de VPN
Negocios de tamaño pequeño a mediano VPN intranet VPN Extranet	Firewall PIX 515E Cisco	63 Mbps Hasta 2000 túneles con tarjeta de acelerador VPN (VAC - *VPN Accelerator Card*)
Empresas y proveedores de servicios VPN intranet VPN Extranet	Firewall PIX 525E Cisco	70 Mbps Hasta 2000 túneles con VAC
Empresas y proveedores de servicios VPN intranet VPN Extranet	Firewall PIX 535E Cisco	95 Mbps Hasta 2000 túneles con VAC

Tabla 1.2: Firewalls PIX Cisco

C. Concentradores VPN 3000 Cisco

Cisco identificó la necesidad de proponer la construcción de dispositivos VPN de acceso remoto y desarrollar la familia de Concentradores de serie VPN 3000.

El Concentrador de serie VPN 3000 Cisco fue diseñado para tener un alto desempeño, soluciones escalables y ofreciendo la habilidad de las técnicas de cifrado y autenticación.

El Concentrador de serie VPN 3000 Cisco viene en una variedad de modelos que pueden contener oficinas pequeñas de 100 o pocas conexiones VPN hasta empresas grandes de 10000 o mas conexiones simultaneas de VPN. La configuración de redundancia es disponible para ayudar a asegurar la alta confiabilidad de estos dispositivos. Los Concentradores VPN 3000 Cisco también poseen tales como PDAs (**PDAs** - *Personal Digital Assistants*) y Teléfonos Smart.

Concentrador	Características
Concentrador VPN 3005 Cisco	Configuración estable Soporta hasta 1000 sesiones simultáneas
Concentrador VPN 3015 Cisco	Mejorable hasta Concentrador 3030 Soporta hasta 1000 sesiones simultáneas
Concentrador VPN 3030 Cisco	Acepta módulos SEP Mejorable hasta Concentrador 3060 Soporta hasta 1500 sesiones simultáneas Configuraciones de redundancia y no redundancia son disponibles
Concentrador VPN 3060 Cisco	Acepta módulos SEP Mejorable hasta Concentrador 3080 Soporta hasta 5000 sesiones simultáneas Configuraciones de redundancia y no redundancia son disponibles
Concentrador VPN 3080 Cisco	Acepta módulos SEP Soporta hasta 10000 sesiones simultáneas configuración solo de redundancia

Tabla 1.3: Concentradores de serie VPN 3000 Cisco

D. VPN *Client*

VPN *client* puede simplificar la administración y mantenimiento de las conexiones VPNs. Esta sección muestra el software y hardware del VPN *client* ofrecidas por Cisco.

- VPN *Client* Cisco

Eventualmente llamado *Unity Client*, el VPN *Client* Cisco es el que interactúa con el VPN 3000 *Client* Cisco; este software viene con el Concentrador de serie VPN 3000 Cisco y esto no tiene un costo adicional para el usuario; este software permite que la estación remota pueda establecer un VPNs IPSec con un producto Cisco de VPN de acceso remoto que esta en la sede central. Aunque es relativamente fácil de configurar, el cliente puede ser preconfigurado para el despliegue masivo, haciendo que la configuración inicial sea sencilla. Este método de instalación es desarrollada para dar un incentivo a los clientes, donde los sistemas de los usuarios realizan el *login* inicial a la red. El VPN *Client* Cisco es

contenido en diferentes sistemas operativos: Linux, Solaris, MAC OS, y Windows 95, 98, Me, NT 4.0, 2000, y XP.

- Hardware de VPN 3002 *Client* Cisco

Una solución alternativa para implementar el software *clients*, en muchas conexiones de estaciones de trabajo, se debe de usar el hardware de VPN 3002 *Client* Cisco. Este dispositivo puede proveer un túnel VPN y es desplegado en un plantel de oficinas remotas con una completa facilidad y con algún sistema operativo que comunique en IP, incluyendo Windows, Solaris, MAC, y Linux.

El hardware del VPN 3002 *Client* Cisco posee EzVPN (*Easy* VPN) Remote, permitiendo a los dispositivos establecer conexiones VPN IPSec con un sistema EzVPN Server. Este hardware *client* puede ser configurado para operar como un software *client* o para establecer una conexión permanente con el lugar central. El hardware del VPN 3002 *Client* Cisco puede ser configurado con o sin *switch* 10/100 ethernet de 8 puertos integrado.

- *Easy* VPN Cisco

En el pasado, la configuración de VPNs entre dispositivos fue una faena diaria. Ambos extremos de la conexión VPN debía ser configurado idénticamente, o el túnel VPN no puede ser establecido. Con la introducción del EzVPN, Cisco ha cambiado. EzVPN tiene dos componentes:

* Cisco *Easy* VPN Remote.
* Cisco *Easy* VPN Server.

Una vez que tienes configurado EzVPN Server en un dispositivo, puedes configurar un dispositivo EzVPN Remote para establecer IPSec que proporciona la contraseña correcta. La tabla 1.4 identifica los dispositivos que contiene cada uno de los componentes EzVPN. El EzVPN es una solución ideal para negocios con algunos locales remotos. El EzVPN es altamente escalable y es un método seguro del despliegue de VPNs a través de organizaciones dispersadas ampliamente.

*** Cisco *Easy* VPN Remote**

Con esto se elimina las configuraciones complejas para el despliegue de la VPN, en este modo Cisco ha desarrollado *routers* y firewalls PIX que son implementadas en los lugares remotos; y asimismo ha desarrollado el software VPN *Client* Cisco que permite ingresar a la sede principal desde una laptop o PC a través del internet o una red publica usando una VPN. Las capacidades de los dispositivos Cisco del CPE depende del modelo del *router*, del firewall y también de la necesidad del cliente. En esta clasificación encontramos los siguientes modelos de dispositivos del CPE:

- *Routers*: 800 Series, uBR900 Series y 1700 Series
- Security Appliances: PIX 501, CVPN 3002 y Cisco VPN Client

*** Cisco *Easy* VPN Server**

Estos dispositivos aceptan la conexión VPN del VPN *Client* Cisco y de los dispositivos Cisco *Easy* VPN Remote. Los VPN Server Cisco son usualmente implementados en la sede principal, estos tipos de dispositivo tienen mayor capacidad y características que los Cisco *Easy* VPN Remote. En esta clasificación encontramos los siguientes modelos de dispositivos del CPE:

- *Routers*: 1700 Series, 2600 Series, 3600 Series y 7100/7200 Series
- Security Appliances: PIX Firewall Series y CVPN 3000 Series

Componente	Cisco Modelo
Cisco *Easy* VPN Remote	Router Serie 800 Cisco Router Serie 1700 Cisco Router Serie uBR900 Cisco Firewall PIX 501 Cisco Hadware de VPN 3002 Client Cisco
Cisco *Easy* VPN Server	Cisco IOS software version 12.2(8)T Routers, incluyendo la serie 1700, serie 7100, serie 7200, así como otros Routers IOS Cisco Firewall PIX 501 Cisco Hadware de VPN 3002 Client Cisco

Tabla 1.4 *Easy* VPN Cisco

A continuación mostraremos en la figura 1.2 como se distribuyen los dispositivo del *Easy* VPN Cisco.

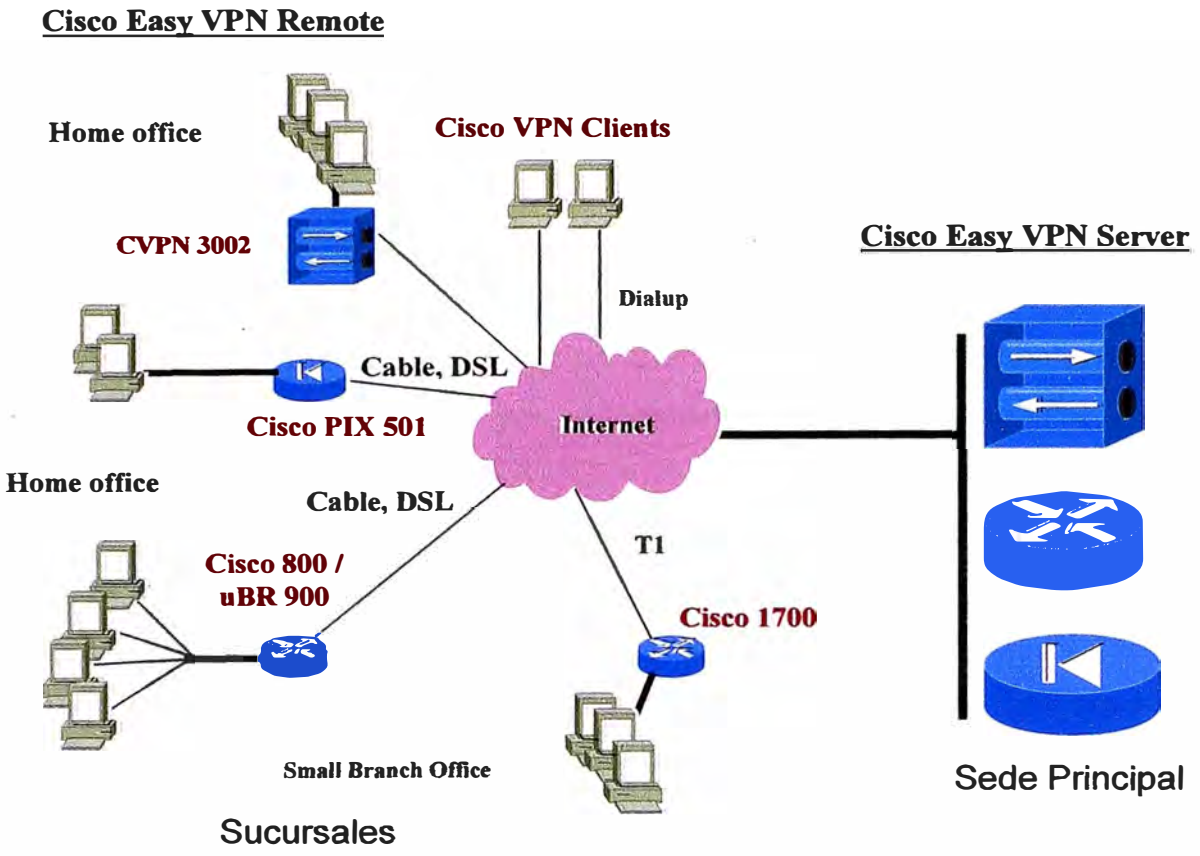

Figura 1.2 *Easy* VPN Cisco

1.2.3 VPNs y extranets

El término "extranet" es comúnmente utilizado para referir a un escenario donde dos o más compañías tienen acceso a una cantidad limitada de cada uno de los datos corporativos de una red. Por ejemplo una compañía de fabricación puede utilizar un extranet para sus proveedores, para permitir que pregunten a la base de datos por la tasación y la disponibilidad de componentes, y después que pida y que siga con el estado de órdenes. Otro ejemplo es el desarrollo común de software, la compañía A permite un grupo de desarrollo dentro de la compañía B tenga acceso a su código fuente del sistema operativo, y la compañía B permite que un grupo de desarrollo de la compañía A tenga acceso a su software de seguridad. Observe que las políticas de acceso se pueden conseguir arbitrariamente complejas. Por ejemplo la compañía B puede restringir internamente el acceso a su software de seguridad a los grupos en ciertas localizaciones geográficas para

cumplir con leyes de control de exportación.

Una característica dominante de un extranet es el control de quién puede tener acceso a los datos, y esto es esencialmente una decisión de políticas. Las decisiones de políticas se hacen cumplir en los puntos de la interconexión entre diversos dominios, por ejemplo entre una red privada y el Internet, o entre un laboratorio de prueba del software y el resto de la red de la compañía. La aplicación se puede hacer vía un firewall o un *router* con funcionalidad de lista de acceso, aplicación de entrada, o cualquier dispositivo similar capaz de aplicar la política al tráfico de tránsito. El control de políticas puede ser implementado dentro de una red corporativa, además entre redes corporativas. También las interconexiones entre las redes puede ser un sistema de enlaces bilaterales, o puede ser una red separada, quizás mantenidas por un consorcio de industria. Esta red separada podía a sí mismo ser un VPN o una red física.

Introducir VPNs en una red no requiere ningún cambio a este modelo. La política se puede hacer cumplir entre dos VPNs, o entre un VPN y el Internet, exactamente de la misma manera que se hace hoy sin VPNs. Por ejemplo dos VPNs pueden ser interconectados; cada administración localmente impone su propia política de control, vía un firewall, en todo el tráfico que ingrese a su VPN desde el exterior, tanto desde otro VPN o desde el Internet.

Este modelo de VPN provee una separación de políticas del modo de transporte del paquete usado. Por ejemplo, un *router* puede dirigir tráfico de voz a la Conexión de Canal Virtual (**VCC** - *Virtual Channel Connection*) ATM para tener QoS garantizado, el tráfico interno no local de la compañía asegura los túneles, y el otro tráfico a un enlace al Internet. En el pasado los túneles seguros pudieron haber sido circuitos de Frame Relay, ahora también pueden ser túneles IP seguros o de MPLS de Camino Conmutado Etiquetado (**LSP** - *Label Switched Path*)

1.3 *Tunneling* VPN

Según lo mostrado anteriormente en la sección 1.2.1, las VPNs deben ser implementadas usando un mecanismo de *tunneling*. Esta sección ve los requisitos genéricos para tales mecanismos.

Un túnel IP que conecta dos puntos extremos de una VPN es un bloque de construcción básico, sobre el cual se puede construir una variedad de diferentes servicios de VPN. Un

túnel IP funciona como un recubrimiento a través del *backbone* IP. En efecto el *backbone* IP se está utilizando como tecnología de *capa de enlace*, y el túnel forma un enlace punto a punto.

Un dispositivo de VPN puede acabar en múltiples túneles IP, y enviar paquetes entre estos túneles y a otras interfaces de red de diferentes maneras. En el capitulo II de este informe se mostrará los diversos tipos de VPNs y se mencionará que la manera por el cual los paquetes se envían entre las interfaces (por ejemplo, *bridged* o *router*) es la característica distintiva y primordial de estos diversos tipos VPN. Un repetidor de dos puertos reenvía los paquetes entre sus puertos, y no examina el contenido del paquete. Un *bridge* reenvía los paquetes usando la información de la capa del Control de Acceso al Medio (**MAC** - *Media Access Control*) contenida en el paquete, mientras que un *router* reenvía los paquetes usando la información de dirección de la capa 3 contenida en el paquete. Cada uno de estos tres panoramas tiene un analogía directa con el VPN, según lo discutido en el siguiente capitulo. Observe que un túnel IP se muestra como otra clase de enlace, que puede ser concatenada con otro enlace, delimitado a una tabla de envío *bridge*, o delimitado a una tabla de envío IP, dependiendo del tipo de VPN.

Las secciones siguientes muestran los requisitos genéricos para un protocolo *tunneling* IP que se puede utilizar para construir diversos tipos de VPNs.

1.3.1 Requerimientos de un protocolo *tunneling* VPN

Hay numerosos mecanismos de *tunneling* IP tales como:

- Encapsulación IP dentro de IP (**IP/IP** - *IP Encapsulation within IP*) **[2].**
- Encapsulación de Ruta Genérica (**GRE** - *Generic Routing Encapsulation*) **[4].**
- Protocolo de *Tunneling* de Capa 2 (**L2TP** - *Layer 2 Tunneling Protocol*) **[5].**
- Protocolo de Seguridad IP (**IPSec** - IP Security Protocol) **[1].**
- Conmutación de Etiquetas de Multiprotocolos (**MPLS** - *Multiprotocol Label Switching*).

Mientras algunos de estos protocolos no se pensaron como protocolos de *tunneling*; hacen que cada uno tenga en cuenta el transporte no transparente de tramas, como carga útil del paquete, a través de una red IP; con el envío se desunen los campos de dirección de los paquetes encapsulados.

Sin embargo, hay una diferencia significativa entre cada uno de los protocolos

tunneling IP mencionados y el MPLS. El MPLS se puede ver como capa de enlace para el IP; en cuanto los mecanismos de MPLS se aplican solamente dentro del alcance de una red MPLS; mientras que los mecanismos basados en IP se extienden al alcance de accesibilidad IP. Como tal, los mecanismos de VPN construidos directamente sobre mecanismos de *tunneling* de MPLS no pueden, por definición, extenderse fuera del alcance de las redes de MPLS; por ejemplo, los mecanismos basados en ATM tales como LANE pueden extenderse fuera de redes ATM. Observe sin embargo, que una red de MPLS puede atravesar muchas tecnologías de capa de enlace, y por eso, como una red IP, su alcance no es limitado por las capas específicas del enlace usado.

Hay un número de requisitos deseables para un mecanismo de *tunneling* VPN, sin embargo, no todos son resueltos por los mecanismos *tunneling* existentes. Estos requisitos incluyen:

- Multiplexación.
- Protocolo de señalización.
- Seguridad de datos.
- Transporte multiprotocolo.
- Secuencia de tramas.
- Mantenimiento de túnel.
- MTUs grandes.
- Minimización de la cabecera del túnel.
- Control de congestión y de flujo.
- Administración de QoS / trafico.

- Multiplexación

Los túneles múltiples de VPNs pueden ser necesarios entre dos puntos IP remotos, por ejemplo, en casos donde las VPNs están basadas en redes, y cada punto extremo contiene múltiples clientes. El tráfico de diversos clientes viaja sobre túneles separados entre los dos dispositivos. Un campo de multiplexación es necesario para distinguir el paquete que pertenece a un túnel específico. Compartir un túnel de este modo puede también reducir la latencia y el proceso del sistema del túnel. Los mecanismos existentes del *tunneling* IP como el L2TP (vía los campos túnel-id y sesión-id), MPLS (vía la etiqueta) e IPSec (vía el campo del Índice del Parámetro de Seguridad (**SPI** - *Security Parameter Index*)) tienen un

mecanismo de multiplexación. En sentido estricto GRE no tiene un campo de multiplexación. Sin embargo el Campo de Llave (*key field*), que se propuso ser utilizado para autenticar la fuente de un paquete, se ha utilizado a veces como campo de multiplexación. IP/IP no tiene un campo de multiplexación.

El IETF y el foro de ATM han estandardizado en un solo formato como un identificador único global que es usado para identificar un VPN (VPN-ID). Un VPN-ID se puede utilizar en el plano de control, para atar un túnel a un VPN en el tiempo del establecimiento del túnel, o en el plano de datos, para identificar el VPN asociado a un paquete, sobre una base por-paquete. En el plano de datos, una cabecera encapsulada de VPN se puede utilizar por MPLS, MPOA y otros mecanismos de *tunneling* para agregar los paquetes de diversos VPNs sobre un solo túnel. En este caso una indicación explícita de VPN-ID se incluye con cada paquete, y no hace uso de ningún campo específico de multiplexación del túnel. En el plano de control, un campo de VPN-ID se puede incluir en cualquier protocolo de señalización de establecimiento del túnel para tener en cuenta la asociación de un túnel con un VPN (por ejemplo, según lo identificado por el campo de SPI). En este caso no hay necesidad de incluir un VPN-ID en cada paquete de datos. Esto se discute más adelante en el Capitulo II en la sección 2.1.1 - B.1.

- Protocolo de señalización

La información acerca de la configuración del punto extremo se debe conocer en el establecimiento del túnel, como las direcciones IP del punto extremo, la cualidad del túnel requerido y el nivel de seguridad necesitado. Una vez que esta información esté disponible, el establecimiento del túnel puede ser completado en una de dos maneras: *vía una operación de administración*, o *vía un protocolo de señalización* que permita que los túneles sean establecidos dinámicamente.

Un ejemplo de una *operación de administración* sería utilizar una Base de Información de Administración (**MIB** - *Management Information Base*) del SNMP para configurar los diferentes parámetros de *tunneling*, por ejemplo, etiquetas de MPLS, direcciones fuentes para ser utilizado en los túneles del IP/IP o del GRE, túnel-ids y sesión-ids de L2TP, o parámetros de asociación de seguridad para el IPSec.

Usar un protocolo de señalización puede reducir perceptiblemente la carga de administración, sin embargo es esencial en muchos escenarios de despliegue. Reduce la

cantidad de configuración necesaria y también reduce la coordinación de administración si un VPN atraviesa múltiples dominios administrativos. Por ejemplo, el valor del campo de multiplexación es local al nodo que asigna el valor, y puede mantenerse local si es distribuido vía un protocolo de señalización; por lo contrario si primero es configurado en una estación de administración y en seguida distribuido a los nodos importantes. Un protocolo de señalización también permite establecer los túneles a pedido o a demanda a los nodos que son móviles o están conectados de manera intermitentemente.

Cuando se está utilizando un protocolo de señalización en un ambiente de VPN, este debe permitir el transporte de un VPN-ID, para permitir que el túnel resultante sea asociado a un VPN particular. Esto también debería permitir que las cualidades de túnel sean intercambiados o negociados, por ejemplo el uso de secuencia de tramas o el uso del transporte de multiprotocolos. Nótese que el papel del protocolo de señalización es para negociar las cualidades de túnel, y no lleva la información acerca de como el túnel es usado: por ejemplo si las tramas llevadas en el túnel son enviadas en la capa 2 o la capa 3. Esto es similar a la señalización ATM Q.2931 - el mismo protocolo de señalización se utiliza para instalar una subred lógica clásica IP así como para LANs emulados (LANE).

De los diversos protocolos *tunneling* IP, los siguientes contienen un protocolo de señalización que se podría adaptar para este propósito: L2TP (el protocolo de control de L2TP), IPSec (el protocolo del Intercambio de la Llave del Internet (**IKE** - *Internet Key Exchange*) **[6]**), y el GRE (utilizado con móvil-IP *tunneling*). También hay dos protocolos de señalización MPLS que puede ser utilizado para establecer los túneles LSP: uno utiliza extensiones para el Protocolo de Distribución de Etiqueta (**LDP** - *Label Distribution Protocol*) del MPLS, y el otro utiliza extensiones al Protocolo de Reserva de Recurso (**RSVP** - *Resource Reservation Protocol*) para los túneles de LSP.

- Seguridad de datos

Un protocolo *tunneling* VPN debe proveer mecanismos para permitir cualquier nivel de seguridad que puede ser deseado por los clientes; incluyendo la autentificación y/o el cifrado. Ninguno de los mecanismos de *tunneling* discutidos, con excepción del IPSec, tienen mecanismos de seguridad intrínseca, pero confían en las características de seguridad del *backbone* IP. En particular, MPLS confía en el etiquetado explícito del camino conmutado de etiquetas para asegurarse de que los paquetes no pueden estar sin dirección,

mientras que los otros mecanismos de *tunneling* se pueden asegurar con el uso del IPSec. Para VPNs implementados sobre un *backbone* no IP (por ejemplo., MPOA, Frame Relay o circuitos virtuales ATM), la seguridad de datos son proporcionados implícitamente por la infraestructura conmutada de la *capa de enlace*.

La seguridad del VPN no es una capacidad de los túneles solamente, sino tiene que ser vista en el contexto más amplio de cómo los paquetes se envía sobre esos túneles. Por ejemplo con VPRNs implementados con *routers* virtuales, el uso del encaminamiento separado y los casos de la tabla de reenvío asegura el aislamiento del tráfico entre VPNs. Los paquetes en un VPN no pueden estar desorientados hacia un túnel de un segundo VPN puesto que esos túneles no son visibles a la tabla de envío del primer VPN.

Si el mecanismo de señalización es utilizado por uno de los puntos extremos del VPN para establecer dinámicamente un túnel con otro punto extremo, entonces hay un requisito para poder autenticar el punto extremo que procura el establecimiento del túnel. IPSec tiene un arreglo de esquemas para este propósito, permitiendo, por ejemplo, que la autentificación sea basada en llaves precompartida, o utilicen firmas digitales y certificados. Otros esquemas de *tunneling* tienen formas más simples de autentificación. En algunos casos pueda ser necesario la no-autentificación.

Actualmente el protocolo de Datos Seguros Encapsulados (**ESP** - *Encapsulating Security Payload*) **[7]** de IPSec puede ser usado para establecer el SAs que provee cifrado o autentificación o ambas. Sin embargo la especificación del protocolo imposibilita el uso de un SA donde no se usa cifrado o autentificación.

- Transporte de multiprotocolo

En muchas aplicaciones de VPNs, el VPN puede llevar tráfico multiprotocolo no transparente. Como tal, el protocolo *tunneling* usado debe también proveer transporte de multiprotocolo. L2TP esta diseñado para transportar paquetes de Protocolo Punto a Punto (**PPP** - *Point-to-Point Protocol*) **[8]**. GRE también provee la identificación del protocolo en el túnel. Los túneles del IP/IP y del IPSec no tienen tal campo de identificación de protocolo, puesto que el tráfico en el túnel se asume que es IP.

Es posible extender la suite del protocolo IPSec para tener en cuenta el transporte de paquetes multiprotocolo. Esto se puede alcanzar, por ejemplo, extendiendo el componente de señalización del IPSec - IKE, que indica el tipo de protocolo en el tráfico del túnel, o

lleva una cabecera de multiplexación en cada paquete del túnel (por ejemplo, una cabecera de LLC/SNAP o cabecera de GRE). Este método es similar al usado para el mismo propósito en redes ATM, donde se utiliza la señalización para indicar el encapsulado usado en el VCC, y donde los paquetes enviados en el VCC pueden utilizar una cabecera de LLC/SNAP o colocar directamente en la carga útil del AAL5, esto último es conocido como VC-*multiplexing* **[9]**.

- Secuencia de tramas

Una cualidad de la calidad de servicio requerida por los clientes de un VPN puede ser la secuencia de tramas, que es equivalente a la característica de las líneas físicas permanentes o de conexiones dedicadas. La secuencia puede ser requerida para una operación eficiente de protocolos o aplicaciones particulares de extremo a extremo. Para implementar la secuencia de trama, el mecanismo de *tunneling* debe contener un campo de secuencia. L2TP y GRE tienen tal campo. IPSec tiene un campo de número de secuencia, pero es utilizado por un receptor para realizar un chequeo contra la repetición, y no garantiza la entrega en orden de los paquetes.

Es posible ampliar IPSec para permitir el uso del campo de secuencia existente para garantizar la entrega en orden de los paquetes. Esto se puede alcanzar, por ejemplo, usando IKE para negociar la secuencia, y para definir un comportamiento del punto extremo que preserve la secuencia de paquetes.

- Mantenimiento de túnel

Los puntos extremos de un VPN deben supervisar la operación de los túneles del VPN para asegurarse de que la conectividad no se ha perdido, y para tomar la acción apropiada (tal como recálculo de la ruta) si ha habido una falla.

Hay dos métodos posibles. Uno es que por sí mismo el protocolo de *tunneling* compruebe periódicamente si hay pérdida de conectividad y proporcione una indicación explícita de la falla. Por ejemplo L2TP tiene un mecanismo opcional de *keep*-alive que permite detectar los túneles no operativos.

El otro método no requiere que por sí mismo el protocolo de *tunneling* realice esta función, sino confía en la operación de algún mecanismo externo para determinar la

pérdida de conectividad. Por ejemplo si un protocolo de encaminamiento tal como el Protocolo de Información de Encaminamiento (**RIP** - *Routing Information Protocol*) **[10]** o Primer Camino Abierto más Corto (**OSPF** - *Open Shortest Path First*) **[11]** que funcionan sobre una maya de túneles, al escuchar una falla desde un vecino dentro de cierto período de tiempo dará lugar a que el protocolo de encaminamiento declare que el túnel no esta activo. Otro método de fuera de banda (*out-of-band*) es realizar pings ICMP regulares. Esto es suficiente para asegurar que el túnel está operativo, debido al hecho que el túnel también funciona a través del mismo *backbone* IP.

Cuando los túneles se establecen dinámicamente, se necesita una diferenciación entre la información requerida por el túnel estático y dinámico. Antes de que un túnel pueda ser establecido, es necesaria una información estática en el nodo, tal como la identificación del punto extremo remoto y las cualidades del túnel. Esto es típicamente el resultado de una operación de configuración. Como resultado del intercambio de señalización, para establecer un túnel, se estable un estado dinámico ce en cada punto extremo, como en el valor del campo de multiplexación o de las llaves que se utiliza. Por ejemplo con IPSec, el establecimiento de una Asociación de Seguridad (**SA** - *Security Association*) coloca el tiempo de vida de ese SA en lugar las llaves que se utilizan.

Se pueden utilizar diferentes políticas en el establecimiento de un túnel dinámico. Un método es utilizar datos de manejo para accionar el establecimiento del túnel, siempre que exista datos a transferir, y para pausar el túnel debido a su inactividad. Este método es particularmente útil si los recursos para el túnel se están asignando en la red para los propósitos de QoS. Otro método es accionar el establecimiento del túnel siempre que la información de configuración de túnel estático esté instalada, y procurar mantener activo al túnel todo el tiempo.

- MTUs grandes

Un túnel IP tiene asociado una Unidad de Transmisión Máxima (**MTU** - *Maximum Transmission Unit*). Es concebible que este MTU puede ser más grande que el MTU de unos o más saltos individuales a lo largo de la trayectoria entre los puntos finales del túnel. Si es así, se requiere fragmentación de trama dentro del túnel.

Si la trama que se transferirá esta dentro de un *datagram* IP, la fragmentación IP normal ocurrirá cuando el *datagram* IP alcance un salto con un MTU más pequeño que el

MTU del túnel IP. Esto puede tener implicaciones indeseables en el funcionamiento del *router* que realiza la fragmentación de túnel.

Un método alternativo que favorece al protocolo de *tunneling* es que por sí mismo incorpora una capacidad de segmentación y de reensamble y funciona a nivel del túnel, a lo mejor usando el número de secuencia del túnel y un marcado de fin de mensaje de algún tipo. (Note que el PPP multi-enlace utiliza un mecanismo similar a esto para fragmentar paquetes). Este evita la fragmentación a nivel IP dentro del mismo túnel. Ningunos de los protocolos de *tunneling* existentes contienen tal mecanismo.

- Minimización de la cabecera del túnel

Existe un beneficio en la minimización de la cabecera de cualquier mecanismo de *tunneling*. Esto es particularmente importante para el transporte de tráfico sensible al *jitter* y a la latencia como la voz y el vídeo paquetizado. Por otra parte, el uso de los mecanismos de seguridad, tales como IPSec, impone sus propias cabeceras, por lo tanto el objetivo debe ser minimizar la cabecera necesitada en la seguridad, y no cargar esos túneles en los cuales la seguridad no sea obligatoria con cabeceras innecesarias.

Un área donde la cantidad de cabeceras puede ser significativa es cuando un *tunneling* voluntario se utiliza para una conexión conmutada de clientes remotos a un VPN, debido al poco ancho de banda de un enlace *dial up*. Esto se discute más adelante en el Capitulo II en la sección 2.1.1 - C.3.

- Control de flujo y de congestión

Los procedimientos del protocolo L2TP fueron desarrollados para el control de flujo y de congestión. En primer lugar esto fue necesario debido al requerimiento de proporcionar un funcionamiento adecuado sobre redes con pérdidas, cuando la compresión del PPP, que es diferente al Protocolo de Compresión IP de Carga útil (**IPComp** - *IP Payload Compression Protocol*). Otra motivación era acomodar los dispositivos con *buffering* muy pequeño, usado por ejemplo para terminar en líneas conmutadas de velocidad baja. Sin embargo los mecanismos de control de flujo y de congestión, definidos en la versión final de la especificación de L2TP, utilizados solamente para los canales de control y no para tráfico de datos.

En general las interacciones entre las múltiples capas con esquema de control de flujo y de congestión pueden ser muy complejas. Dado el predominio del tráfico TCP en las redes de hoy y el factor de que el TCP tiene sus propios mecanismos de control de flujo y de congestión de extremo a extremo, no está claro que hubiera mucha ventaja para implementar mecanismos similares dentro de protocolos de *tunneling*. Los buenos esquemas de control de flujo y de congestión pueden adaptarse a una variedad amplia de condiciones y de escenarios de despliegue de la red; son complejos para el desarrollo y prueba, ambos por sí mismos, y entendiendo la interacción con otros esquemas que puedan funcionar en paralelo. Puede haber ventaja, sin embargo, tener la capacidad por el que un emisor pueda enviar tráfico a la capacidad de un receptor y suministrar los mecanismos de protocolo para permitir que un receptor señale sus capacidades al emisor.

- Administración de QoS / trafico

Según lo discutido, los clientes pueden requerir que el comportamiento del VPN sea similar al rendimiento de las líneas arrendadas físicas o a las conexiones dedicadas con respecto a los parámetros de QoS como garantía de tasa de perdidas, del jitter, de la latencia y del ancho de banda. Cómo tales garantías pueden ser entregadas y ser una función de la característica de administración del tráfico de los nodos del VPN, de la red de acceso y del *backbone* a través del cual están conectados.

Una discusión completa de QoS y de VPNs está fuera del alcance de este informe, no obstante modelando un túnel de VPN como otro tipo de capa de enlace, muchos de los mecanismos existentes desarrollados para asegurar el QoS sobre enlace físicos pueden también ser aplicados. Por ejemplo en un nodo de VPN, los mecanismos de vigilar, etiquetar, enfilar, formar y programar (*policing, marking, queuing, shaping and scheduling*) pueden ser aplicados al tráfico de VPN con los parámetros de VPN específicos, hacer cola e interfaces, tal como para tráfico no VPN. Las técnicas desarrolladas para Diffserv, Intserv y para la ingeniería del tráfico en MPLS son también aplicables. Vea también **[15]** para una discusión de QoS y de VPNs.

Sin embargo, debe observar que este modelo de operación de túnel no es constante con el método en el cual los protocolos de *tunneling* son modelados actualmente. Mientras que un modelo es una ayuda a la comprensión, y no parte de una especificación del protocolo; tener diferentes modelos pueden complicar discusiones, particularmente si un modelo se

mal interpreta como parte de una especificación del protocolo o como obligación de la opción del método implementado. Por ejemplo, el proceso del túnel de IPSec se puede modelar en ambos como interfaz y como una cualidad particular del flujo de paquetes.

1.3.2 Recomendaciones

IPSec es necesario siempre que exista un requisito para un cifrado o una autentificación. Esto también provee la multiplexación y un protocolo de señalización - IKE. No obstante, extender la suite del protocolo IPSec, también para cubrir las siguientes áreas sería beneficioso, para proveer los requisitos *tunneling* en un ambiente VPN.

- El transporte de un VPN-ID donde establecen un SA (*Signalling Protocol*)
- Una opción de cifrado nulo y autenticación nula (*Data Security*)
- Operación de multiprotocolo (*Multiprotocol Transport*)
- Secuencia de tramas (*Frame Secuency*)

L2TP no proporciona ninguna seguridad de datos y el mecanismo usado para seguridad PPP no se aplican al protocolo L2TP por sí mismo, de modo que la seguridad sea proporcionado por L2TP, este debe funcionar sobre IPSec. Definir un modo específico de operación para el IPSec, cuando es utilizado para contener el tráfico de L2TP, ayudará a la interoperabilidad.

Las implementaciones de VPN se han convertido más y más complejas y para su solución los servicios de VPN modernos recorren una gran variedad de tecnologías y topologías.

En capitulo siguiente se mostrará una clasificación según tipos de IP VPN dados en el RFC 2764, una división en categorías según alcance de las VPN para las organizaciones, además se mencionará las características y topología de cada uno de los tipos de VPN y se clasificará los VPNs según modelos implementados superpuestos, y par a par. También se tratará de los tipos de protocolos *tunneling* mas conocidos, se mencionará las características de cada protocolo.

CAPITULO II
TIPOS, CLASIFICASIÓN Y PROTOCOLOS DE UNA VPN

2.1 Tipos de VPN

Los tipos de VPN serán tratados en este documento de la siguiente manera:

- Según el RFC 2764
- Según el alcance de la VPN para la organización.

2.1.1 Tipos de VPN según RFC 2764

En esta sección mostraremos los tipos de VPNs según lo definido en el RFC 2764 y estos son los siguientes:

A. Línea Dedicada Virtual (**VLL** - *Virtual Leased Lines*)
B. Red Encaminada Privada Virtual (**VPRN** - *Virtual Private Routed Networks*)
C. Red de Marcado Privado Virtual (**VPDN** - *Virtual Private Dial Networks*)
D. Segmento LAN Privado Virtual (**VPLS** - *Virtual Private LAN Segments*)

También se mencionará las características y topología de cada uno de los tipos de VPN según el RFC 2764.

A. Línea Dedicada Virtual (VLL)

La forma más simple de un VPN es un servicio de "línea dedicada virtual". En este caso un enlace punto a punto es proporcionada a un cliente, conectando dos dispositivos del CPE, según se ilustrado en la figura 2.1. El tipo de *capa de enlace* usado para conectar los dispositivos del CPE con los nodos del ISP pueden ser por ejemplo un VCC ATM o un circuito Frame Relay. Los dispositivos del CPE pueden ser *routers, bridges* o *hosts*.

Los dos nodos ISP son conectados con una red IP, y un túnel IP se establece entre

ambos. Cada nodo del ISP se configura para unir el enlace *stub* y el túnel IP por medio de la capa 2 (por ejemplo, un VCC ATM y el túnel IP). Las tramas se retransmiten entre los dos enlaces. Por ejemplo la carga útil de la Capa de Adaptación ATM 5 (**AAL5** - *ATM Adaptation Layer 5*) se toma y se encapsula en un túnel de IPSec, y viceversa. El contenido de la carga útil AAL5 no es transparente al nodo del ISP, y no se examina allí.

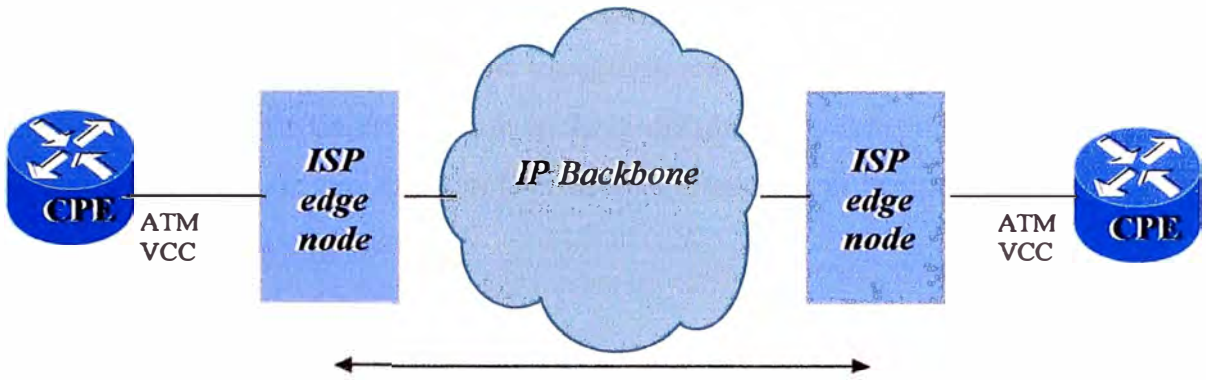

Figura 2.1: Ejemplo VLL

Un cliente observa como si fuera una sola VCC ATM o circuito Frame Relay, utilizada para interconectar los dispositivos del CPE. El cliente podría desconocer que la parte del circuito está implementado sobre un *backbone* IP. Esto puede ser útil, por ejemplo, si un proveedor desea proporcionar un servicio de interconexión LAN usando ATM como una interfase de red, pero no tiene una red ATM que interconecte directamente todos los sitios de cliente posibles.

No es necesario que los dos enlaces usados, que conectan los dispositivos del CPE con los nodos del ISP, estén en el mismo tipo de medio; pero en este caso los nodos del ISP no pueden tratar el tráfico de una manera no transparente. En lugar de ello los nodos del ISP deben realizar las funciones de dispositivo de trabajo entre los dos tipos de medios (por ejemplo, ATM y Frame Relay), y realizan funciones tales como LLC/SNAP para la conversión de NLPID, trazando entre las variantes del protocolo ARP y realizando un proceso específico de los medios que pueda ser esperado por los dispositivos del CPE (por ejemplo, *ATM OAM cell handling célula o Frame Relay XID Exchange*).

Observe que el uso del término "VLL" en este documento es diferente al usado en la definición del Envío Acelerado del Diffserv por el Comportamiento del Salto (**EF-PHB** - *Diffserv Expedited Forwarding Per Hop Behaviour*). En este documento un VLL se utiliza para indicar una latencia baja, un jitter bajo, un ancho de banda asegurado, y que se puede proporcionar usando el PHB descrito. Así, en primer lugar el enfoque está en la característica del enlace que es temporal por naturaleza. En este documento el término VLL no implica el uso de un mecanismo específico de QoS, Diffserv u otro. En lugar de ello el enfoque está sobre todo en las características del enlace que son más topológicas (por ejemplo, construir un enlace que incluya un túnel IP como un segmento de enlace). Para una emulación de una capa enlace ambos aspectos, el temporal y los topológicos, necesitan ser tomados en cuenta.

Requerimientos:

- Los mecanismos de *tunneling* IP son necesarios porque el envío desune los campos de dirección de los paquetes encapsulados, y permite el transporte no transparente de tramas como carga útil de paquete. Túneles por ejemplo, de IP/IP, de GRE, L2TP (paquetes del PPP), MPLS, e IPSec
- Proveer multiplexación VLL (e.g. túnel-id y call-id para L2TP, label MPLS)
- Proveer un protocolo de señalización, para negociar cualidades del túnel tales como el nivel de seguridad, direcciones IP de los puntos extremos remotos (por ejemplo, LDP de MPLS).
- Proveer seguridad de datos, que permite que los clientes especifiquen los niveles de seguridad.
- Proveer el transporte multiprotocolo
- Proveer secuencia de trama, requerido para garantizar la entrega en orden de paquetes.

B. Red Encaminada Privada Virtual (VPRN)

B.1. Característica de una VPRN

Una red encaminada privada virtual se define como una emulación de red encaminada de área amplia usando facilidades IP. Esta sección muestra cómo se puede proporcionar

una red basada en servicios VPRN. Con redes basadas en VPRNs, muchos de los temas necesitan ser involucrados con los temas de configuración y de operación, que debe ser tomado en cuenta en la división de la responsabilidad administrativa entre el proveedor de servicio y el usuario de servicio.

La característica que se distingue de un VPRN, en comparación a otros tipos de VPNs, es que el envío de paquete es realizado en la capa de red. Un VPRN consiste en un enlace de túneles IP, entre los *routers* del ISP, junto con las capacidades de encaminamiento necesario para enviar el tráfico recibido en cada nodo del VPRN al sitio apropiado del destino. Junto a los *routers* del ISP están los *routers* del CPE conectados vía uno o más enlaces, llamados enlaces *stub*. Hay una tabla de envío de VPRN en cada *router* del ISP con la cual los miembros del VPRN están conectados. El tráfico se envía entre los *routers* del ISP y los sitios del cliente, usando estas tablas de envío, que contienen la información de accesibilidad de la capa de red (en contraste a un tipo Segmento LAN Privado Virtual (VPLS) de VPN donde las tablas de envío contienen la información de accesibilidad de la capa MAC - vea la sección 2.1.1 - D).

Un ejemplo VPRN se ilustra en la figura 2.2, que demuestra 3 *routers* de borde del ISP, conectadas vía una malla completa de túneles IP, usado para interconectar 4 *routers* del CPE. Una de los *routers* del CPE es *multihomed* a la red del ISP. En el caso de *multihomed*, todos los enlaces *stub* pueden ser activos o según lo mostrado puede haber un primario y uno o más enlaces de reserva que se utilizarán en caso de que falle el primario. El término enlace secreto o "*backdoor*" se utiliza para referir a un enlace entre dos sitios de cliente, esto no atraviesa la red ISP.

La ventaja principal de un VPRN es que la complejidad y la configuración de los *routers* del CPE serán mínimas. A un *router* del CPE, el *router* de borde del ISP aparece como *router* vecino en la red del cliente, a la cual envía todo el tráfico, usando una ruta por defecto. La malla de túnel que se establece para transferir tráfico, que se extiende entre los *routers* de borde del ISP y no a los *routers* del CPE. En efecto la carga del establecimiento del túnel, del mantenimiento y de la configuración del encaminamiento es dada en *outsourcing* al ISP. Además, otro servicio necesario para la operación de un VPN es la disposición de un firewall y el proceso de QoS, lo cual es manejado por un número pequeño de *routers* de borde del ISP, y no por una gran cantidad de dispositivos potencialmente heterogéneos del CPE. La introducción y la administración de nuevos servicios pueden también ser manejadas más fácilmente, mientras que esto se puede

alcanzar sin la necesidad de aumentar los equipos del CPE. Esta última ventaja es particularmente importante cuando puede haber una gran cantidad de suscriptores residenciales usando servicios de VPN para tener acceso a redes corporativas privadas. De este modo, el modelo esta relacionado con el usado para los servicios de telefonía, por el que los nuevos servicios (por ejemplo, llamada en espera) se puedan introducir sin cambio en el equipo del suscriptor.

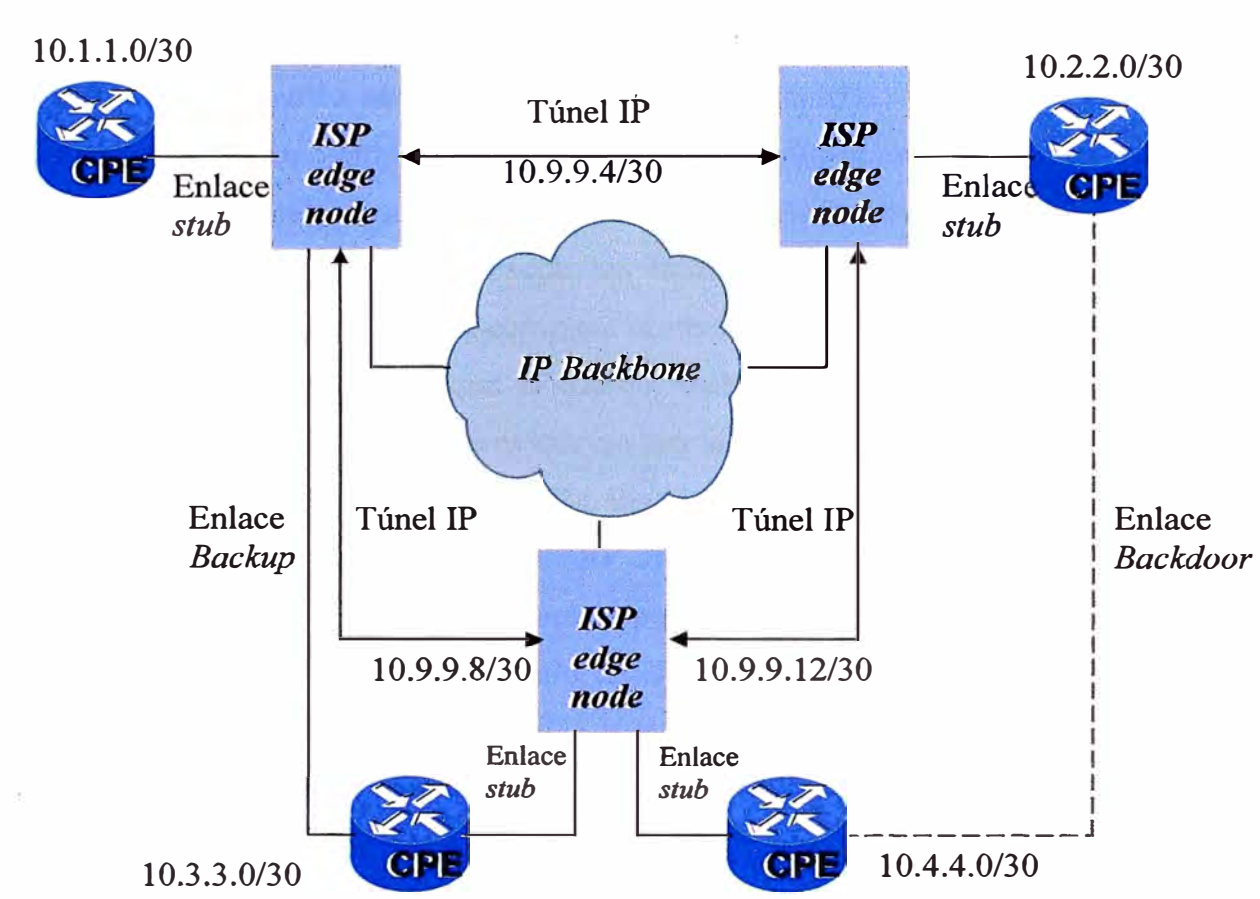

Figure 2.2: Ejemplo VPRN

El VPRN es en contraste a un tipo de VPN donde la malla de túneles se extiende a los *routers* del CPE, y donde la red del ISP proporciona conectividad de capa 2 solamente. El último caso se puede poner en ejecución como un sistema de VLLs entre los *routers* del CPE (véase la sección 2.1.1 - A), en el que la red del ISP proporciona un sistema de enlace de punto a punto de capa 2, o como VPLS (véase la sección 2.1.1 - D), en el cual la red del ISP se utiliza para emular un segmento LAN de multi acceso. Con estos escenarios un cliente puede tener más flexibilidad (por ejemplo, cualquier IGP o cualquier protocolo puede funcionar a través de todos los sitios del cliente) pero esto es posible generalmente a

expensas de una configuración más compleja para el cliente. Así, dependiendo de requisitos del cliente, un VPRN o un VPLS puede ser la solución más apropiada.

B.1.1 Topología

La topología de un VPRN puede consistir en una malla completa de túneles entre los nodos del VPRN, o puede ser una topología arbitraria, tal como un sistema de oficinas remotas conectadas con el sitio regional más cercano. Con VPRNs usando túneles IP, es mucho menos el costo asumido con el enmallado completo que en los casos donde los recursos físicos (por ejemplo, una línea arrendada) se deben asignar por cada par conectado en los sitios, o donde el método de *tunneling* requiere recursos para ser asignado en los dispositivos usados para interconectar los *routers* de borde (por ejemplo, Frame Relay DLCIs). Una topología de malla completa produce un encaminamiento óptimo, puesto que imposibilita la necesidad de que el tráfico, entre dos sitios, atraviese un tercero. Otra atracción de una malla completa es que no hay necesidad de configurar la información de la topología del VPRN. En lugar de ello, los *routers* miembros de un VPRN y la topología están implícitos. Si el número de *routers* de borde del ISP en un VPRN es muy grande, entonces una topología de malla completa puede no ser apropiada, debido al escalamiento implicada. Por ejemplo, el crecimiento en el número de los túneles necesitados entre los sitios, (que para los n sitios es n(n-1)/2), o el número de encaminamiento es observado por el *router*. La política de red puede también conducir topologías de malla no completas, por ejemplo un administrador puede desear establecer la topología de modo que el tráfico entre dos sitios remotos pase a través de un sitio central, y no pase directamente entre los sitios remotos. Es también necesario ocuparse del escenario donde hay conectividad parcial, a través del *backbone* IP, bajo ciertas condiciones de error (por ejemplo, A puede alcanzar B, y B puede alcanzar C, pero A no puede alcanzar C directamente), que pueden ocurrir si se está utilizando la política de encaminamiento.

Para una red basada en VPRN, se asume que cada *router* del CPE en el sitio del cliente se conecta con un *router* de borde del ISP a través de uno o más enlaces *stub* punto a punto (por ejemplo, líneas dedicadas, conexiones ATM o Frame Relay). Los *routers* del ISP son responsables de aprender y de diseminar la información de accesibilidad entre sí. Los *routers* del CPE deben aprender el sistema de destinos accesibles vía cada enlace *stub*, aunque ésta puede ser tan simple como un *router* por defecto.

El enlace *stub* puede ser enlace dedicado. Se establece vía aprovisionamiento, o puede ser enlace dinámico establecido en demanda, por ejemplo con PPP, *tunneling* voluntario (véase la sección 2.1.1 - C), o señalización ATM. Con enlaces dinámicos es necesario autenticar al suscripto y determinar los recursos autorizados a que el suscriptor puede tener acceso (por ejemplo, a que VPRNs el suscriptor puede unirse). Aparte de la manera que el suscriptor está delimitado inicialmente al VPRN, (y a este proceso puede implicar consideraciones adicionales tales como asignación de direcciones IP dinámicas), los mecanismos y servicios de VPRN subsecuentes se pueden utilizar para ambos tipos de suscriptores de la misma manera.

B.1.2 Dirección

La dirección usada dentro de un VPRN no puede tener relación a la dirección usada en el *backbone* IP sobre cual el VPRN es implementado. En particular pueden usarse la dirección IP privado no-único. Múltiple VPRNs pueden ser implementados sobre el mismo sistema de dispositivos físicos, y pueden utilizar lo mismo o cubrir una parte de direcciones.

B.1.3 Envío

Para una VPRN la malla de túneles forma una red de recubrimiento que funciona sobre un *backbone* IP. Dentro de cada uno de los *routers* de borde del ISP debe haber un estado específico de envío de VPN para enviar los paquetes recibidos de los enlaces *stub* ("tráfico del ingreso") al siguiente salto apropiado del *router*, y envío de paquetes recibidos del núcleo ("tráfico de salida") al enlace *stub* apropiado. Para los casos donde un *router* de borde del ISP contiene los múltiples enlaces *stub* que pertenecen al mismo VPRN, los túneles pueden terminar en el *router* de borde, o en un enlace *stub*. En el caso anterior, una tabla específica de envío de un VPN es necesaria para el tráfico de salida, en el último caso esto no es necesario. Una tabla específica de envío de un VPN se necesita generalmente en la dirección de ingreso, para dirigir el tráfico recibido en un enlace *stub* sobre el túnel IP correcto hacia el núcleo.

Puesto que un VPRN funciona en la capa de red interna, los paquetes IP enviados sobre un túnel tendrán su campo el Tiempo Para Vivir (**TTL** - *Time to Live*) decreciendo de

manera normal, previniendo los paquetes que circulan indefinidamente en el lazo de encaminamiento dentro del VPRN.

B.1.4 Conectividad múltiple de VPRN concurrente.

Observe también que un solo sitio del cliente puede pertenecer concurrentemente a múltiples VPRNs y puede desear transmitir tráfico sobre uno o más VPRNs y al Internet, sobre el mismo enlace *stub*. Hay varios métodos posibles para este problema, pero éstos están fuera del alcance de este informe.

B.2. Requisitos genéricos de una VPRN

Hay un número de requisitos comunes, que cualquier red basada en soluciones VPRN debe abordar, y hay diversos mecanismos que se pueden utilizar para resolver estos requisitos. Estas cuestiones genéricas son:

1.- El uso de un **identificador** global único de VPN para poder referir a un VPN particular.
2.- **Determinación de membresía del VPRN**. Un *router* de borde debe aprende de los enlaces *stub* locales que están en cada VPRN, y debe aprender del sistema de otros *routers* que tenga miembros en ése VPRN.
3.- **Información de accesibilidad del enlace *stub***. Un *router* de borde debe aprender que el sistema de direcciones y de prefijos de dirección accesibles vía cada *stub*.
4.- **Información de accesibilidad de Intra-VPRN**. Una vez que un *router* de borde haya determinado el sistema de prefijos de dirección asociados con cada uno de sus enlaces *stub*, después esta información se debe diseminar a cualquier otro *router* de borde en el VPRN.
5.- **Mecanismo de *tunneling***. Un *router* de borde debe construir los túneles necesarios a otras *routers* que tengan miembros en el VPRN, y debe realizar el encapsulado y el desencapsulado necesario para enviar y recibir los paquetes sobre los túneles.

C. Redes de Marcado Privados Virtuales (VPDN)

Una red de marcado privada virtual (VPDN) permite a un usuario remoto conectarse en demanda a través de un túnel *ad hoc* dentro de otro lugar. El usuario es conectado a una red IP pública vía un enlace de marcación a la PSTN o ISDN, y los paquetes del usuario son enviados a través de la red pública hacia el sitio deseado, dando la impresión al usuario de estar conectado directamente en ese sitio. Una característica clave de tales conexiones *ad hoc* es la necesidad de la autentificación del usuario como primer requisito, puesto que cualquier persona podría potencialmente intentar acceder a tal sitio usando una red de marcación conmutada.

Actualmente, muchas redes corporativas permiten el acceso a los usuarios remotos a través de conexiones de marcado hechas a través del PSTN, con usuarios estableciendo conexiones tipo PPP a través de una red de acceso a un servidor de acceso de red, punto en el cual las sesiones tipo PPP son autentificadas usando los sistemas AAA corriendo protocolos estándares tales como Radius. Dado el despliegue de tales sistemas, cualquier sistema de VPDN debe permitir en la práctica la reutilización transparente de tales sistemas existentes.

El IETF ha desarrollado el L2TP **[5]** que permite la extensión de las sesiones PPP del usuario desde un Concentrador de Acceso del L2TP (**LAC** - *L2TP Access Concentrator*) a un Servidor de Red del L2TP (**LNS** - *L2TP Network Server*) remoto. El protocolo de L2TP fue basado en dos protocolos anteriores, el Protocolo de Reenvío de Capa 2 (**L2F** - *Layer 2 Forwarding*) **[12]**, y el Protocolo *Tunneling* Punto a Punto (**PPTP** - *Point-to-Point Tunneling Protocol*) **[13]**, y esto se refleja en los dos panoramas absolutamente diversos para los cuales L2TP puede ser utilizado como *tunneling* obligatorio y *tunneling* voluntario.

Este documento se centra en el uso de L2TP sobre una red del IP (que usa el UDP), pero L2TP puede también funcionar directamente sobre otros protocolos tales como ATM o Frame Relay. Temas relacionados específicamente con el funcionamiento del L2TP sobre las redes no-IP, como por ejemplo cómo asegurar tales túneles, no se tratan aquí.

C.1. Características del protocolo de L2TP

Esta sección apunta las características del protocolo *tunneling* L2TP usando las categorías descritas en la sección 1.3.

C.1.1 Multiplexación

L2TP tiene soporte inherente para la multiplexación de múltiples llamadas de diversos usuarios sobre un solo enlace. Entre los mismos dos puntos finales de IP, puede haber múltiples túneles de L2TP, según lo identificado por una túnel-id, y múltiples sesiones dentro de un túnel, según lo identificado por una sesión-id.

C.1.2 Señalización

Esto es contenido vía el protocolo de conexión de control incorporado, permitiendo que los túneles y las sesiones se establezcan dinámicamente.

C.1.3 Seguridad de Datos

Teniendo en cuenta la extensión transparente del PPP desde el usuario, a través del LAC hacia el LNS, el L2TP permite el uso de cualquier mecanismo de seguridad. Con respecto a ambas conexiones y la transferencia de datos puede ser utilizado con las conexiones normales de PPP. Sin embargo esto no provee seguridad a causa del protocolo de control del L2TP. En este caso L2TP podría ser seguro, si este funciona conjuntamente con IPSec a través del *backbone* IP o mecanismos relacionados en *backbone* no IP.

La interacción del L2TP con los sistemas AAA en la autentificación y la autorización del usuario, es una función por el cual L2TP es usado con los dispositivos que contienen el LAC y el LNS.

Los medios por los cuales el *host* determina el LAC correcto a la cual conectarse, y los medios por los cuales el LAC determina qué usuarios fomentan el túnel, y los parámetros del LNS asociados a cada usuario, esta fuera del alcance de la operación de un VPDN, pero puede ser tratado, por ejemplo, desarrollando las especificaciones del Internet.

C.2. *Tunneling* obligatorio

El *tunneling* obligatorio se refiere al escenario en el cual un nodo de la red - un *dial* o un servidor de acceso de red, por ejemplo, actuando como un LAC, extiende una sesión PPP a través de un *backbone* usando L2TP hacía un LNS remoto, según lo mostrado en la figura 2.3. Esta operación es transparente al usuario que inicia la sesión PPP hacía el LAC. Esto permite el desacoplo de la localización y/o el dominio de la combinación de módems usados para terminar las llamadas marcadas, desde el sitio en el cual los usuarios tienen acceso. Lo contenido para este escenario fue el intento original de la especificación del L2F, sobre la cual la especificación L2TP fue basada.

Existen diferentes escenarios, un ejemplo es mostrado en la figura 2.3, donde un *host* del suscriptor marca en un NAS que actúa como LAC, y hace *tunneling* a través de una red IP (por ejemplo el Internet) a una entrada que actúa como LNS. El *gateway* proporciona el acceso a una red corporativa, y podría ser un dispositivo de la red corporativa, o podría ser un *router* de borde del ISP, en el caso donde un cliente tiene en *outsourcing* el mantenimiento de la funcionalidad del LNS hacia un ISP. Otro escenario es donde una ISP utiliza el L2TP para proveer a un suscriptor, acceso a Internet. El *host* suscriptor marca en el NAS que actúa como LAC, y hace tunneling a través de una red de acceso a un *router* de borde del ISP comportándose como un LNS. Este *router* de borde del ISP alimenta el tráfico del suscriptor en el Internet. Aunque otros escenarios son donde un ISP usa el L2TP para proveer un suscriptor con acceso a un VPRN, o con acceso concurrente a un VPRN y al Internet.

Un VPDN se puede ver como otro tipo de método de acceso para el tráfico del suscriptor, si se esta usando un *tunneling* obligatorio o voluntario, y como tales se pueden utilizar para proporcionar conectividad a diversos tipos de redes, por ejemplo una red corporativa, al Internet, o un VPRN. El escenario anterior es también un ejemplo de cómo un servicio de VPN vista desde el punto del cliente, se puede ejecutar usando una combinación de diversos tipos de VPN.

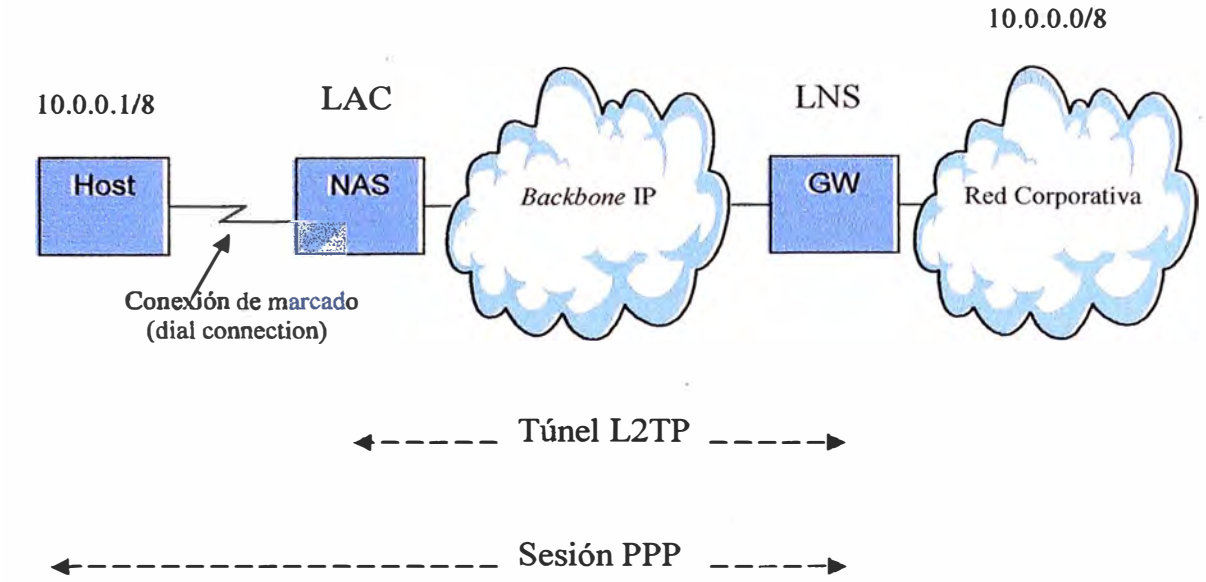

Figura 2.3: Ejemplo de *tunneling* obligatorio

El *tunneling* obligatorio fue pensado originalmente para el despliegue en los servidores de acceso de red, que contiene al por mayor el servicios de marcado, permitiendo el acceso remoto de marcado a través de instalaciones comunes en el sitio de la empresa, mientras que imposibilita la necesidad de que la empresa despliegue sus propios servidores de marcación. Otro ejemplo de esto es donde un ISP en *outsourcing* tiene su propia conectividad de marcado hacia un proveedor de red de acceso, tal como un Portador de Intercambio Local (**LEC** - *Local Exchange Carrier*), que elimina la necesidad de que un ISP mantenga sus propios servidores de marcado y que permite que el LEC sirva múltiples ISPs. Más recientemente, los mecanismos de *tunneling* obligatorio también se han propuesto para desarrollar los servicios de Línea de Suscriptor Digital (**DSL** - *Digital Subscriber Line*), los cuales también intentan influenciar la infraestructura existente AAA.

C.3. Túneles Voluntarios

El *tunneling* voluntario se refiere al caso donde un *host* individual se conecta con un sitio remoto usando un túnel originado en el *host*, sin intervención de nodos de red intermedios, como se muestra en la figura 2.4. La especificación PPTP, parte del cual se ha incorporado en el L2TP, fue basado sobre un modelo de *tunneling* voluntario.

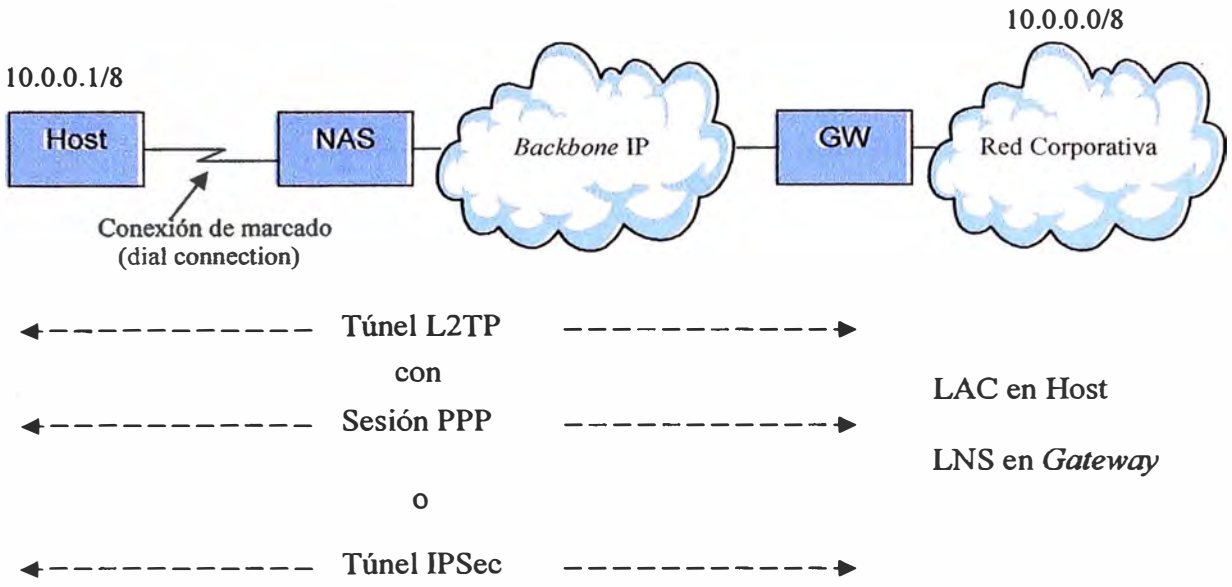

Figura 2.4: Ejemplo de *tunneling* voluntario

D. Segmento LAN Privado Virtual (VPLS)

Un segmento LAN privado virtual (VPLS) es la emulación de un segmento LAN usando instalaciones de Internet. Un VPLS puede ser usado para proveer lo que es también conocido como un Servicio Transparente LAN (**TLS** - *Transparent LAN Service*), que se puede utilizar para interconectar múltiples *stub* de nodos del CPE, *bridge* o *routers*, de una manera transparente del protocolo. Un VPLS emula un segmento de LAN sobre IP, de la misma manera que protocolos tales como LANE emulan un segmento del LAN sobre ATM. Las ventajas primarias de un VPLS es la transparencia completa del protocolo, que puede ser importante para el transporte de multiprotocolos y por razones reguladoras en contextos particulares del proveedor de servicio.

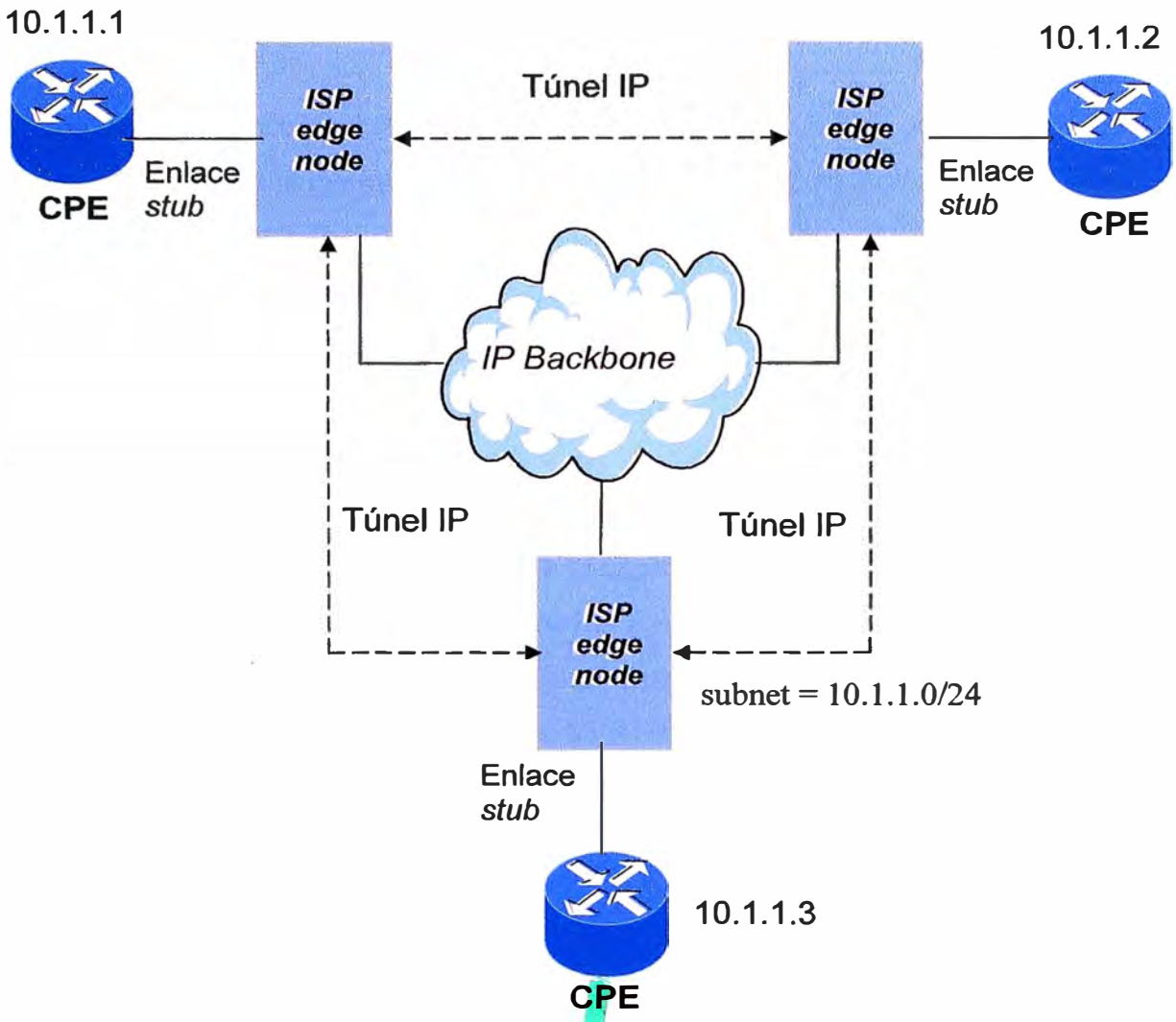

Figura 2.4: Ejemplo de VPLS

D.1. Requisitos de VPLS

Un VPLS fácilmente se puede modelar topológica y operacionalmente. Es esencialmente equivalente a un VPRN, excepto que cada nodo borde VPLS se implementa como un puente de capa de enlace más que un direccionamiento de capa de red. Como tal, la mayoría de *tunneling* VPRN y de mecanismos de la configuración discutidos previamente se pueden también utilizar para un VPLS, con los cambios apropiados de información de paquetes y de dirección para acomodar la capa de enlace, más que la capa de red. Las secciones siguientes discuten los cambios primarios necesarios en la operación de VPRN para proveer VPLSs.

D.1.1. Protocolo *Tunneling*

Los protocolos de *tunneling* empleados dentro de un VPLS pueden ser exactamente iguales que los usados dentro de un VPRN, si el protocolo *tunneling* permite el transporte del tráfico multiprotocolo.

D.1.2. Proveer multidifusión y difusión (*Multicast y Broadcast*)

Un VPLS necesita tener capacidad de *broadcast*. Esto es necesario para tramas *broadcast*, y para el exceso de paquetes en la capa de enlace, donde una trama *unicast* se excede porque la trayectoria al destino de la capa de enlace es desconocida. Los Protocolos de Resolución de Dirección (**ARP** - *Address Resolution Protocols*) que funcionan en una red *bridge* usan tramas *broadcast*. El mismo sistema de mecanismos posibles de *tunneling multicast* discutidos anteriormente para VPRNs se aplica también a un VPLS, aunque generalmente el uso más frecuente de *broadcast* en VPLSs puede aumentar la presión para contener el *multicast* nativo, por ejemplo, reduce la carga de la réplica en los nodos de borde del VPLS.

D.1.3. Configuración y topología de membresía del VPLS

La configuración de membresía del VPLS es análoga a la del VPRN puesto que ésta requiere del conocimiento de las asignaciones de los enlace locales del VPN en un determinado nodo de borde del VPLS, y la identidad o ruta de los otros nodos de borde del VPLS; en detalle, tal configuración es independiente de la naturaleza del reenvío en cada nodo de borde del VPN. Como tal, cualquiera de los mecanismos para la configuración y difusión de la membresía del VPN discutidos durante la configuración del VPRN puede ser aplicado a la configuración del VPLS. También como con VPRNs, la topología del VPLS puede ser manipulada fácilmente controlando la configuración de los nodos semejantes en cada nodo de borde del VPLS. Es probable que los VPLSs sean mallas completas, sin embargo, a fin de prevenir la necesidad del tráfico entre los dos nodos del VPLS se transmite a través de otro nodo de VPLS, lo que entonces requeriría el uso del protocolo *Spanning Tree* para la prevención del lazo.

D.1.4. Tipos de nodo stub del CPE

Un VPLS puede contener los *bridges* o los *routers* como dispositivo del CPE.

Los *routers* del CPE analizaran transparentemente a través de un VPLS sin requerir que el *router* analice cualquier nodo del VPLS. Los mismos asuntos de escalabilidad que se aplican a una topología de malla completa para VPRNs, solamente que ahora el número de *routers* que analicen es potencialmente mayor, puesto que el dispositivo de borde del ISP ya no actúa como punto de agregación.

Con los dispositivos *bridge* del CPE, el dominio de *broadcast* abarca todos los sitios así como también el VPLS por si mismo. Hay restricción significante de escalabilidad en este caso, debido a la necesidad del desborde del paquete, y el hecho de que cualquier cambio de la topología en el dominio de *bridge* no es localizado, pero es visible a través del dominio. Como tal este escenario generalmente se satisface para contener los protocolos *non-routable*.

La naturaleza del CPE afecta la naturaleza del encapsulado, de la dirección, del reenvío y de la accesibilidad del protocolo en el VPLS.

D.1.5. Encapsulado de paquetes del enlace *stub*

D.1.5.1. *Bridge* del CPE

En este caso, los paquetes enviados hacia y desde el VPLS a través de enlaces *stub* son tramas de la capa de enlace, con un encapsulado conveniente del enlace de acceso. El caso más común es probablemente la trama Ethernet, usando un encapsulado apropiada a la tecnología particular de acceso, tal como ATM, conectando los *bridges* del CPE con los nodos de borde del VPLS. Tales tramas entonces se envían en la capa de enlace sobre un túnel usado en el VPLS. Según lo observado, esto ordena el uso de un protocolo *tunneling* IP que pueda transportar las tramas de la capa de enlace. Observe que esto no necesariamente ordena el uso de un protocolo con campo de identificación en cada paquete del túnel.

D.1.5.2. *Router* del CPE

En este caso, los *routers* del CPE envían los paquetes de la capa de enlace y desde el VPLS a través del enlace *stub*, destinado a las direcciones de la capa de enlace de sus *routers* del CPE. Otros tipos de encapsulado también pueden ser factibles en tal caso, sin embargo, un VPLS necesita un espacio de direcciones obligadas por el cual solamente el *router* del CPE está conectado, podría permitir un encapsulado alternativa.

E. Recomendaciones de los tipos de VPN

En este documento se han discutido individualmente diversos tipos de VPNs, pero hay muchos requisitos y mecanismos comunes que se aplican a todos los tipos de VPNs, y muchas redes tendrán una mezcla de diversos tipos de VPNs. Es útil tener tanta concordancia como sea posible a través de estos diversos tipos de VPN. En detalle, es posible permitir que una variedad amplia de VPNs sea puesta en ejecución.

Las ventajas de adicionar soporte a causa de los siguientes mecanismos deberían ser examinadas cuidadosamente.

Para IKE/IPSec:

- El transporte de un VPN-ID al establecer un SA (2.3.1 Protocolo de señalización)
- Un cifrado nulo y una opción nula de autentificación (2.3.1 Seguridad de datos)
- Operación multiprotocolo (2.3.1 Transporte de multiprotocolo)
- Secuencia de trama (2.3.1 Secuencia de trama)
- Autentificación de usuario asimétrico/herencia (C.3)
- Asignación y configuración de la dirección del *host* (C.3)

Para L2TP:

- Definir los modos de operación de IPSec cuando sea utilizado para soportar L2TP (2.3.2)

Para VPNs en general:

- Definir un mecanismo de la configuración y del *broadcast* de la información de membresía del VPN, que use una cierta forma del directorio o de MIB (B.3.2)
- Asegúrese de que las soluciones desarrolladas, lo más lejos posible, sean aplicables a diversos tipos de VPNs, más que siendo específicas a un solo tipo de VPN.

2.1.2 Tipos de VPN según el alcance del VPN para la organización.

Según la utilización que le dan las organizaciones las dividiremos en tres categorías:

VPN intranet

VPN extranet

VPN con Accesos Remotos

2.1.2.1 VPN intranet

Las VPN intranet que se utilizan para interconectar departamentos o dependencias de una misma organización son generalmente redes con un alto nivel de aislamiento y seguridad, además requieren de garantías de calidad de servicio para aplicaciones críticas, principalmente por estas dos razones es que no muchas organizaciones utilizan Internet para este tipo de VPN. Las VPN Intranet han sido generalmente implementadas con tecnologías tradicionales como X.25, Frame Relay o ATM.

Con VPN Intranet, las pasarelas situadas en diferentes emplazamientos dentro de la misma empresa negocian un canal de comunicación seguro a través de Internet denominado túnel VPN. Los usuarios de la red que se hallan a cada uno de los lados del túnel pueden comunicarse entre sí como si se tratara de una sola red. Gracias a las VPN a través de Intranet las empresas con sucursales distribuidas por todo el mundo pueden comunicarse entre sí como si formaran una gran red. Las VPN a través de Intranet suponen una reducción significativa de costes frente a la tecnología Frame Relay y las líneas dedicadas, ya que utilizan Internet para reducir las distancias, en ocasiones grandes, entre los sitios web.

En la figura 2.6 se muestra un ejemplo de VPN Intranet donde se observa que se tiene tres sedes A, B y C de una mis organización y a la vez se tienen túneles VPNs que comunican los tres sitios es decir es una malla completa de túneles VPN por el cual se podrá pasar información segura y confiable utilizando el internet, por lo tanto simulando un enlaces dedicado entre los sitios de la organización. Usualmente se configura uno de los sitios como sede principal y este se conecta a todas las de más sedes, seria como un punto – multipunto. En este ejemplo las tres sedes se pueden verse entre sí pero no es conveniente si el número de sedes incrementa ya que el enmallado completo no es recomendable por que el procesador de los *routers* se saturaría al tener tantos túneles.

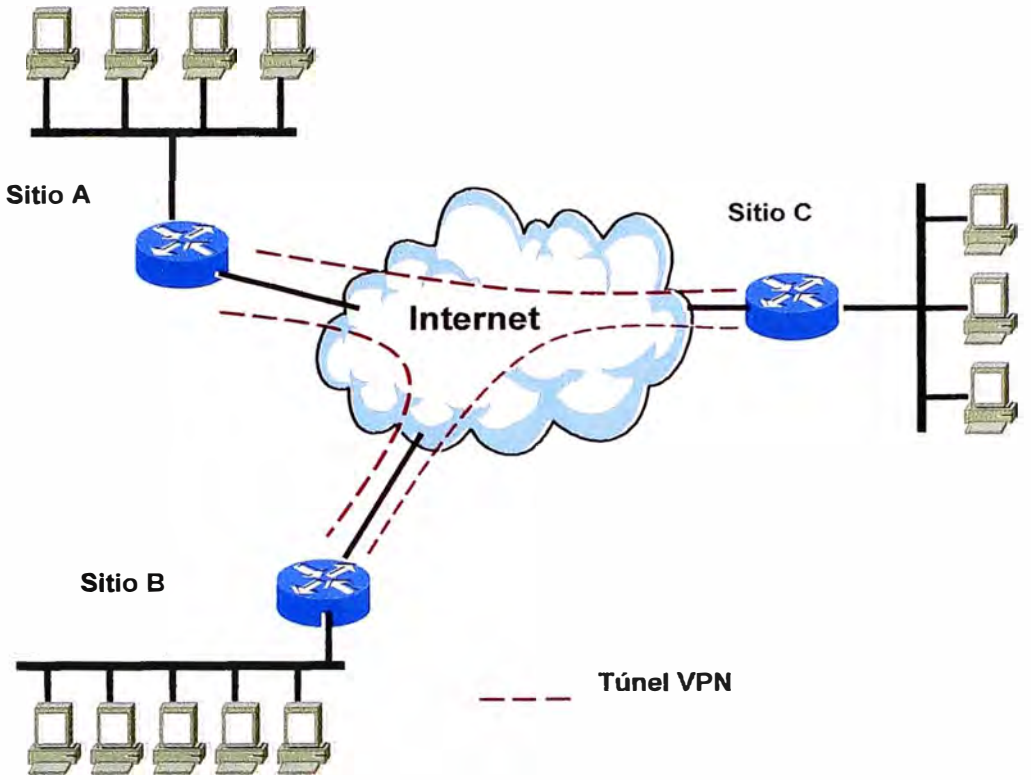

Figura 2.6: Ejemplo de VPN intranet

2.1.2.2 VPN extranet

Las Extranets son casi idénticas a las Intranets, excepto que están dirigidas a socios externos. Por este motivo se combinan las restricciones de acceso de firewall con túneles VPN, para que las empresas asociadas puedan acceder de forma segura a determinados recursos específicos, sin tener por ello acceso a toda la información corporativa confidencial. Por ejemplo, un fabricante podría crear una Extranet con un proveedor para que éste pudiera acceder a una base de datos del inventario sin que pudiera ver ninguna otra información contenida en la red corporativa.

Las VPN extranet frecuentemente tienen lugar interconectando sitios principales de diferentes organizaciones usualmente dedicando dispositivos de seguridad como firewall o de encriptación, similar a la configuración mostrada en la figura 2.7.

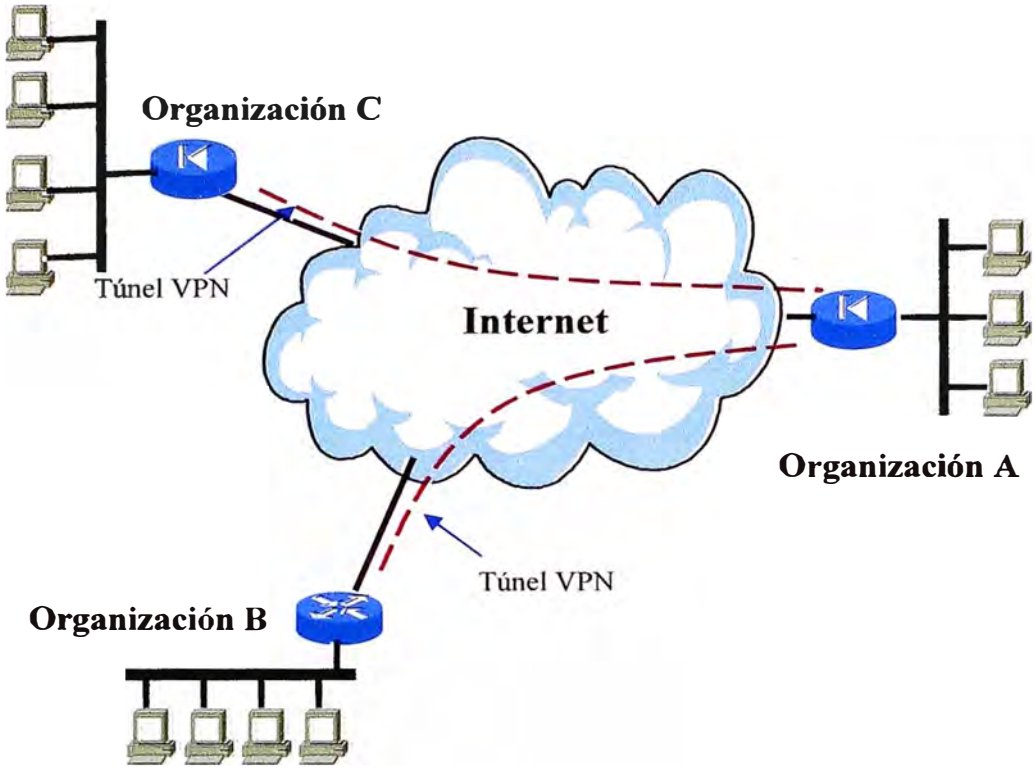

Figura 2.7: Ejemplo de VPN extranet utilizando el internet

En la figura 2.7 nos muestra la comunicación de tres organizaciones a través de túneles VPN utilizando el internet. Las organizaciones B y C pueden acceder a una base de datos o información de la organización A, esta información son permitidas por las políticas de administración de acceso que es dada por la organización A, esto se mostró con más detalle en la sección 1.2.3.

Esta configuración presenta menos requerimientos de calidad de servicio y hace a Internet más adaptable para este tipo de VPN para comunicación entre organizaciones. No es una sorpresa que cada vez más el tráfico entre organizaciones se realice a través de Internet. La figura 2.8 nos muestra una VPN extranet utilizando una WAN.

En la figura 2.8 se muestra otro ejemplo de VPN extranet, pero en este caso se utiliza una WAN que puede ser de un proveedor, se usa túneles VPN para tener mayor seguridad y confiabilidad dentro de la WAN eso ocurre por que no se confía en la seguridad que te puede dar la WAN, se usa la WAN de un proveedor con la finalidad de tener un calidad de servicio garantizada por el proveedor, como sabemos esto resulta mas costoso por que se tiene enlaces dedicados brindados por el proveedor, mientras en el caso anterior solo se gasta en el acceso a internet y con los túneles nos brinda la seguridad pero no nos garantiza la calidad de servicio, como se tiene usando la red del proveedor.

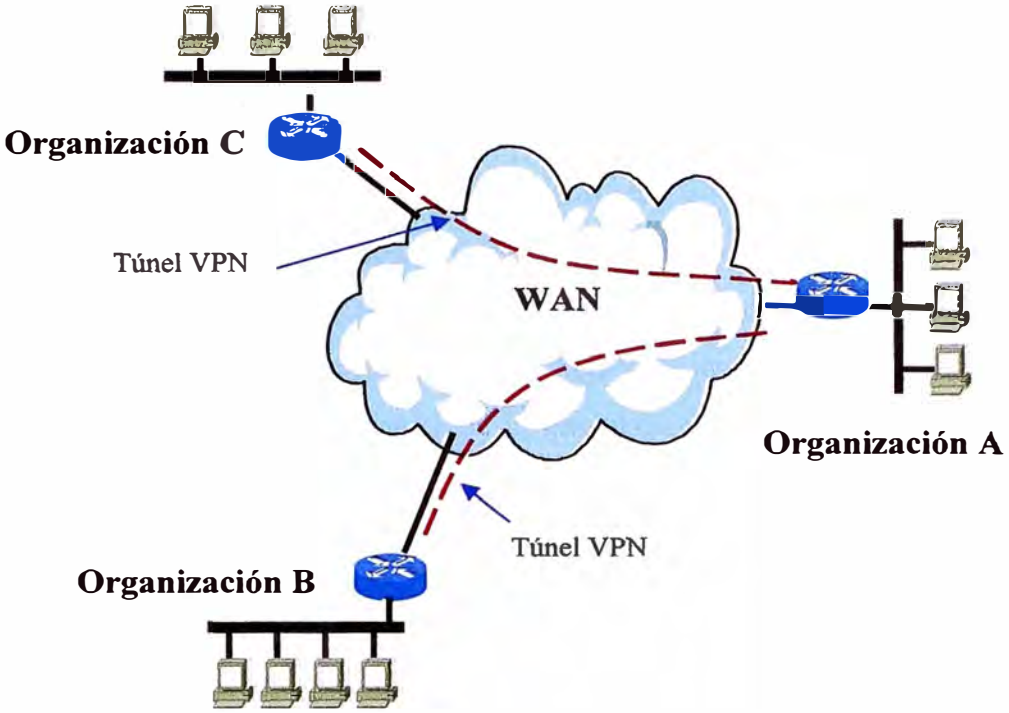

Figura 2.8: Ejemplo de VPN extranet utilizando una WAN

2.1.2.3 VPN de acceso remoto

Por último las VPN con accesos remotos, presentan características similares a las VPDN de la RFC 2764 descritas anteriormente y utilizan protocolos como L2F o L2TP.

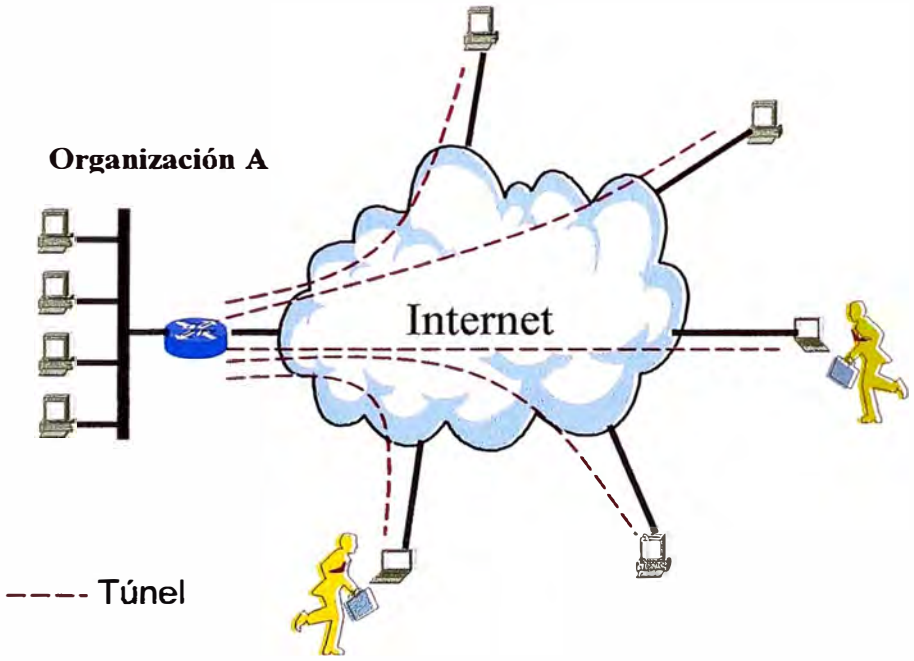

Figura 2.9: Ejemplo de una VPN con acceso remoto

La diferencia entre las VPN para el acceso remoto y para las aplicaciones LAN to LAN es que en los RAS sólo hay un *gateway* VPN. La otra parte implicada en la negociación del canal de comunicación segura con el *gateway* VPN es una PC que se haya conectado a Internet y que tiene instalado el software para Clientes de VPN. El software VPN para clientes permite a los usuarios remotos y los usuarios móviles que se estén de viaje puedan comunicarse con la red central y acceder a los servidores como si estuvieran presentes físicamente. Las VPN para el Acceso Remoto suponen un ahorro significativo, ya que reducen los costes de las comunicaciones de largas distancias asociadas a los accesos *dial up*. Las VPN para RAS ayudan así mismo a aumentar la productividad y garantizan un acceso seguro a la red, independientemente del lugar en donde se halle el usuario.

2.2 Clasificación de una VPN

Las redes VPN pueden ser clasificadas por varias vías. La clasificación más ampliamente utilizada está basada en si la información de encaminamiento es intercambiada o no entre los clientes y los ISP. En el **modelo de VPN par a par**, es intercambiada la información de enrutamiento entre los *routers* de los clientes y los *routers* del ISP. En el **modelo de VPN superpuesta**, el ISP solo brinda VC (similar a líneas dedicadas) y la información de enrutamiento es intercambiada directamente entre los *routers* de los clientes. En grandes redes de ISP los dos modelos pueden ser combinados, el modelo VPN par a par puede utilizar VPN superpuestas en la parte de acceso (ejemplo, los clientes conectados a los *routers* de borde del proveedor a través de Frame Relay o ATM) o en el núcleo (ejemplo, enlazando los *routers* del Proveedor del ISP a través de ATM).

En la siguiente Figura 2.9 observamos una clasificación de las diferentes VPN. El modelo de VPN superpuesto puede ser implementado con tecnologías de conmutadores de redes WAN de Nivel 2 (Frame Relay, SMDS, ATM) o con tecnologías de túneles de Nivel 3 (IP sobre IP, IPSec). El modelo de VPN par a par tradicionalmente ha sido implementado con complejos artificios de enrutamiento o con listas de acceso IP, lo cual ha presentado un número de inconvenientes. Las VPN basadas en MPLS que describiremos en otros artículos superan la mayor parte de los inconvenientes de las otras tecnologías de VPN par a par, posibilitando a los SP combinar los beneficios de los modelos par a par (simplificar el enrutamiento, simplificar la implementación de los requerimientos de los clientes), con la seguridad y el aislamiento del modelo de VPN superpuesto.

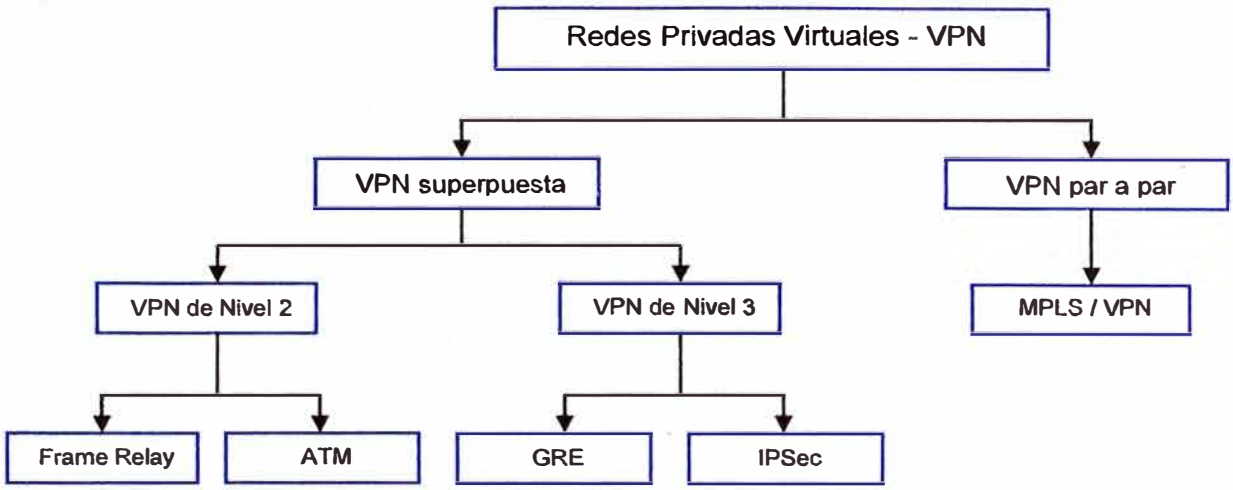

Figura 2.9: Clasificación de las VPN según tecnología subyacente.

El modelo superpuesto (*overlay*), donde el ISP simula líneas dedicadas para el cliente. El modelo superpuesto se puede comprender de una forma mejor porque en el existe una clara separación entre las responsabilidades del cliente y del proveedor de servicio. El proveedor de servicio brinda al cliente una configuración que simula líneas dedicadas llamadas circuitos virtuales (**VC** - *Virtual Circuit*), los que pueden estar disponibles constantemente con circuito virtuales permanentes (**PVC** - *Permanent Virtual Circuit*) o establecidos bajo demanda con circuito virtual conmutado (**SVC** - *Switched Virtual Circuit*). (La siguiente figura 2.10 muestra un ejemplo de topología de VPN superpuesta).

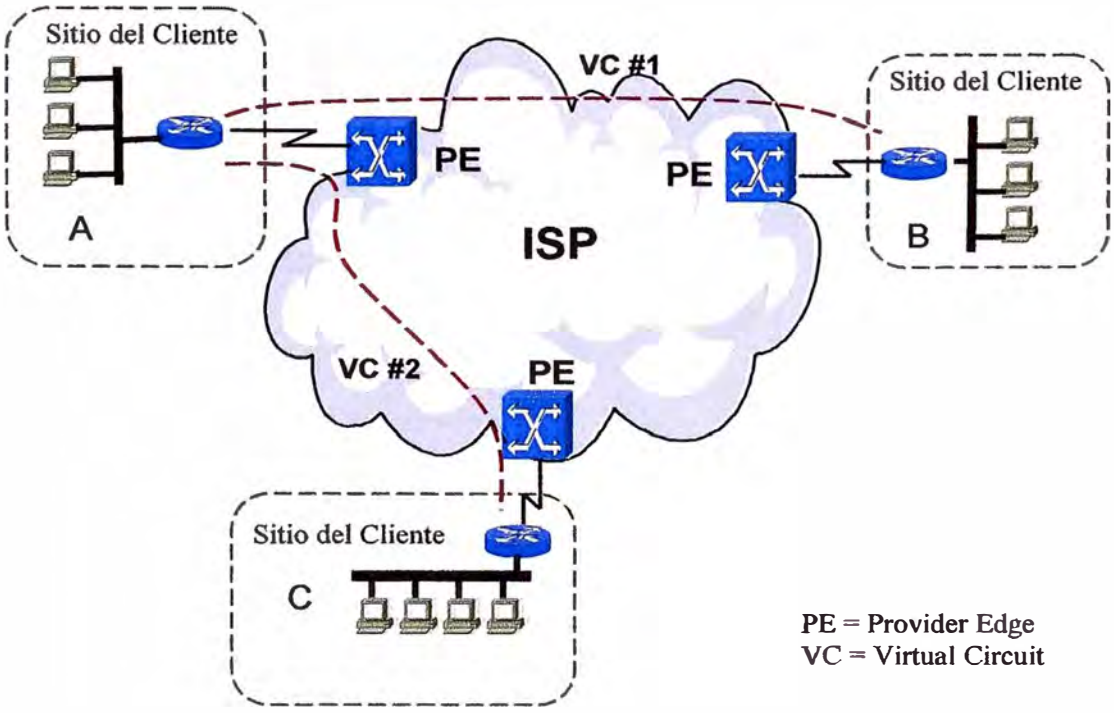

Figura 2.10: Ejemplo de topología de red VPN superpuesta

Como se observa en la Figura 2.10 el cliente establece comunicación entre sus *routers* sobre los VCs suministrados por el proveedor de servicio. La información de los protocolos de enrutamiento siempre es intercambiada entre los dispositivos del cliente por lo que el proveedor de servicio desconoce la topología interna de la red del cliente. La figura 2.11 muestra la topología del enrutamiento en la red de la Figura 2.10.

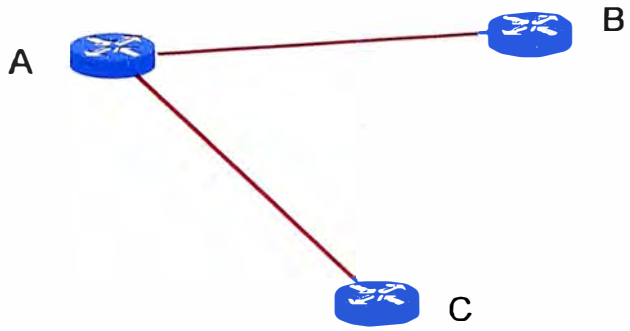

Figura 2.11: Ejemplo de enrutamiento en red VPN superpuesta

El modelo par a par (*peer to peer*) donde el ISP y el usuario intercambian información de enrutamiento de Nivel 3, con la cual el proveedor transporta los datos entre los sitios del usuario por un trayecto óptimo en lo cual el usuario no interviene.

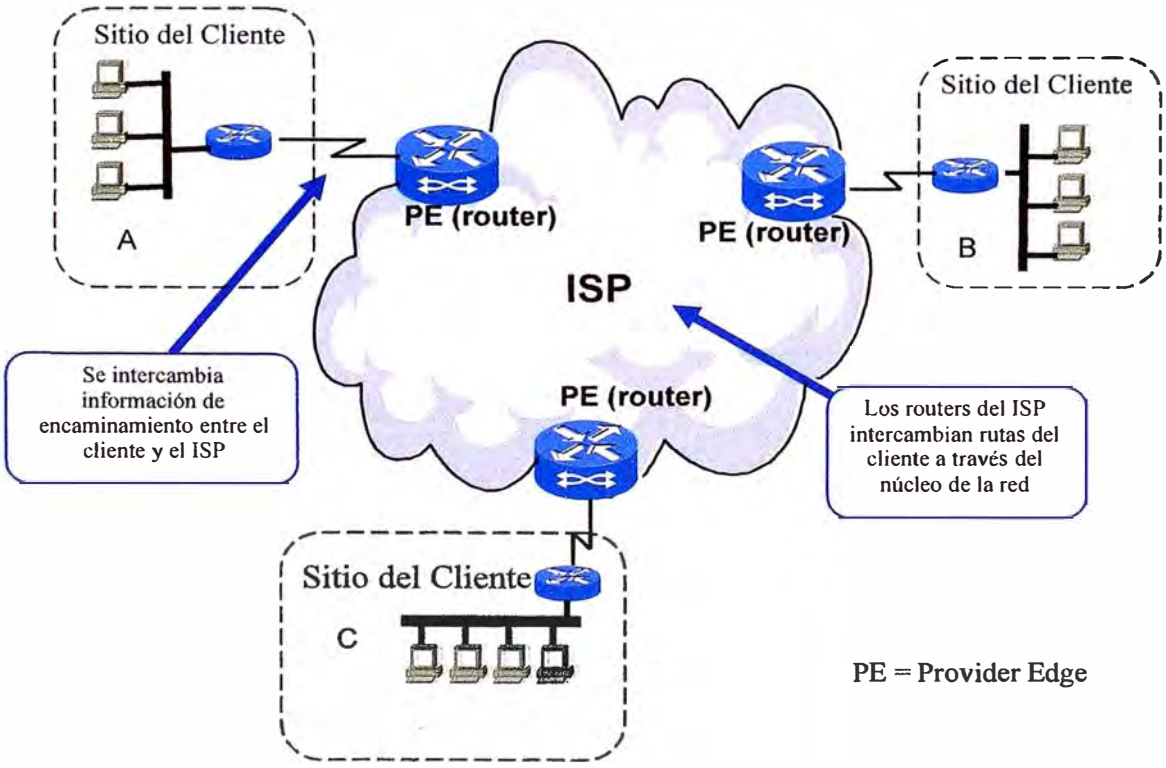

Figura 2.12: Ejemplo de VPN par a par.

2.3 Protocolos de una VPN

Para que pueda establecerse un túnel es necesario que los extremos implicados utilicen los mismos protocolos de *tunneling*. Los protocolos más comunes son:

- **MPPE** (*Microsoft Point-to-Point Encryption,* descrito en el RFC 3078).
- **IPIP** (*IP in IP Tunneling,* descrito en el RFC 1853).
- **PPTP** (*Point-to-Point Tunneling Protocol*, descrito en el RFC 2637).
- **L2TP** (*Layer 2 Tunneling Protocol*, descrito en el RFC 2661).
- **IPSec** (*IP Security*, descrito en el RFC 2411).
- **MS-CHAP** (descrito en el RFC 2433).

- **MPPE** (*Microsoft Point-to-Point Encryption*)

Es un protocolo que se basa en encriptar los datos de PPP (Point to Point Protocolo). El algoritmo de cifrado que emplea es el RSA RC4 para proporcionar la confidencialidad de los datos. La longitud de la clave para la sesión puede ser negociada, actualmente soporta claves de sesión de 40 bits y 128 bits. **[15]**

- **IPIP** (*IP in IP Tunneling*)

La encapsulación IP en IP ha sido empleada por *bridges* que tienen diferentes capacidades o políticas. Pero también se puede emplear para implementar técnicas de *Tunneling.* La técnica de encapsulado es muy simple. Una cabecera IP exterior es añadida antes que la cabecera IP original. Entre ellas hay otras cabeceras para la ruta, por ejemplo cabeceras de seguridad que configuran el túnel. **[14]**

- **PPTP** (*Point-to-Point Tunneling Protocol*)

Protocolo de encapsulado de PPP sobre IP. Es una especificación desarrollada por un consorcio de fabricantes, entre los que estaban gente como Microsoft, 3Com o U.S. Robotics. El protocolo se diseñó originalmente como una forma de encapsular protocolos no TCP/IP (como IPX) para poder ser transmitidos por Internet usando GRE. Es una especificación genérica, que permite la adición de diversos mecanismos de autentificación

y algoritmos de encriptación. Nótese que estas técnicas de seguridad no están dentro del protocolo, sino que se añaden a posteriori. **[13]**

- **L2TP** (*Layer 2 Tunneling Protocol*)

Es una extensión del PPTP, mezclando lo mejor de los protocolos PPTP de Microsoft y L2F de Cisco. Los dos componentes principales del L2TP son: El LAC que es el dispositivo que físicamente termina una llamada; y el LNS que es el dispositivo que autentifica y termina el enlace PPP. L2TP utiliza redes conmutadas de paquetes para hacer posible que los extremos de la conexión estén ubicados en distintas computadoras. El usuario tiene una conexión L2 al LAC, el cual crea el túnel de paquetes PPP. Así, los paquetes pueden ser procesados en el otro extremo de la conexión, o bien, terminar la conexión desde un extremo. **[5]**

- **IPSec** (*IP Security*)

Protocolo que sirve para establecer una sesión segura entre dos *hosts* que se comuniquen a través de IP, proporcionando encriptación a nivel de la capa de red.

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

Define nuevos formatos de paquete: la cabecera de autentificación (AH), que permite asegurar la integridad de los datos y el ESP que permite asegurar la privacidad e integridad de los datos. AH protege la integridad y autenticidad de los datos, incluyendo los campos invariantes de la cabecera IP. Esta cabecera no proporciona confidencialidad, mientras que ESP protege tanto la confidencialidad como la integridad y la autenticidad de los datos. Cuando se usa para comprobar la integridad de los datos no incluye los invariantes de la cabecera IP.

- **MS-CHAP**

Microsoft creó MS-CHAP para autentificar estaciones remotas Windows. Proporciona la funcionalidad a la cual los usuarios LAN están acostumbrados, integrando algoritmos de

cifrado y hash sobre redes Windows **[16]**.

En el Capitulo III se mostrará un proyecto integral de comunicación de la red extranet financiera para el Banco Central de Reserva del Perú, esté servicio es brindado por Telmex S.A., en el cual se tratará la solución y propuesta del proyecto; y por la importancia de los datos que se va ha transmitir entonces se examinará la vulnerabilidad del primer diseño propuesto lo cual induce a plantear una contingencia a la solución del proyecto y brindar encriptación a la solución, también se mostrará la oferta económica de la solución propuesta, ingreso del proyecto, egreso del proyecto y como parte culminante se describirá las pruebas realizadas en el proyecto.

CAPITULO III

PROYECTO INTEGRAL DE COMUNICACIONES DE LA RED EXTRANET FINANCIERA DEL BCRP

3.1 Solución y propuesta del proyecto

3.1.1 Solución para la red de comunicaciones.

Esta red permitirá que las distintas instituciones puedan intercambiar información con alta performance y con los niveles de seguridad que la propia información requiera (Aplicativo LBTR). Para tal fin se implementará una red basada en Circuitos Virtuales Permanentes (PVCs) que unirá las distintas instituciones al *backbone* ATM de **Telmex S.A**. Cada nodo remoto será provisto con una puerta serial de interfase RS-232 capaz de manejar el tráfico y proporcionar la performance requerida por la red, depende de la red del punto remoto.

El Nodo Central de la red será la sede del Banco Central de Reserva, la cual contará con dos enlaces de Fibra Óptica a 10Mbps cada uno, configurándose uno como principal y el otro como respaldo, cada uno con Fibra Óptica hacia la red. A partir de este enlace se generarán todos los circuitos (PVCs) hacia los distintos nodos remotos (Bancos) que forman parte del LBTR. Ante una contingencia al interior del CORE de la red, toda la información será reencaminada a través del segundo enlace de Fibra Óptica a 10Mbps provisto como enlace secundario en el Nodo Central del Banco Central de Reserva. Para este enlace secundario se configuraran PVCs *en demanda*, los cuales ante una caída de los PVCs del enlace principal permitirán continuidad en el servicio de manera automática, estando estos configurados con un MCR de 0Kbps y un PCR de 128Kbps, no representando caída del servicio ni corte.

En el Nodo Central del Banco Central de Reserva se instalarán dos *Switchs Routers* Cisco Systems modelo 7206, que serán los equipos principales de conmutación de la red. Los *Switchs Routers* Cisco Systems modelo 7206 propuestos están configurados cada uno

con un procesador principal MIPS RISC de 225MHz (NPE-225) capaz de procesar 225,000 paquetes por segundo (pps), cuatro puertas Ethernet 10Base-T, cuatro puertos Token Ring y fuente de poder redundante. Posee configurado software operativo Cisco IOS Enterprise IPSEC 56 para manejo de encriptación de data, tarjeta de encriptación de data, memoria DRAM de 128 Mbytes y memoria FLASH de 20 Mbytes.

Se esta configurando en un *Switch Router* Cisco Systems modelo 7206, una tarjeta ISDN PRI con 2 puertas, para conector E1 G.703 balanceado (120ohm), para activar la contingencia por ISDN entre el Nodo Central del Banco Central de Reserva y los puntos remotos (bancos e instituciones financieras) que forman parte de la red LBTR.

Los puntos remotos están representados por los diversos Bancos e instituciones financieras que formaran parte de la red LBTR del Banco Central de Reserva, en los cuales se utilizarán los *Routers* Cisco 2611 ó Cisco 2612 ya instalados por el proyecto BANCARED como se muestra en la figura 3.1, a los cuales se les adicionara una puerta serial RS-232. Este modelo esta equipado con un procesador de 40MHz MPC 860 RISC con capacidad de procesamiento de 25,000 paquetes por segundo (pps). También tiene configurado software operativo Cisco IOS Enterprise, memoria DRAM de 32 Mbytes y memoria FLASH de 8 Mbytes. Los *Routers* Cisco 2611 ó Cisco 2612 cuentan con puertas ISDN BRI para activar la contingencia por este medio. Para brindar el servicio de encriptación solicitado para el proyecto LBTR será necesario realizar adecuaciones en el Software IOS y en las memorias DRAM y FLASH como requerimiento indispensable para manejar encriptación en estos *Routers* (Cisco 2611 – Cisco 2612).

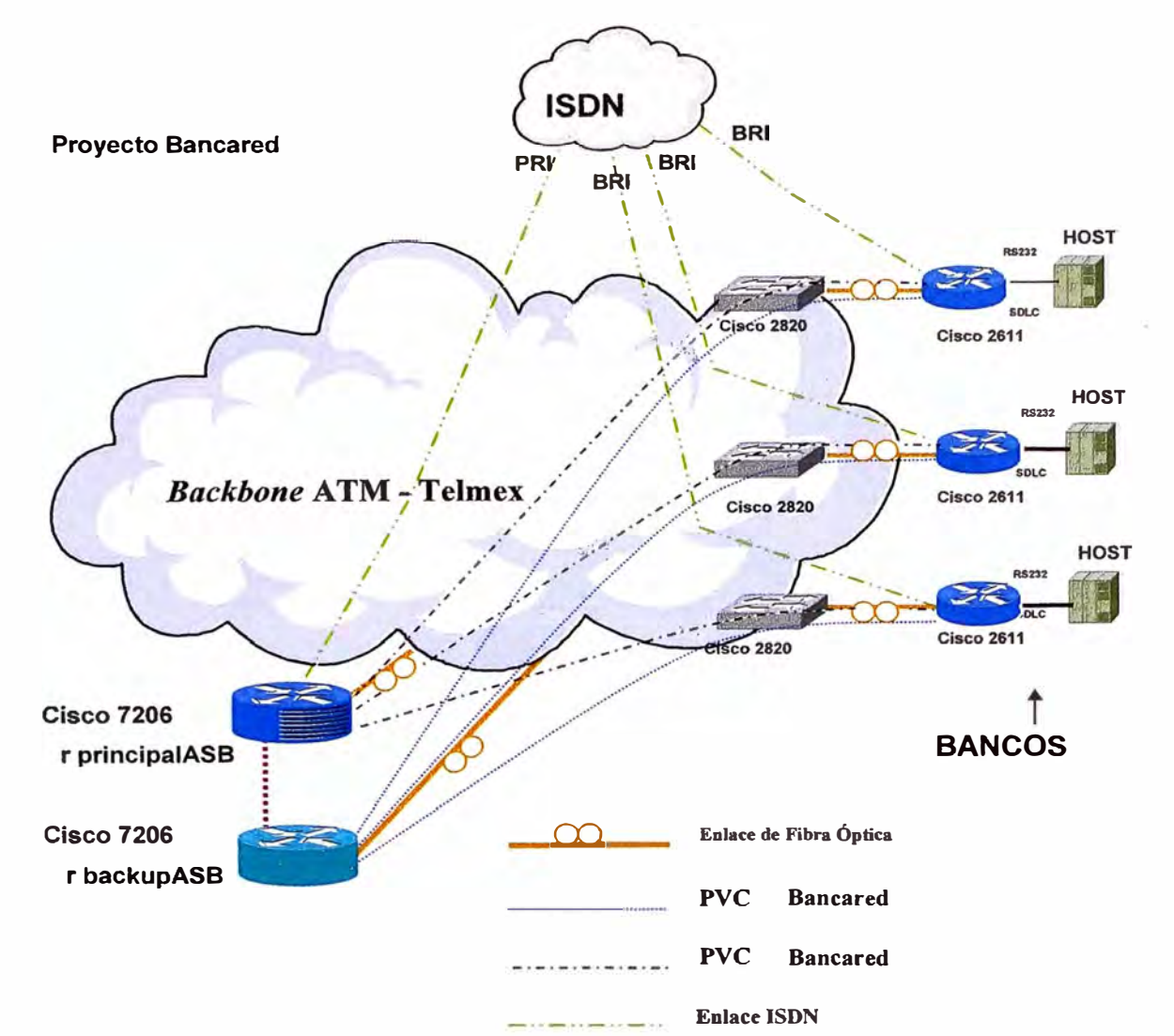

Figura 3.1: Red del proyecto Bancared

Los dos *Routers* Cisco Systems modelo 7206 propuestos para el Nodo Central del BCR (LBTR) incluyen el sistema operativo, memorias y hardware para realizar la encriptación de datos entre el BCR y todos los bancos participantes de la red. Los *Routers* Cisco Systems modelo 2611 y 2612 de BANCARED, que son utilizados por todos los bancos para conectarse al nodo central del BCR (LBTR) se están potenciando para soportar la encriptación de datos, adicionándoseles el sistema operativo de encriptación de datos, memorias y hardware necesario para la encriptación de datos. Este potenciamiento estará a cargo de ASBANC.

El ancho de banda asignado a cada nodo remoto será de 128Kbps.

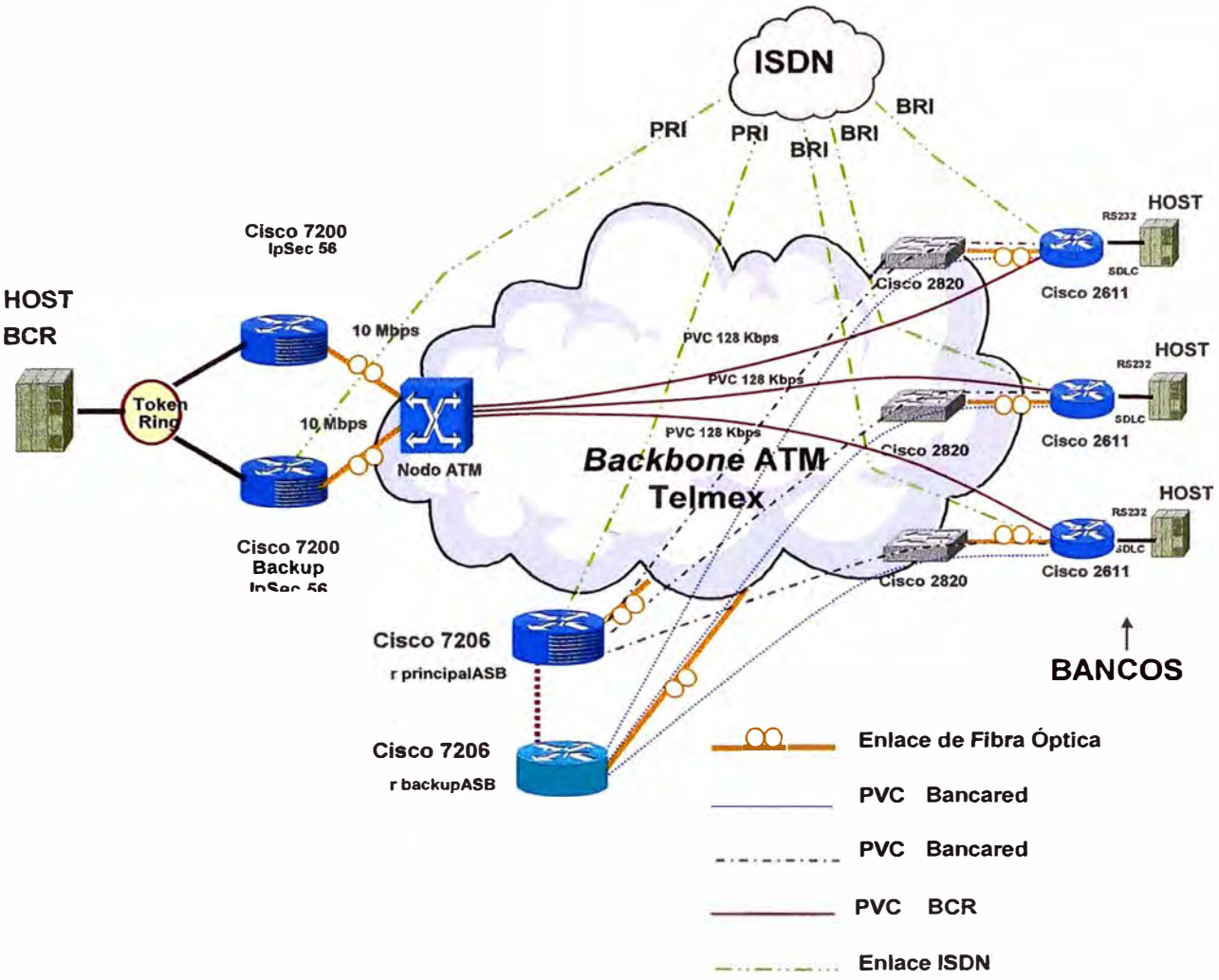

Figura 3.2: Red del proyecto del BCR considerando un solo Nodo ATM

3.1.2 Vulnerabilidad del diseño y redundancia.

Como se muestra en la figura 3.2, los *routers* de la sede del BCRP estarán conectados a un solo Nodo de la red ATM de Telmex S.A. Por lo tanto se tendrá las siguientes vulnerabilidades:

1) Si el Nodo ATM de Atención a la sede central del BCRP tuviera problemas, toda la red del BCRP estaría sin servicio pudiendo solo utilizar el enlace ISDN a 64K.
2) No hay una redundancia efectiva de PVCs al salir ambas conexiones desde un mismo Nodo ATM (Nodo ATM de atención a la sede central BCRP).

Todos estos puntos de Vulnerabilidad al escenario propuesto, nos hacen ver que se debe cambiar la propuesta a implementar en el cliente, debido al alto grado de vulnerabilidad y no se estaría cumpliendo con el SLA contratado por el cliente.

3.1.3 Recomendaciones

Para evitar el los puntos de vulnerabilidad antes mencionados, es necesario que cada uno de los equipos (*routers*) de la sede central del BCRP se conecte a Nodos ATM diferentes.

Con lo mencionado se podrá generar diferentes PVC desde cada equipo del POP hacia los bancos remotos, obteniendo de esa manera redundancia de PVC.

Con estas recomendaciones se tiene un mejor respaldo en la contingencia de la red del BCRP como se muestra en la figura 3.3.

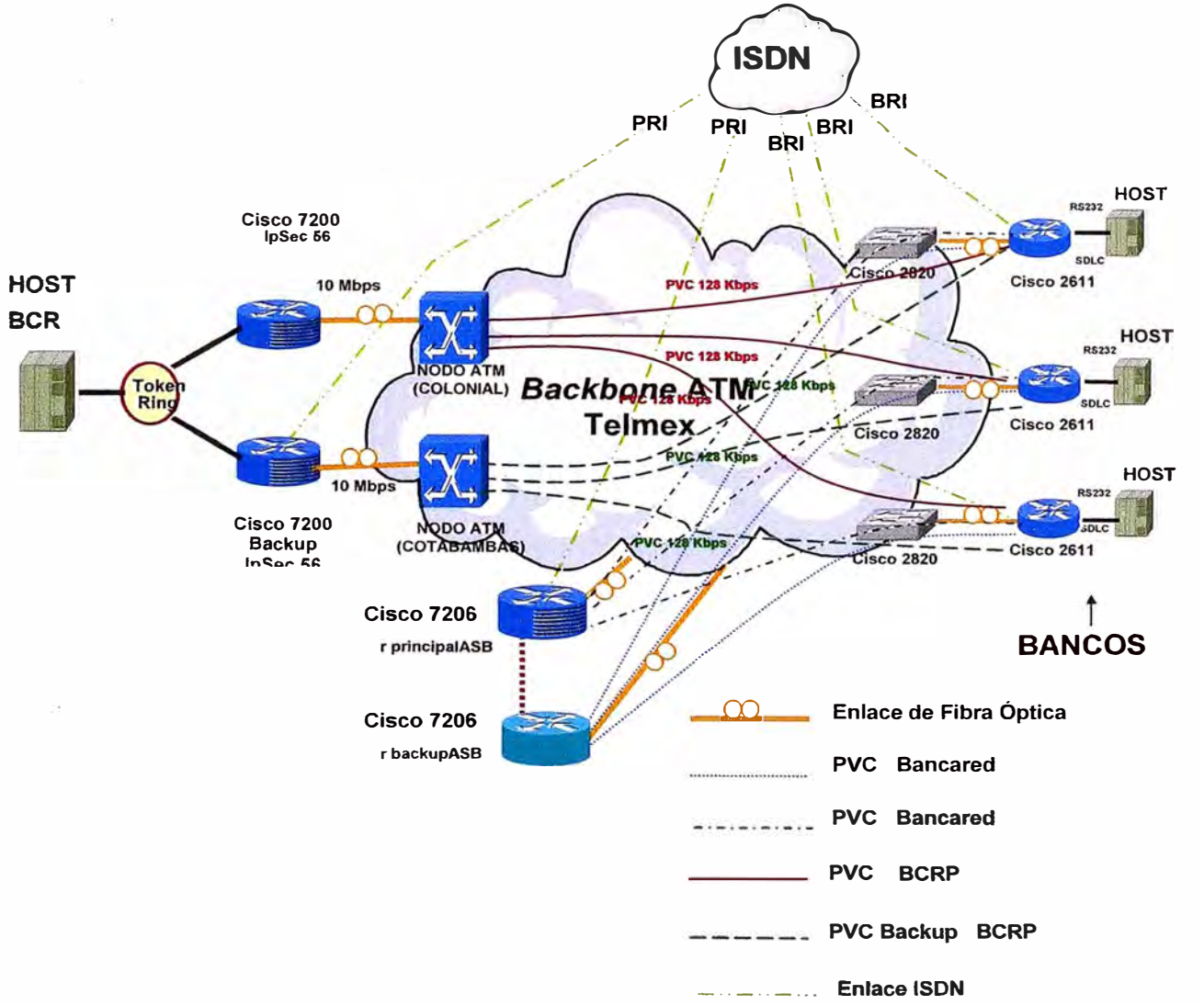

Figura 3.3: Red del proyecto del BCR considerando dos Nodos ATM

3.1.4 Contingencia para la solución propuesta.

La propuesta contempla todos los elementos necesarios para brindar servicios de Contingencia para la red de transporte que soportara las comunicaciones de la red del Banco Central de Reserva (Aplicativo LBTR). Los elementos de contingencia considerados son:

1ro. Contingencia por Segunda Puerta de Fibra Óptica a 10Mbps en el Nodo Central del Banco Central de Reserva: Como se indico, nuestra propuesta considera una segunda puerta de Fibra Óptica a 10Mbps conectándose a un nodo ATM proveniente del segundo *Switch Router* Cisco Systems modelo 7206 en la Sede Central del Banco Central de Reserva (Redundancia en Hardware). Esta segunda conexión servirá para reencaminar y conectar ante contingencias de Hardware y/o Enlace toda la información de los Nodos Remotos. Es importante detallar que esta contingencia provee Hardware Redundante así como Enlace de Transporte y PVC en demanda redundante.

2do. Contingencia de los Nodos Remotos por ISDN: Se están considerando en uno de los *Routers* Centrales del Banco Central de Reserva puertas ISDN PRI (dos puertas ISDN PRI en la tarjeta en total) y en los *Routers* Remotos (*Routers* BANCARED Cisco 2611 ó Cisco 2612) una puerta ISDN BRI la cual esta instalada. Los canales "B" de los accesos básicos ISDN BRI de los *Routers* Remotos Cisco Systems 2611 ó Cisco Systems 2612 serán configurados para conectarse ante contingencia de última milla a los Nodos Centrales del Banco Central de Reserva y Nodo BANCARED en forma simultánea utilizando un canal "B" de 64Kbps para cada conexión de contingencia.

Adicionalmente, los dos canales "B" de los accesos ISDN BRI podrán conectarse a uno u otro Nodo Central, asumiendo la caída de un solo PVC. Es decir, si el PVC de la red LBTR (Banco Central de Reserva) sufriese la caída lógica y el PVC de BANCARED siguiese activo, la contingencia por ISDN BRI asumirá la totalidad de canales "B" (2 en total, 128Kbps) únicamente para el tráfico proveniente de la conexión LBTR.

La redundancia quedará garantizada para los dos enlaces con los dos canales "B", especificándose un canal para BANCARED y la otra para LBTR. Si BCR ocupase dos canales y la conexión de ultima milla con ASBANC también cae la redundancia de ASBANC no funcionaría pues LBTR ocupa los dos canales, por lo tanto solo se debe

mencionar que se reservará un canal B para cada banco para garantizar disponibilidad de acceso ISDN desde la sede central.

3ro. Contingencia de los Nodos ATM: como se indico en las recomendaciones que es necesario dos nodos ATM diferentes conectados a cada *router* es decir un nodo ATM con un *router*, con la finalidad si se presenta fallas en el nodo ATM del *router* principal que el otro nodo como respaldo y así no perder la comunicación con los puntos remotos que son bancos o entidades financieras.

3.1.5 Problemas de encriptación.

- Se ha planteado a ASBANC la utilización de Encriptación 3DES.
- Se ha planteado al BCR la utilización de Encriptación IPSEC 56.
- La tarjeta encriptadora SA-Encrypt soporta sólo IPSEC 56 y no soporta 3DES, para lo cual se necesita la tarjeta SA-ISA y que hace requerimiento del IOS 12.1E para soportar 3DES pero no soporta IPSEC56. Cabe mencionar que 3DES consume muchos recursos de memoria y procesador pudiendo ser el 2611 un equipo no apropiado para esta solución (Encriptar 1M para ASBANC y 128K para BCRP)
- Se debe definir con ASBANC y BCR que encriptación utilizará, se recomienda usar IPSEC56.

3.1.6 Modalidad de mantenimiento.

Nuestra propuesta de solución considera los siguientes mantenimientos:

- Para los equipos propuestos en Lima Metropolitana y Callao en calidad de alquiler se consideran los Mantenimientos Preventivos, Correctivos y Backup sin costo durante todo el tiempo de duración del contrato (24 meses).
- El mantenimiento Preventivo, correctivo implica gastos operativos no presentados en la Oferta Comercial.

3.1.7 Oferta económica de la solución propuesta.

Propuesta Económica

Contrato de Prestación de Servicios a 24

Item	Descripción	Cant.	P. Unitario US$	P.Total US$
A	*Alquiler Mensual por Servicio Integral de Comunicaciones para el Nodo Central del Banco Central de Reserva. Incluye :*			
A.1	**Equipos en Sede Principal**			
1	Router Cisco Systems modelo 7206 IOS ENTERPRISE IPSEC56	1	0.00	0.00
2	Router Cisco Systems modelo 7206 IOS ENTERPRISE IPSEC56	1	0.00	0.00
		Total Mensual US$		**0.00**

Nota:

1. Monto mínimo Equipos en Sede Principal en función a 18 Bancos: US$ 3.096.00

2. Monto máximo Equipos en Sede Principal en función a 23 Bancos: US$ 3,956.00

Item	Descripción	Cant.	P. Unitario US$	P.Total US$
B	*Alquiler Mensual por Servicio Integral de Comunicaciones para Bancos. Incluye:*			
B.1	**Servicio de Transporte por Mes para cada Banco**			
	Incluye:			
1	PVC Adicional 128 Kbps ATM dedicado	1	165.00	165.00
B.2	**Utilización de Nodo Central BCR para cada Banco**			
	Incluye:			
1	Acceso a Nodo BCR	1	172.00	172.00
		Total Mensual US$		**337.00**

Ite	Descripción	Cant	P. Unitario US$	P.Total US$
C	**Servicio de Instalación pago por única vez para cada Banco. Incluye:**			
C.1	**Instalación para cada Banco**			
	Incluye:			
1	PVC Adicional 128 Kbps ATM	1	275.40	275.40
			Total US$	**275.40**

Nota:

- Los costos del BCR están prorrateados en los costos de enlace e instalación de los Bancos participes de la EXTRANET.
- Los costos de Utilización de Nodo Central BCR considera un mínimo de 18 Bancos. Se consideraran los costos de US$ 172.00 + IGV por Banco hasta completar la conexión número 23.
- La conexión número 24 y en adelante no estarán sujetas al pago por utilización del nodo central. Se entiende que para la conexión 24 y en adelante, solo estas no estarán sujetas al pago de utilización del nodo central.
- Los costos de la propuesta son unitarios y corresponden al pago de cada Banco participante del LBTR (mínimo 18 Bancos).
- Los costos no incluyen el I.G.V.

Tabla 3.1: Oferta económica

Observaciones a la oferta comercial:

- No se está considerando la licencia para el Upgrade de IOS a cada sede Remota.
- No se está considerando el Cable Serial y las Tarjetas V.35 en cada sede remota (Ver figura 3.3).
- No se está considerando el Upgrade de Memoria en Cada sede remota a 40-64MB DRAM Mínimo.

3.1.8 Ingreso y egreso del proyecto.

Estos valores deben ser ingresados en un cash Flow para calcular el TIR del proyecto y el tiempo de retorno de inversión.

DESCRIPCION	COSTOS	
	ANUAL US$.	TOTAL US$.
EGRESOS		
RESPALDO ISDN PRI INSTALACION	-	2,996.57
RESPALDO ISDN PRI COSTO BASICO MENSUAL 36 MESES	4,936.11	14,808.34
COSTO TOTAL EQUIPOS CISCO	-	149,865.66
COSTO DE REDUNDANCIA PLANTA EXTERNA - TENDIDO OC3	-	7,526.75
CONSUMO BASICO LLAMADAS ISDN BRI 0.5HxMesxSede	182.05	546.15
MANTENIMIENTO ANUAL x 3 AÑOS	11,486.35	34,459.05
UPGRADE DE FLASH A 18 SEDES	-	13,948.00
SUBTOTAL	**16,604.51**	**224,150.52**
INGRESOS		
TRANSPORTE 18 BANCOS 3 AÑOS	35,640.00	106,920.00
INSTALACION 18 BANCOS	-	4,957.20
CONEXIÓN AL NODO 18 BANCOS 3 AÑOS	37,152.00	111,456.00
UPGRADE DE IOS Y MEMORIAS A 40 MB DRAM 18 BANCOS 36 MESES	-	18,299.52
SUBTOTAL	**72,792.00**	**241,632.72**

Tabla 3.2: Ingreso y Egreso del Proyecto

3.2 Pruebas del proyecto.

3.2.1 Pruebas de conectividad.

3.2.1.1 Pruebas sin encriptación con sistemas operativos a utilizar.

A) Prueba en sistema operativo Windows NT

- Interface Ethernet:

Escenario: Se usó un servidor con Windows NT 4.0 con el aplicativo cliente servidor SIB v3.01, que es la misma que usan los bancos para LBTR. Este servidor cuenta con una tarjeta Ethernet. Esta tarjeta Ethernet esta conectada a un hub, el mismo que esta conectado al *router* Cisco 2611:

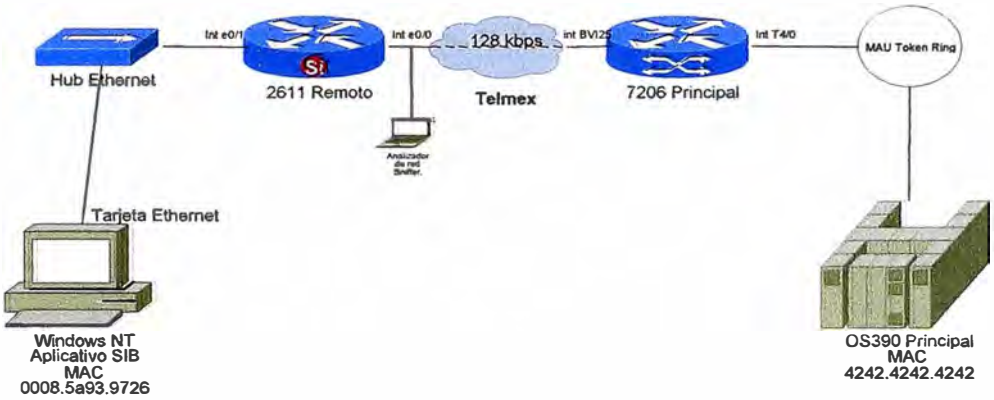

Figura 3.4: Prueba sin encriptación con Windows NT - Ethernet

Desempeño de las consultas: Se efectuó una consulta típica, se tomaron los siguientes datos:

- Tiempo de respuesta por consulta: 3 seg.
- Uso del CPU: Se uso el 1% del CPU.
- Uso Máximo del Ancho de banda: Se tuvo un pico de 14,4Kbps.

Conclusiones: Se observó que el tiempo de respuesta es bastante rápido, el *router* no usa muchos recursos y el ancho de banda es aceptable ya que las consultas son amplias y se efectúan una por vez en el enlace. El resultado es aceptable, ya que se usa menos del 10% de los recursos de ancho de banda y CPU.

- Interface Token Ring:

Escenario: Se usó un servidor con Windows NT 4.0 con el aplicativo cliente servidor SIB v3.01, que es la misma que usan los bancos para LBTR. Este servidor cuenta con una tarjeta Token Ring. Esta tarjeta se conectó a un MAU, el mismo que se conecto a un *router* Cisco 2612.

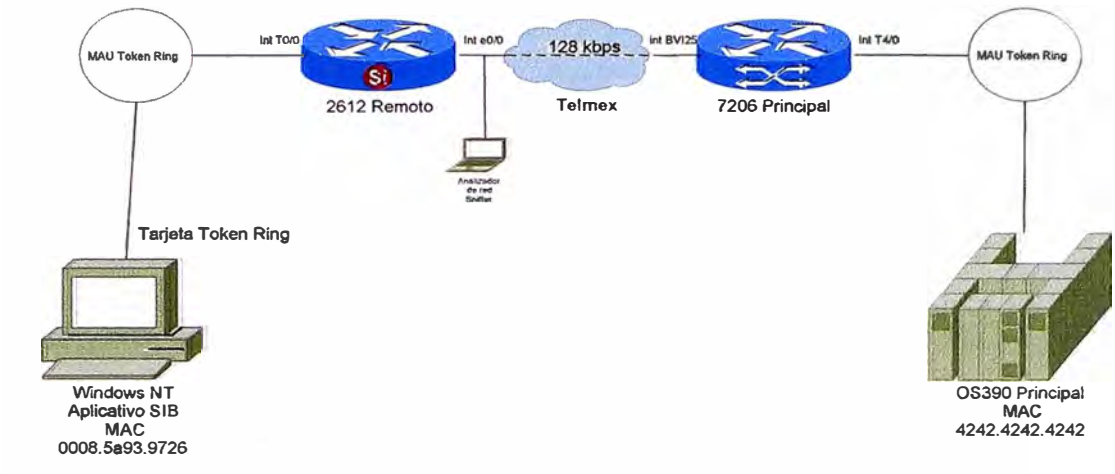

Figura 3.5: Prueba sin encriptación con Windows NT - Token Ring

Desempeño de las consultas: Se efectuó una consulta típica, se tomaron los siguientes datos.

- Tiempo de respuesta por consulta: 3 seg.
- Uso del CPU: Se uso el 1% del CPU.
- Uso Máximo del Ancho de banda: Se tuvo un pico de 22,4Kbps.

Conclusiones: Se observó que el tiempo de respuesta es bastante rápido, el *router* no usa muchos recursos pero el ancho de banda es mayor al anterior pero aceptable ya que las consultas son amplias y se efectúan una por vez en el enlace. El resultado es aceptable, ya que se usa menos del 10% de los recursos de ancho de banda y CPU.

- Interfase Serial:

Escenario: Se usó un servidor con Windows NT 4.0 con el aplicativo cliente servidor SIB v3.01, que es la misma que usan los bancos para LBTR. Este servidor cuenta con una tarjeta Multiprotocolo serial la cual se conecta por un cable RS232 a la tarjeta Serial del *router* 2611:

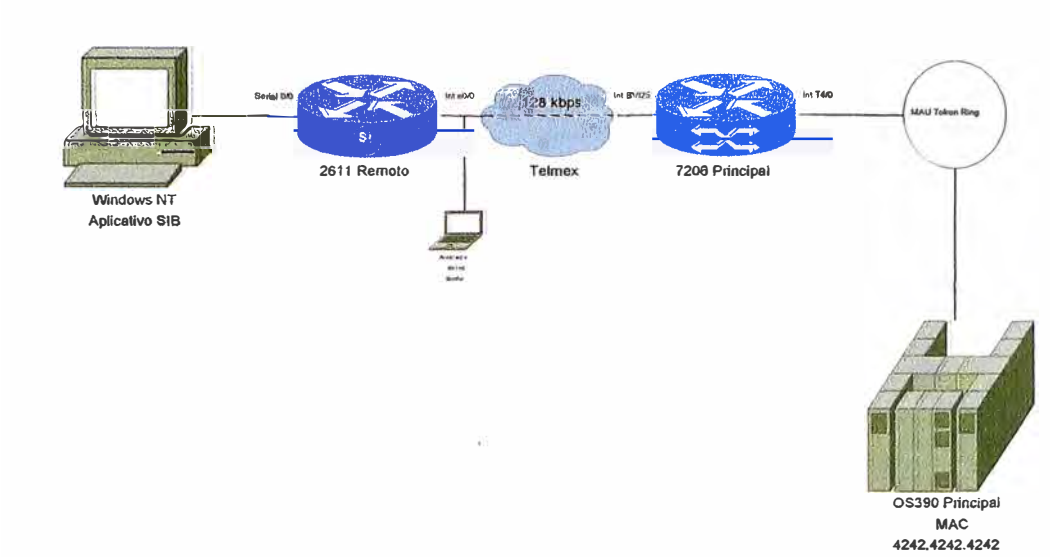

Figura 3.6: Prueba sin encriptación con Windows NT - Serial

Desempeño de las consultas: Se efectuó una consulta típica, se tomaron los siguientes datos:

- Tiempo de respuesta: 2 seg.
- Uso del CPU: Se uso el 3% del CPU.
- Uso Máximo del Ancho de banda: Se tuvo un pico de 5,7kps.

Conclusiones: Se observó que el tiempo de respuesta bastante aceptable, el *router* tampoco uso muchos recursos y el ancho de banda fue menor que en los otros casos. El resultado es aceptable, ya que se usa menos del 10% de los recursos de ancho de banda y CPU.

B) Prueba del aplicativo con sistema operativo AS400

- Interface Ethernet:

Escenario: Se usó un servidor AS400 con el aplicativo SIB v.3.01.Este servidor tiene una Interface Ethernet, la cual esta conectada a un Hub y este al *router* Cisco 2611:

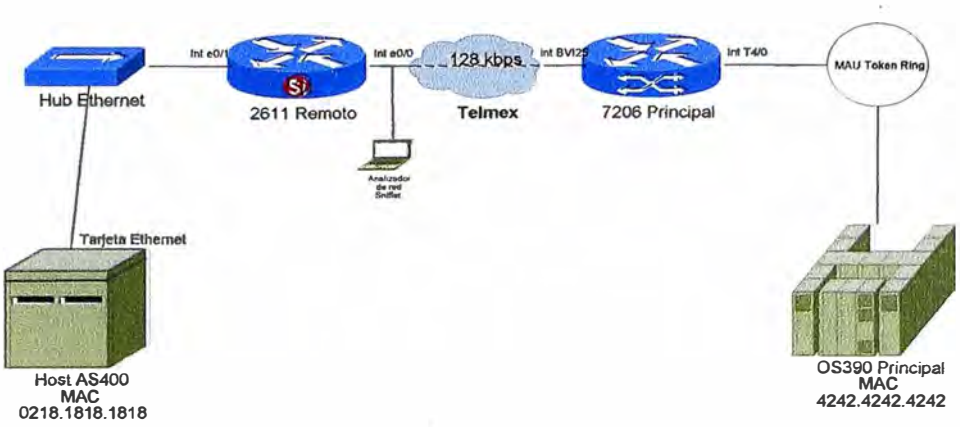

Figura 3.7: Prueba sin encriptación con AS400 – Ethernet

Desempeño de las consultas: Se efectuó una consulta típica, se tomaron los siguientes datos:

- Tiempo de respuesta: 2 seg.
- Uso del CPU: Se uso el 2% del CPU.
- Uso Máximo del Ancho de banda: Se tuvo un pico de 5,7kps.

Conclusiones: Se observó que el tiempo de respuesta bastante aceptable, el *router* tampoco uso muchos recursos y el ancho de banda fue menor que en los otros casos. El resultado es aceptable, ya que se usa menos del 10% de los recursos de ancho de banda y CPU.

- Interface Serial:

Escenario: Se usó un servidor AS400 con el aplicativo SIB v.3.01.Este servidor tiene una Interface Serial, la cual esta conectada a el puerto serial y este al *router* Cisco 2611:

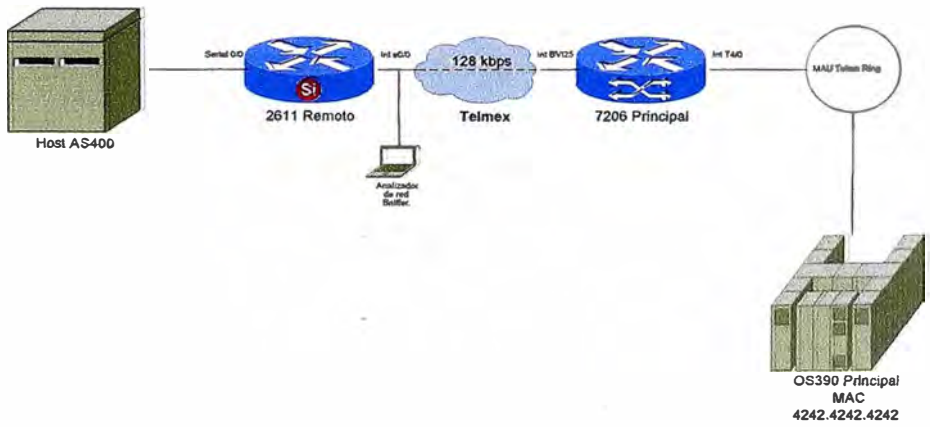

Figura 3.8: Prueba sin encriptación con AS400 - Serial

Desempeño de las consultas: Se efectuó una consulta típica, se tomaron los siguientes datos:

- Tiempo de respuesta: 2 seg.
- Uso del CPU: Se uso el 3% del CPU.
- Uso Máximo del Ancho de banda: Se tuvo un pico de 5,7kps.

3.2.1.2 Pruebas con encriptación con sistemas operativos a utilizar.

Se procede a cifrar la data trasmitida por el enlace WAN. Para efectuar esta comprobación se efectuó una transacción típica primero sin encriptación y luego con encriptación. En los dos casos se captura la data con el *Sniffer* y se comparo observando el nivel de encriptación.

A) Prueba en sistema operativo Windows NT

- Interface Ethernet

Escenario: Se usó un servidor con Windows NT 4.0 con el aplicativo cliente servidor SIB v3.01. Se efectuaron consultas iguales al del punto 2.1 pero cifrando los datos desde que salen del puerto Ethernet 0/0 del Cisco 2611 hasta la entrada de la BVI 25 en el *router* 7206 principal.

Desempeño del aplicativo:

- Tiempo de respuesta: 3 seg.
- Uso del CPU: Se uso el 2% del CPU.
- Uso Máximo del Ancho de banda: Se tuvo un pico de 19,2kps.

Encriptación: Se efectuó la siguiente captura sin encriptación, donde se observa que se puede entender el texto del payload de algunas consultas:

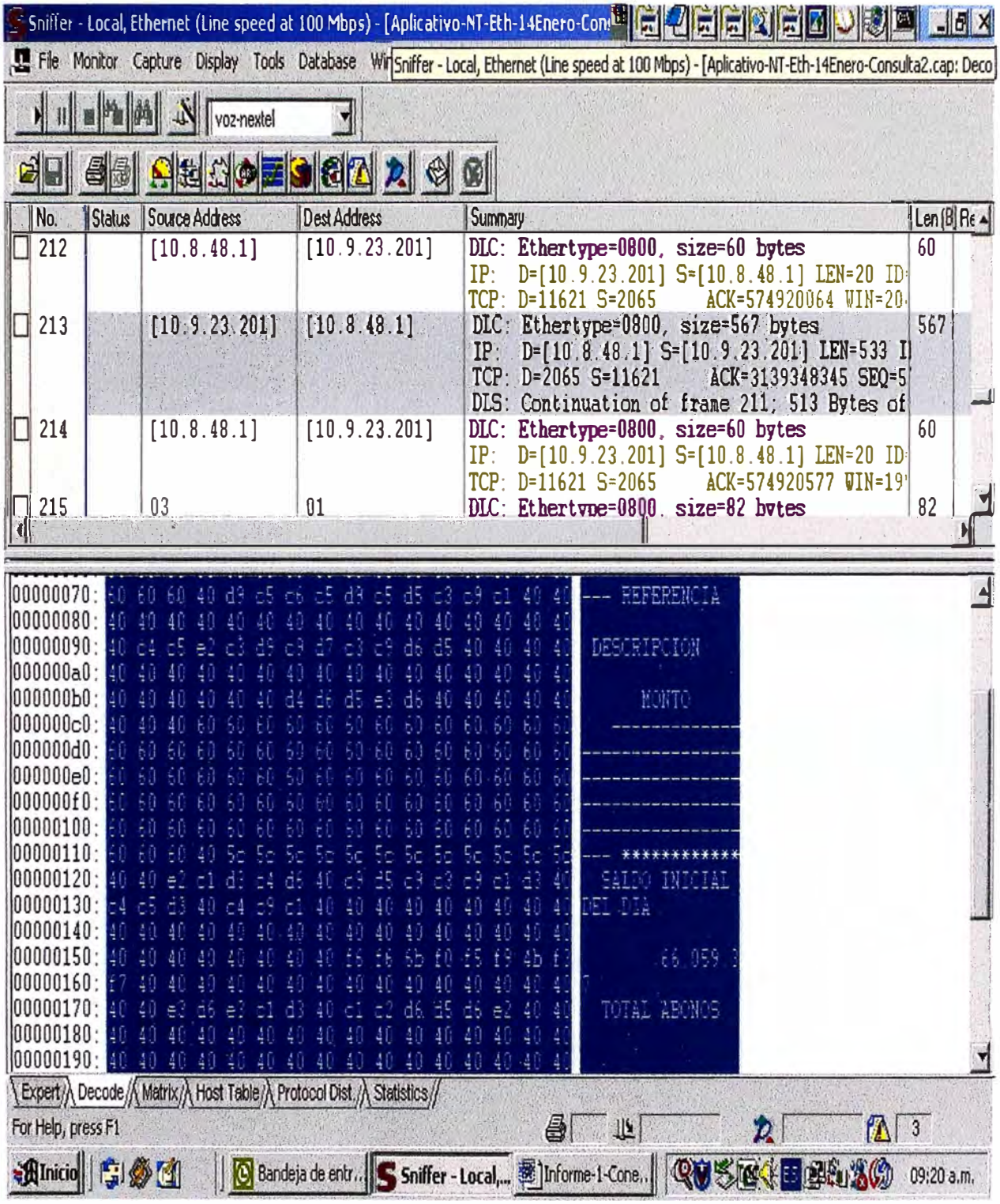

Figura 3.9: Captura del Sniffer sin encriptación

Luego de cifrar se observa la misma consulta y se observa que el texto del payload no se puede descifrable.

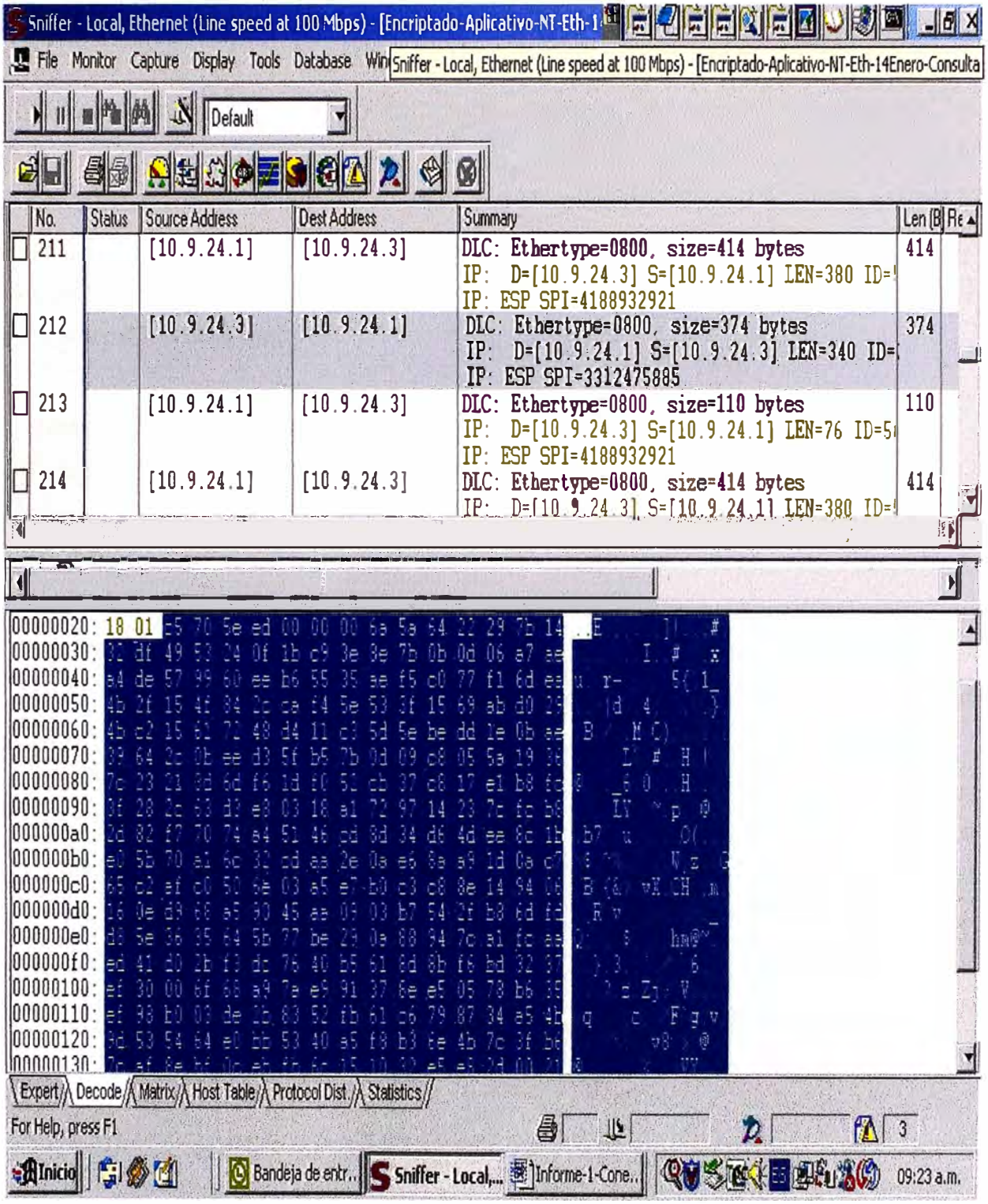

Figura 3.10: Captura del Sniffer con encriptación

Conclusiones: Como vemos el proceso de encriptación no consume altos recursos en los *routers* para este tipo de consultas. Además se comprueba que la data es efectivamente cifrada.

B) Prueba en sistema operativo AS400:

- Interface Ethernet

Escenario: Se usó un servidor AS400 con el aplicativo SIB v.3.01.Este servidor tiene una Interface Ethernet. . Se efectuaron consultas iguales al del punto 2.3 pero cifrando los datos desde que salen del puerto Ethernet 0/0 del Cisco 2611 hasta la entrada de la BVI 25 en el *router* 7206 principal:

Desempeño del aplicativo:

- Tiempo de respuesta: 2 seg
- Uso del CPU: Se uso el 1% del CPU.
- Uso Máximo del Ancho de Banda: Se tuvo un pico de 25kbps.

Encriptación: Se efectuó la siguiente captura sin encriptación, donde se observa al igual que la prueba anterior de que se puede entender el texto del payload de algunas consultas.

Conclusiones: Se observó que el proceso de encriptación no consume altos recursos en los *routers* para este tipo de consultas. Además se comprueba que la data es efectivamente encriptada. El resultado es aceptable, ya que se usa menos del 10% de los recursos de ancho de banda y CPU.

3.2.2 Pruebas de redundancia de nodos.

Se realizaron las pruebas respectivas para corroborar que el sistema de redundancia del proyecto funcionaba, estas pruebas de redundancia de nodos confirman la continuidad del servicio a pesar de la caída del nodo principal. Para ello se configuro los peer de DLSW en forma de Backup en el *router* de Prueba.

Se realizaron tres pruebas las cuales se describen a continuación:

- **CASO I:** *Falla de fibra principal de router 7206 Principal.*

La prueba se efectuó desconectando el jumper de fibra en el *router* 7206 Principal, dando como resultado que inmediatamente en menos de 2 segundos el DLSW PEER del

router secundario pasara a estado conectado y del *router* secundario ha estado desconectado. Mientras tanto el aplicativo demoró 1 minuto y 30 segundos en reestablecer su conexión con el *host* nuevamente. Creando el circuito nuevamente. El mismo resultado se obtiene si se apaga el *router* 7206 Principal.

En conclusión, si el enlace al *router* principal falla, el *host* del Banco tomara 1 minuto y 30 segundos en reestablecer su conexión por el enlace secundario. Esta prueba se realizo con la funcionalidad de encriptación activada.

- **CASO II:** *Falla de fibras en router principal y secundario ó falla de fibra en router 2600 remoto. Se activa ISDN con encriptación.*

Una vez caído el enlace principal, puede darse el caso que también falle la fibra secundaria. Este caso también se aplica en el caso que falle la fibra que llega el cliente remoto. Para ello se usa la redundancia por llamada desde el *router* remoto al *router* secundario por enlace ISDN. Se creo el *Dialer* 1 en el *router* remoto y el *Dialer* 250 en el *router* 7206 Secundario. Antes de caerse la fibra vemos el DLSW PEER al secundario conectado. Apenas cae el enlace secundario se levanta la llamada ISDN al *router* secundario, la perdida de comunicación es por 2 segundos. Nunca se llega a caer ni el DLSW PEER ni el DLSW CIRCUIT. La comunicación sigue encriptada.

En caso caigan las dos fibras al mismo tiempo, es decir si el DLSW PEER estaba en el *router* principal y se caen las dos fibras, se activa el ISDN y se demora 1min 30 seg. es reestablecer la sesión por el *router* secundario.

- **CASO III**: *Recuperación de la Fibra Principal o del router 7206 Principal.*

Una vez que se recupera el enlace principal, existe un tiempo de recuperación para que las sesiones vuelvan a usar el enlace principal y dejen el enlace secundario. Para ello se usa un parámetro en el *router* 2611 que especifica el tiempo desde que se recupera el enlace principal y se anulan las sesiones por el enlace secundario. Una vez recuperada la fibra principal, el DLSW PEER se mantiene por 1 minuto. Luego de pasado el minuto se observa que los dos DLSW PEER están conectados por 30 segundos. Durante este tiempo las sesiones se mantienen activas. Luego, se activa solamente la sesión DLSW PEER con el *router* Principal y se pierden las sesiones durante 5 segundos

Finalmente las sesiones se reestablecen y la pérdida total de conexión fue de 5 segundos cuando se recupera la fibra principal o el equipo principal.

En el Capitulo IV se mostrará las ventajas e inconvenientes de una VPN

CAPITULO IV
VENTAJAS E INCONVENIENTES DE UNA VPN

4.1 Ventajas e inconvenientes de una VPN

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no esta bien definido pueden existir consecuencias serias.

4.1.1 Ventajas de una VPN

La principal ventaja de usar una VPN es que permite disfrutar de una conexión a red con todas las características de la red privada a la que se quiere acceder. El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de un ordenador en esa red privada, pudiendo acceder a la información publicada para esa red privada: bases de datos, documentos internos, etc. a través de un acceso público. Al mismo tiempo, todas las conexiones de acceso a Internet desde el ordenador cliente VPN se realizaran usando los recursos y conexiones que tenga la red privada. Aparte de esta encontramos dos importantes ventajas:

- **Bajo Coste:** Una forma de reducir coste en las VPN es eliminando la necesidad de largas líneas de coste elevado. Con las VPN, una organización sólo necesita una conexión relativamente pequeña al proveedor del servicio. Otra forma de reducir costes es disminuir la carga de teléfono para accesos remotos. Los clientes VPN sólo necesitan llamar al proveedor del servicio más cercano, que en la mayoría de los casos será una llamada local.

- **Escalabilidad:** La implementación y configuración de la VPN es sencilla y rápida, permitiendo un crecimiento escalable en cantidad de puntos. De esta manera evitamos el

problema existía en el pasado al aumentar las redes de una determinada compañía, gracias a Internet, se deriva simplemente en accesos distribuidos geográficamente.

4.1.2 Inconvenientes de una VPN

Las VPN presentan algunos inconvenientes como se muestra a continuación:

- Las redes VPN requieren un conocimiento en profundidad de redes públicas y tomar precauciones en su desarrollo.
- Las redes VPN dependen de un área externa a la organización, y por lo tanto depende de factores externos al control de la organización.
- Las diferentes tecnologías de VPN podrían no trabajar bien juntas.
- Las redes VPN necesitan diferentes protocolos que los de IP.
- Mayor carga en el cliente VPN puesto que debe realizar la tarea adicional de encapsular los paquetes de datos una vez más, situación que se agrava cuando además se realiza encriptación de los datos que produce una mayor ralentización de la mayoría de conexiones.
- Mayor complejidad en el tráfico de datos que puede producir efectos no deseados al cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (proxy, servidor de correo, permisos basados en nombre o número IP).
- Las redes VPN requieren un conocimiento en profundidad de la seguridad en las redes públicas y tomar precauciones a lo largo del desarrollo.
- Las redes VPN dependen de un área externa a la organización, en concreto de Internet, y por lo que depende de factores externos al control de la organización.

CONCLUSIONES

1. Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso.
2. La VPN es utilizado para realizar intranet, extranet y así mismo tener acceso remoto, lo cual puede usar un backbone IP, ATM, Frame Relay o MPLS para poder realizar la comunicación de los puntos remotos, es decir se ha desarrollado diversos protocolos para poder usar los diversas tecnologías de transporte.
3. El Internet ha cambiado la forma como las personas se comunican, cortando distancias geográficas y acelerando la globalización que se esta gestando sobre todo en el aspecto comercial, con esto uno puede aprovechar el Internet para poder comunicar diferentes sedes para esto debemos usar túneles VPNs con esto evitamos el gasto de usar líneas dedicadas o conmutadas, solo tendrías que pagar por el acceso a internet mensualmente, pero hay que tomar en cuenta que el internet no es seguro.
4. La necesidad del uso de la VPN en el proyecto integral de comunicaciones de la red extranet financiera del Banco Central de Reserva del Perú es debido a que los datos necesitan ser enviados en forma segura y para que nadie pueda acceder a dicha información y por que el BCRP no confía en la seguridad que es brindada en el backbone del proveedor.
5. Telmex S.A. ofrece en su solución redundancia de nodos ATM, enlaces BRI en cada sede y un PRI en el *router* de redundancia de la sede principal debido a que los datos que se van a transferir son de alta importancia y la comunicación debe estar siempre activa.

6. Por necesidad de seguridad, confiabilidad y seguridad del servicio el costo de la implementación sería muy elevado es por que Telmex S.A. reduce este costo de implementación usando una red de Bancared ya implementada.
7. Se utiliza en el proyecto del BCRP, según la clasificación de un VPN, el modelo superpuesto y con VPN de nivel 2 debido a que se usa un backbone ATM y VPN de nivel 3 por que se usa el protocolo IPSec; asimismo se usa el VPN extranet según el alcance del VPN para la organización.
8. Las pruebas de conectividad y de redundancia fueron satisfactorias para el cliente y para Telmex S.A., actualmente se van agregando puertas remotas a esta red.

GLOSARIO

A

AAA *Authentication, Authorization and Accounting*: Equipo que controla el acceso de un usuario a la red.

AAL5 *ATM Adaptation Layer* 5: Una de las cuatro AALs recomendadas por ITU-T. AAL5 soporta servicios VBR orientados a conexión, y se utiliza principalmente para transferir IP convencional por tráfico ATM y LANE. AAL5 usa SEAL y es la menos compleja de las recomendaciones AAL actuales. Ofrece una baja sobrecarga en el ancho de banda y requisitos de procesamiento más simples, a cambio de una capacidad de ancho de banda reducida y recuperación de errores.

Ad hoc: donde cada estación puede comunicarse con cualquier otra directamente. También conocida como conexión *peer to peer*.

ARP A*ddress Resolution Protocols*: Un protocolo de resolución de direcciones electrónicas en números IP que corre en redes locales. Parte del conjunto de protocolos TCP/IP.

B

***Bridge*:** Dispositivo que pasa todos los mensajes de una red a otra sin distinguir a cuál red pertenece el destino del mensaje.

C

CPE *Customer Premises Equipment*: Equipo de usuario

D

Datagram: Entidad de datos auto contenido e independiente que transporta información suficiente para ser encaminada desde su ordenador de origen a su ordenador de destino sin tener que depender de que se haya producido anteriormente trafico alguno entre ambos y la red de transporte.

DHCP *Dynamic Host Configuration Protocol*: Un protocolo TCP/IP que asigna dinámicamente una dirección IP a un ordenador.

DSL *Digital Subscriber Line*: Suministra el ancho de banda suficiente para numerosas aplicaciones, incluyendo además un rápido acceso a Internet utilizando las líneas telefónicas; acceso remoto a las diferentes Redes de área local (LAN), videoconferencia, y Sistemas de Redes Privadas Virtuales (VPN).

E

ESP *Encapsulating Security Payload*: proporciona confidencialidad integridad, autenticación y cierta confidencialidad en el flujo de tráfico. Para mayor confidencialidad, la ESP es compatible con los algoritmos de clave cifrada, como DES y triple DES.

G

GRE *Generic Routing Encapsulation*: Un método para enviar datos cifrados desde un ordenador a otro a través de una red local.

I

IKE *Internet Key Exchang*: Intercambio de claves para seguridad en Internet. Estándar que trabaja sobre IP, y establece las reglas para el intercambio de claves de seguridad.

ISDN *Integrated Service Digital Network*: Servicio de acceso al usuario a velocidad de 144 kb/s (2B+D) que aprovecha la planta externa convencional y la señalización SS7.

ISP *Internet Service Provider*: Organización, habitualmente con ánimo de lucro, que además de dar acceso a Internet a personas físicas y/o jurídicas, les ofrece una serie de servicios (por ejemplo, hospedaje de páginas web, consultoría de diseño e implantación de webs e Intranets, etc., etc.)

J

Jitter: Variación del retardo entre los paquetes que se reciben. Fluctuación de fase de una señal digital. El jitter corresponde a una fluctuación de alta velocidad (superior a 10 Hz).

L

L2F *Layer 2 Forwarding*: El protocolo L2F tiene como objetivo proporcionar un mecanismo de *tunneling* para el transporte de tramas a nivel de enlace: HDLC, PPP, SLIP, etc

LAC *L2TP Access Concentrator*: Es un dispositivo físico que se añade a los elementos de interconexión de la red conmutada; como lo es la red telefónica convencional RDSI, o se coloca con un sistema de terminación PPP capaz de gestionar el protocolo L2TP. Un LAC sólo necesita implementar el medio sobre el cual opera el L2TP para admitir el tráfico de una o más LNS. LAC es el iniciador de las llamadas entrantes y el receptor de las llamadas salientes. También se le conoce como el servidor de acceso a la red.

LANE *LAN Emulation*: Servicio ofrecido en ATM que permite emular mediante el protocolo ALL5 la entrada de una LAN.

LDP *Label Distribution Protocol*: Protocolo de Distribución de Etiquetas.

LEC *Local Exchange Carrier*: La compañía de servicio público de teléfono que ofrece servicio local.

LNS *L2TP Network Server*: Opera sobre cualquier plataforma con capacidad de terminación PPP. LNS gestiona el lado del servidor del protocolo L2TP. Ya que L2TP se

apoya sobre el medio al que llegan los túneles L2TP, LNS sólo puede tener una única interfaz LAN o WAN, aunque es capaz de terminar las llamadas entrantes en cualquiera de la amplia gama de las interfaces PPP LAC (asíncronos, RDSI, PPP sobre ATM, PPP sobre Frame Relay). LNS también se conoce como *Home Gateway* (HGW).

LSP *Label Switched Path*: Un camino de datos de envío determinado por etiquetas adjuntas a cada paquete de datos donde los datos son enviados a cada salto de acuerdo con el valor de las etiquetas.

M

MAC *Media Access Control*: Protocolo de capa 2 definido en IEEE 802.1. Las direcciones MAC de 6 bytes sirven para identificación de los componentes en una LAN.

MIB *Management Information Base*: Base de información de datos definido en los protocolos de gestión de redes (por ejemplo en SNMP y CMIP).

MPOA *Multiprotocol over ATM*: Desarrollo del foro de ATM para estandarizar el uso de esta tecnología, especifica cómo los protocolos existentes y futuros de capa 3, como lo son IP, Ipv6, Apple Talk e IPX, corren sobre una red ATM con host, enrutadores y switches de multicapa LAN directamente conectados.

MTU *Maximum Transmission Unit*: Tamaño máximo de paquete en protocolos IP como el SLIP.

Multihomed: Que tiene muchas direcciones en el internet, relacionado a varios puntos de interfase.

N

NAS *Network Access Server*: Un dispositivo de red que proporciona acceso a una red (firewall, dispositivo VPN) a través del protocolo RADIUS.

NAT *Network Address Translation*: Metodología por la cual en una red IP se pueden utilizar direcciones no normalizadas en el interior de la red y normalizadas en la salida al exterior.

O

OSPF *Open Shortest Path First*: Protocolo de resolución de routing usado por los router en una red IP y que se basa en el algoritmo del próximo paso.

Outsourcing: Término que se utiliza para referirse a una forma de organización de la empresa por la cual la dirección de la misma subcontrata a otras empresas externas especializadas una parte de sus actividades, aquellas que considera que no son básicas o esenciales para el cumplimiento de sus objetivos, y en las que no posee una ventaja competitiva, como puede ser el mantenimiento, la seguridad, e incluso, los sistemas informáticos. De este modo, la empresa puede concentrarse en todas aquellas actividades consideradas fundamentales para el desarrollo de su estrategia.

P

PAT *Port Address Translation*: Básicamente consiste en que el router, cuando le solicitan información a través de un puerto TCP determinado, este le pasa la solicitud al servidor apropiado ubicado dentro de la red, y vuelve a enviar la respuesta del servidor al usuario de Internet que lo solicitó.

PDA *Personal Digital Assistants*: Computadora pequeña con reconocimiento de escritura, como entrada de datos.

PKI *Public Key Infraestructure*: Conjunto integrado de tecnologías que se necesitan para ofrecer servicios de encripción de claves públicas y de firma electrónica.

PPP *Point-to-Point Protocol*: Protocolo de comunicaciones serial utilizado en enlaces de redes.

PSTN *Public Switched Telephone Network*: Denominación genérica para las redes de telefonía pública convencionales.

R

RADIUS *Remote Authentication Dial-In User Service*: Método de autenticación remota soportado por la mayoría de redes y vendedores de software.

RIP *Routing Information Protocol*: Este protocolo asociado al IP en Internet es el primero que permitió la comunicación entre router para actualizar las tablas de ruta en forma periódica.

Router: Un dispositivo (o programa de software) que maneja la conexión entre dos o más redes. Los ruteadores se encargan de buscar la dirección de destino de los paquetes que pasan por ellos y deciden hacia cual ruta enviarlos.

RSVP *Resource Reservation Protocol*: Protocolo utilizado para reservar recursos en redes.

S

SA *Security Association*: Conjunto de parámetros que define los servicios y los mecanismos necesarios para proteger las comunicaciones de seguridad de Protocolo Internet. Consulte también seguridad de Protocolo Internet (IPSec).

SOHO *Small Office/Home Office*: Segmento del mercado compuesto por empresas de pequeña envergadura (Small Office) y toda la gama de profesionales liberales (Home Office).

SPI *Security Parameter Index*: Parámetro utilizado en IPSec para la identificación de una asociación segura.

Switch: Dispositivo de red que filtra, envía e inunda de frames en base a la dirección de destino de cada frame. El switch opera en la capa de enlace de datos del modelo OSI. En

general se aplica a un dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar.

T

TACACS+ *Terminal Access Controller Access Control System Pluss*: Mejora a TACACS propietaria de Cisco. Provee un soporte adicional para autenticación, autorización y costos

TTL *Time to Live*: Contador interno que incorporan los paquetes Multicast y determinan su propagación antes de ser eliminado de la red y notificada dicha acción.

Tunneling: En Internet, este término se aplica al uso de la Red como parte de una red privada segura. El túnel es un conducto específico por el que viajan los mensajes o ficheros de una determinada empresa.

V

VPN *Virtual Private Network*: Referido al servicio de interconectar dos o más redes de usuario mediante una red pública pero manteniendo la privacidad y calidad.

VCC *Virtual Channel Connection*: Circuito lógico compuesto por VCLs, que transporta datos entre dos puntos finales en una red ATM. También llamada conexión de circuito virtual.

BIBLIOGRFÍA

[1] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[2] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[3] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[4] Hanks, S., Li, T., Farinacci, D. and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994.

[5] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[6] Harkins, D. and C. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[7] Kent, S. and R. Atkinson, "IP Encapsulating Security Protocol (ESP)", RFC 2406, November 1998.

[8] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[9] Perez, M., Liaw, F., Mankin, A., Hoffman, E., Grossman, D. and A. Malis, "ATM Signalling Support for IP over ATM", RFC 1755, February 1995.

[10] Malkin, G. "RIP Version 2 Carrying Additional Information", RFC 1723, November 1994.

[11] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[12] Valencia, A., Littlewood, M. and T. Kolar, "Cisco Layer Two Forwarding (Protocol) "L2F"", RFC 2341, May 1998.

[13] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W. and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999.

[14] G. Pall, G. Zorn "Microsoft Point-To-Point Encryption (MPPE) Protocol", RFC 3078, March 2001.

[15] W. Simpson, "IP in IP Tunneling", RFC 1853, October 1995

[16] G. Zorn, S. Gobb "Microsoft PPP CHAP Extensions", RFC 2433, October 1998