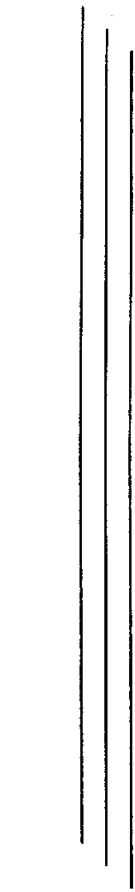
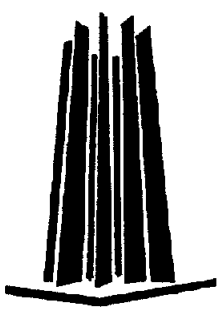
VNIVERSIDAD NACIONAL
AVFNOMA DE
MEXICO





UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

"IMPLEMENTACION DE UNA VPN (RED PRIVADA VIRTUAL) SOBRE UN MODELO VPN-SUPERPUESTO"

DESARROLLO DE UN CASO PRÁCTICO

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN
P R E S E N T A N:

PEDRO HERRERA MARTÍNEZ
ISRAEL VILLANUEVA QUINTANA

ASESOR:
ING. FRANCISCO RAÚL ORTÍZ GONZÁLEZ

SAN JUAN DE ARAGÓN, ESTADO DE MÉXICO, 2005

A MIS PADRES

A mis padres por darme la vida, porque siempre confiaron en mí y nunca dejaron de apoyarme para poder terminar mi carrera. A ellos porque me dieron la mejor herencia de la vida.

A MI MADRE

Que es el ser mas maravilloso del mundo. Gracias por tu cariño y comprensión que desde pequeño me has brindado por guiar mi camino y estar junto a mi en los momentos mas difíciles. ,

A MI PADRE

Porque desde pequeño ha sido para mí un hombre grande y maravilloso que siempre he admirado. Gracias por guiar mi vida con energía, esto es lo que ha hecho de mi lo que soy

Al amor de mi vida

Por darle esa luz al túnel de mi vida y la alegría más grande del mundo, por ese alguien que por el destino no llegó a mi vida. Gracias por tu comprensión y amor.

A ANTONIO SOLANO

Que sin su valioso apoyo no hubiese podido realizar este proyecto.

A mi familia

Por los valores que me inculcaron, así como todos los esfuerzos y sacrificios que asumieron durante toda mi formación. Quiero darles las gracias por haber estado a mi lado en todo momento a lo largo de mi vida y por el tiempo que duró esta carrera que hoy por fin llega el momento de culminar.

A mi papá

Quiero que sepas que para mí tu eres el mejor del mundo y siempre estaré orgulloso de ti.
(Gracias por apoyarme siempre)

A mi mamá

Por que nunca dejaste de confiar en mí y tuviste la paciencia eterna de esperarme hasta este día.
(Te quiero mucho)

A mis hermanos

Por soportarme tantos años, por su paciencia, por su apoyo incondicional y por su confianza.

Pero en especial quiero dedicar este trabajo a la persona que hizo girar mi vida y darme la creatividad necesaria para poder terminar este trabajo, creo que nunca hubiera llegado a su final sino hubiera sido por mi Chikitere.

A mi esposa quien me enseñó a superar los momentos de flaqueza y a convertir los grandes problemas en simples preocupaciones y sobre todo me ha dado toda la energía que necesito para poder realizar un trabajo así de enorme.
Sólo espero saber corresponderle en los momentos en que me necesite.

"MÍA, gracias por haber logrado retornarme a la conciencia después de estar oculto como un río subterráneo"

CAPÍTULO 3. IPSEC

La práctica de la ingeniería siempre ha estado relacionada con la evolución de las nuevas tecnologías. Los ingenieros han explotado nuevos sistemas y conceptos que han ampliado sus posibilidades, hoy en día, la tecnología de las microcomputadoras ha proporcionado un sinnúmero de nuevas herramientas poderosas que tienen un profundo efecto en la ingeniería.

Debido a que el alcance de la computación tiene que ver con su capacidad para la manipulación y almacenamiento de datos, la ingeniería, por su dependencia de las matemáticas y su necesidad de información exacta, es un área ideal para el uso potencial de la computadora, por lo que en este trabajo se utilizará como herramienta principal.

La seguridad es un aspecto de gran relevancia en las redes actuales, se considera un requisito indispensable hoy en día para la creación y diseño de las nuevas redes.

El caso práctico en estudio hace referencia a la Implementación de un RPV (Red Privada Virtual) sobre un modelo RPV-SUPERPUESTO.

Para poder comprender el protocolo IPSec se define su funcionamiento detallando los dos modos de operación: túnel y transporte apuntando hacia el primer modo, ya que es el que proporciona los servicios de encriptación de información y sobretodo nos brinda la seguridad necesaria para que opere correctamente una RPV sobre Internet.

El protocolo de seguridad IP (IPSec), juega un papel importante para las redes que utilizan como protocolo de comunicación fundamental a IP, brinda una solución general para aplicar mecanismos de seguridad como autentificación, confidencialidad, integridad, protección a la réplica, independientemente de las aplicaciones que se utilicen a nivel de usuario.

El hecho de desarrollar un proyecto de este tipo es para buscar una solución de conectividad entre las redes distantes geográficamente, siendo muchas las alternativas que aparecen como posibles. La clave está en encontrar una solución que supla las necesidades de los usuarios. Es por ello que hay que tener en cuenta aspectos como:

- Seguridad en el manejo de la información.
- Costos de implementación y manutención.
- Conexión segura a servidores.
- Unión de los diferentes componentes de una red.

- Identificación de plataformas.
- Recursos existentes que se pueden utilizar.

Teniendo claro los requerimientos de la conectividad hay que evaluar las posibles soluciones. Este proyecto busca dar solución de conectividad a un grupo de redes distantes las cuales pueden estar en diferentes plataformas de trabajo. Su estructura de funcionamiento requiere que estas redes funcionen con una lógica local lo cual se torna complejo por un tema de distancias. Bajo esta perspectiva muchas de las soluciones a este problema (Fibra Óptica, RDSI, Frame Relay, etc.) quedan fuera por temas de costo y manutención. Es necesario por ello analizar estándares de conectividad que además de trabajar en múltiples plataformas, cumplan con los requerimientos del usuario siempre orientado a una lógica local de trabajo. Por lo anterior, se hace necesario el estudio de las Redes Privadas Virtuales, las cuales no necesitan de una inversión grande y que para poder comunicar a sus puntos remotos con seguridad solamente necesita la conexión a la red pública de Internet.

Una Red Privada Virtual (RPV), 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 RPV's es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables.

La seguridad supone aislamiento y "privacidad" porque el usuario "cree" que posee los enlaces. Las RPV's son soluciones de comunicación RPV basadas en el protocolo de red IP.

1.1 Introducción a las Redes Privadas Virtuales

Las primeras redes de computadoras fueron implementadas con dos tecnologías fundamentales: líneas dedicadas para una conectividad permanente y conexiones conmutadas 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 proporcionaban una buena relación costo-beneficio por dos razones fundamentales:

- El promedio de tráfico entre dos sitios de una red varía basado en muchos factores, siendo el principal: la hora crítica del día, de la semana y del mes.

- 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 nuestro país las primeras soluciones de este tipo de conectividad que fueron implementadas se basaron en el protocolo X.25, luego Frame Relay y más tarde ATM. A continuación se muestra un ejemplo de una RPV típica construida con tecnologías Frame Relay.

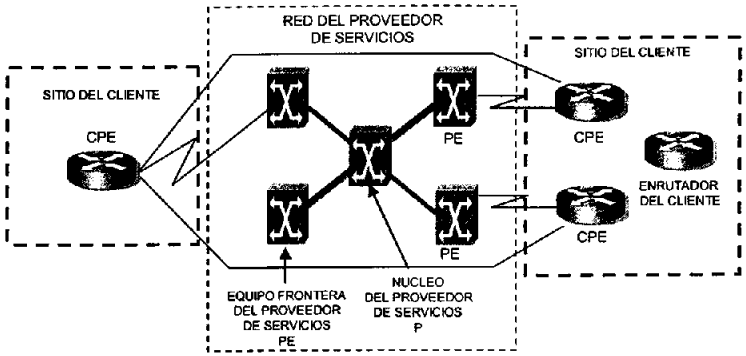


Figura 1. RPV Frame – Relay.

Como se puede observar, las soluciones RPV tienen como componentes:

- El proveedor de servicio (SP, Service Provider), es la organización propietaria de la infraestructura (el equipamiento y el medio de transmisión) con la que brinda emulación de líneas dedicadas a los clientes.

- La conexión del cliente a la red del SP a través del equipo local del cliente (CPE, Customer Premises Equipment).

Usualmente el CPE es un PAD (Packet Assembly and Disassembly) que brinda conectividad terminal, un bridge o un enrutador; el dispositivo CPE es a veces llamado también frontera del cliente (CE, Customer Edge). El CPE es conectado a través de un medio de transmisión (usualmente líneas dedicadas, pero también puede ser de forma conmutada) al equipo del SP el que puede ser X.25, Frame Relay, ATM o un enrutador IP; el dispositivo de frontera del SP es llamado PE (Provider Edge). El SP generalmente tiene equipos de núcleo en la red, los que son llamados P, (Provider).

1.2 Clasificación de RPV's

Con la introducción de nuevas tecnologías en las redes de los SP y nuevos requerimientos de los clientes, las implementaciones de RPV's se han vuelto más y más complejas y para su solución los servicios de RPV's modernos recorren una gran variedad de tecnologías y topologías.

A continuación se expone una clasificación según los tipos de RPV's, así como una división en categorías, según el alcance de las RPV's para las organizaciones y se

clasificarán las Redes Privadas Virtuales con el modelo implementado superpuesto e Igual a Igual.

Las redes RPV's pueden ser clasificadas por varias vías. La clasificación más utilizada está basada en la información de enrutamiento que es intercambiada o no entre los clientes y los SP's.

- El modelo superpuesto (overlay), donde el SP simula líneas dedicadas para el cliente.
- El modelo Igual a Igual donde el SP y el usuario intercambian información de enrutamiento de Nivel 3, en el que el proveedor transporta los datos entre los sitios del usuario por un trayecto óptimo en lo cual el usuario no interviene.

1.2.1 Modelo Superpuesto (Overlay)

El modelo superpuesto se puede comprender de una forma mejor porque en él existe una clara separación entre las responsabilidades del cliente y del SP.

El SP brinda al cliente una configuración que simula líneas dedicadas llamadas circuitos virtuales (VC, Virtual Circuit), que pueden estar disponibles constantemente (PVC, Permanent Virtual Circuit) o establecidas bajo demanda (SVC, Switched Virtual Circuit).

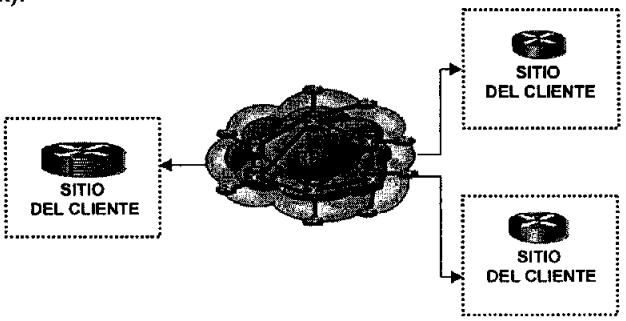


Figura 2. Topología de red RPV Superpuesta.

Como se observa el cliente establece comunicación entre sus enrutadores sobre los VC's suministrados por el SP. La información de los protocolos de enrutamiento siempre es intercambiada entre los dispositivos del cliente por lo que el SP desconoce la topología interna de la red del cliente.

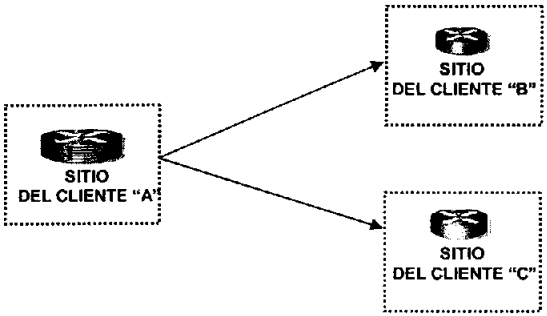


Figura 3. Enrutamiento en red RPV Superpuesta.

1.2.2 Modelo Igual a Igual

En el modelo Igual a Igual el PE es un enrutador que intercambia directamente información de Nivel 3 con el CPE como se indica en la Figura 4.

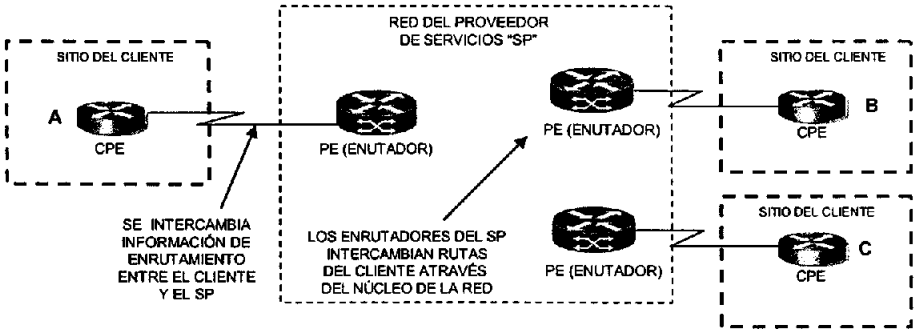


Figura 4. RPV Igual a Igual.

En grandes redes de SP los dos modelos pueden ser combinados, el modelo de RPV Igual a Igual puede utilizar RPV superpuestas en la parte de acceso (ejemplo, los clientes conectados a los enrutadores PE a través de Frame Relay o ATM) o en el núcleo (ejemplo, enlazando los enrutadores P del SP a través de ATM).

El modelo de RPV superpuesto puede ser implementado con tecnologías de conmutadores de redes WAN de Nivel 2 (Frame Relay, ATM) o con tecnologías de túneles de Nivel 3 IPSec (Internet Protocolo Security).

El modelo tradicional de RPV Igual a Igual ha sido implementado con complejos artificios de enrutamiento o con listas de acceso IP, lo cual ha presentado un número de inconvenientes.

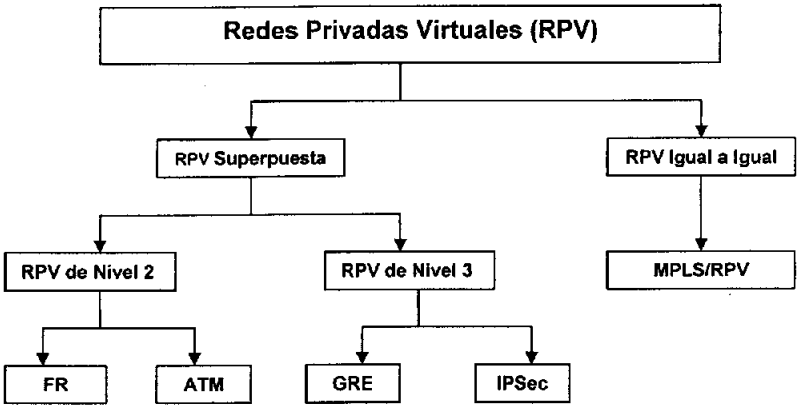


Figura 5. Clasificación de las RPV según tecnología subyacente.

Las RPV's basadas en MPLS superan la mayor parte de los inconvenientes de las otras tecnologías de RPV Igual a Igual, posibilitando a los SP combinar los beneficios de los modelos Igual a Igual (simplificar el enrutamiento, simplificar la implementación de los requerimientos de los clientes) con la seguridad y el aislamiento del modelo de RPV superpuesto.

1.3 Categorías de RPV

De acuerdo a la implementación que le da una organización a la RPV, ésta se divide en tres categorías:

- RPV intranet, entre departamentos de una misma organización.
- RPV extranet, entre una organización, sus socios, clientes y suministradores.
- RPV con accesos remotos, entre la organización y empleados móviles o remotos.

1.3.1 RPV Intranet

Las RPV's 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 RPV. Las RPV's Intranet han sido generalmente implementadas con tecnologías tradicionales como X.25, Frame Relay o ATM.

Característica:

- Extiende el modelo IP a través de la WAN compartida.

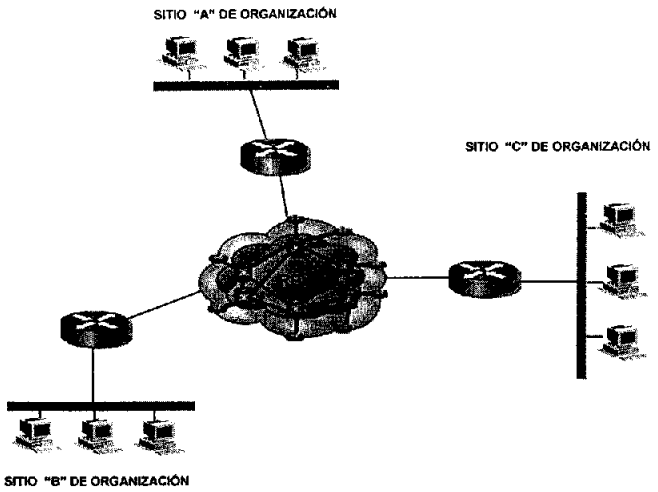


Figura 6. RPV como Intranet.

1.3.2 RPV Extranet

Las RPV Extranet frecuentemente tienen lugar interconectando sitios principales de diferentes organizaciones usualmente dedicando dispositivos de seguridad como firewall o de encriptación.

Características:

- Extiende la conectividad a proveedores y clientes sobre una infraestructura compartida usando conexiones virtuales dedicadas.
- Los pharters tienen diferentes niveles de autorización.
- Listas de Control de Acceso, Filtros (firewalls), según decida la empresa.

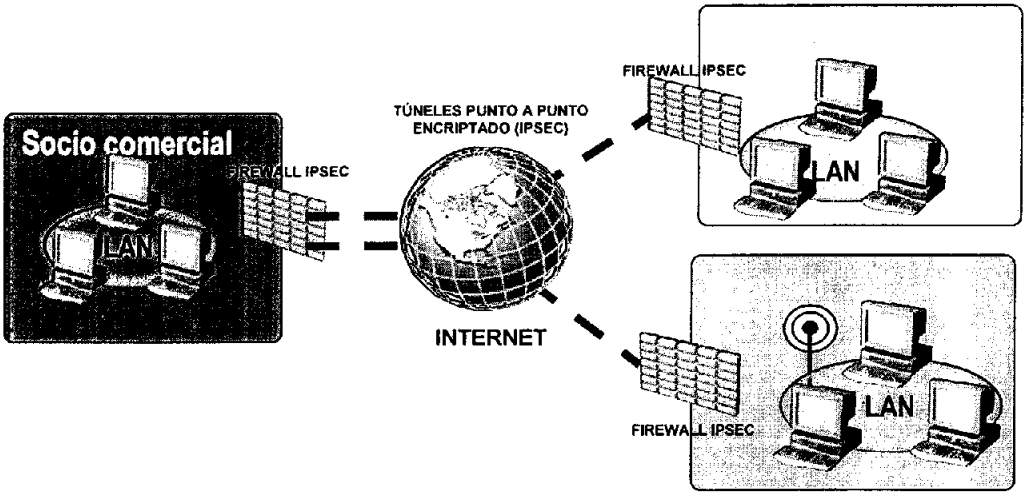


Figura 7. RPV extranet utilizando Internet.

Esta configuración presenta menos requerimientos de calidad de servicio y hace a Internet más adaptable para este tipo de RPV para comunicación entre organizaciones. No es una sorpresa que cada vez más el tráfico entre organizaciones se realice a través de Internet.

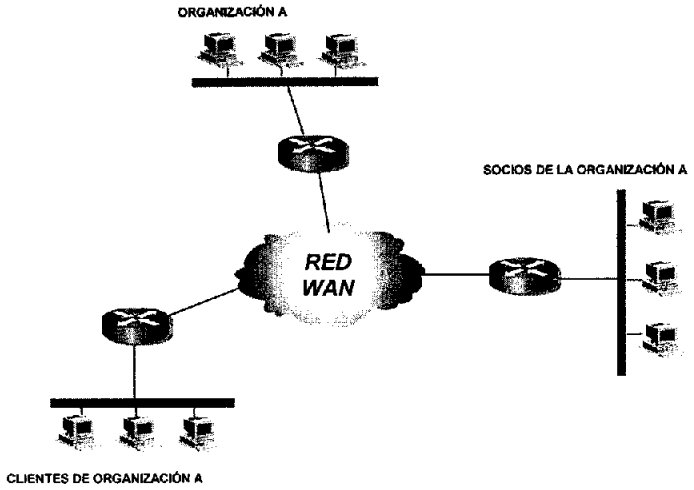


Figura 8. RPV como Extranet.

1.3.3 RPV Con Accesos Remotos

Por último las RPV con Accesos Remotos, utilizan protocolos como L2F, Layer 2 Forwarding o L2TP, Layer 2 Tunneling Protocol.

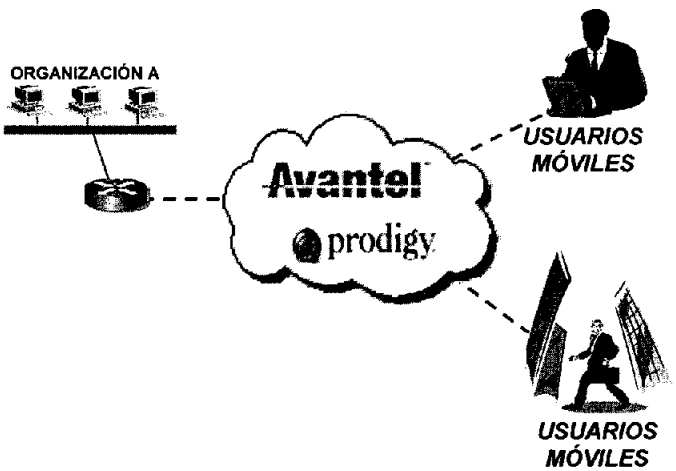


Figura 9. RPV con Accesos Remotos.

Las categorías expuestas anteriormente no son excluyentes, es decir, una red puede estar conformada por una combinación de ellas, incluso por la unión de las tres categorías; RPV intranet, RPV extranet y accesos remotos.

Características:

- Outsourcing de acceso remoto.
- Instalación y soporte del SP (Proveedor de Servicio).
- Acceso único al nodo central (elimina la competencia por puertos).
- Tecnologías de acceso ISDN, XDSL.
- Movilidad IP.
- Seguridad reforzada por el cliente AAA (Autentificación, Autorización, Contabilidad) en el ISP (Proveedor de servicio de Internet) proporciona 1° y posiblemente 2° nivel de seguridad.

1.4 Ventajas de una RPV

- Seguridad: provee encriptación y encapsulación de datos de manera que hace que estos viajen codificados y a través de un túnel.

- Costos: ahorran grandes sumas de dinero en líneas dedicadas o enlaces físicos.

- Mejor administración: cada usuario que se conecta puede tener un número de IP fijo. Asignado por el administrador, lo que facilita algunas tareas como por ejemplo mandar impresiones remotamente, aunque también es posible asignar las direcciones IP dinámicamente si así se requiere.

- Facilidad para los usuarios con poca experiencia para conectarse a grandes redes corporativas transfiriendo sus datos de forma segura.

A lo largo de este capítulo se describieron todas las características y tipos de las redes privadas virtuales ayudando con esto a comprender el beneficio que trae implementarla en una organización en donde se busca tener una seguridad apropiada para el manejo de datos, además de tener un ahorro considerable en la implementación de éstas. A continuación se detallará la forma en que trabaja el protocolo Frame Relay indicando también sus ventajas de operación esto con el fin de comparar ambas tecnologías y entender el por qué de el modelo propuesto para este trabajo.

2.1 Antecedentes

Las técnicas actuales de conmutación de paquetes llamadas conmutación rápida de paquetes toman ventaja de los medios de transmisión confiables, como la fibra óptica y la de alta velocidad de procesamiento de los conmutadores para eliminar algunos procesos de control de flujo y detección/corrección de errores como en X.25. Dentro de las técnicas de conmutación rápida de paquetes se encuentra Frame Relay.

Frame Relay fue aceptado porque dio repuesta a necesidades concretas del mercado, tales como: la necesidad de mayor velocidad en las comunicaciones, mayor rendimiento y seguridad en la transmisión. Dentro de los principales factores que impulsaron el desarrollo de Frame Relay se encuentran:

- El cambio en el contenido de la información de texto a gráficas.
- Incremento en aplicaciones de datos de tráfico tipo ráfaga.
- Dispositivos de usuario más inteligentes y más demandantes de ancho de banda.
- Alta proliferación de redes de área local.

La tecnología Frame Relay optimiza la transferencia de información sobre las facilidades actuales de transmisión digital y opera en las dos primeras capas del modelo OSI. El protocolo que utiliza Frame Relay en la capa se basa en el protocolo LAPD. Su función es delimitar tramas, cálculo y verificación de los códigos de redundancia, así como controlar la congestión para proporcionar un servicio de transmisión de tramas confiable.

Frame Relay cambia el multiplexaje estadístico de X.25 con las características de alta velocidad y bajo retardo de TDM. Es decir, organiza los datos en unidades individuales conocidas como tramas, a las cuales agrega direccionamiento, en lugar de usar ranuras de tiempo como TDM.

Frame Relay es una tecnología con base a tramas que usan circuitos virtuales para transportar datos desde una localidad de usuarios hasta las instalaciones de otro, proporcionando múltiples conexiones lógicas sobre un solo circuito físico, además delimita y entrega las tramas en el orden correcto, enruta, multiplexa y deja a los protocolos de capas superiores, como TCP/IP, las funciones de corrección de errores, acuse de recibo, y retransmisión de tramas, así como la secuencia numerada.

Las capas superiores son las responsables de la transmisión de datos extremo a extremo libre de error. El CRC es la única verificación de error que realiza la red. Las tramas que contienen un CRC equivocado se descartan.

Características

- Es una tecnología de conmutación de paquetes a alta velocidad.
- Consta de componentes físicos y lógicos (realiza la conexión a través de Circuitos Virtuales).
- Frame Relay se generó para satisfacer necesidades específicas del mercado.
- Bajo costo: permite la integración de diferentes tecnologías en un mismo enlace.
- Arquitectura abierta, con base a estándares.
- Realiza el transporte de tramas en forma transparente.
- Detecta errores de transmisión y de formato (no los corrige).
- Conserva el orden de las tramas.
- Combina los beneficios de X.25 y TDM.
- Opera en las capas 1 y 2 del modelo OSI.

2.2 Elementos de una red Frame Relay

El modo en que opera Frame Relay se encuentra determinado por la creación de PVC´s, SVC´s, y DLCI´s. Por ejemplo si una estación de trabajo envía paquetes de datos a un dispositivo de acceso Frame Relay (enrutador o FRAD), éste envía los datos a través de conexiones de puerto compuesto por circuitos virtuales permanentes o conmutados (PVC o SVC) a un conmutador de Frame Relay, el cual lee la dirección destino contenida en el subcampo DLCI de la cabecera de la trama, entonces el dispositivo de la red (conmutador / switch) enruta la trama al destino adecuado a través de la red Frame Relay. En el otro extremo de la red, la información de tramas Frame Relay se elimina y los datos se ensamblan en su formato de paquetes original (IP) para ser procesados por la estación receptora.

Una red Frame Relay se encuentra compuesta por elementos físicos y lógicos donde:

- Elementos Físicos: incluyen todos los elementos de hardware que permiten llevar a cabo la comunicación en una red Frame Relay. Dentro de estos elementos se encuentran: el equipo de usuario (servidores, estaciones de trabajo, etc.), el equipo de acceso a la red Frame Relay (enrutadores, Frads), conmutadores / switches Frame Relay), y por supuesto los enlaces digitales (E1, E3, DS0) que proporciona la red pública.

- Elementos Lógicos: son circuitos y trayectorias virtuales, los cuales permiten llevar a cabo las conexiones a través de elementos físicos entre los diferentes nodos que conforman la red.

2.2.1 Switches Frame Relay

Los conmutadores o switches Frame Relay son los que componen a la "nube" o red Frame Relay y son los encargados de conmutar o enrutar las tramas a través de la red hasta el dispositivo destino. Esto lo hacen mediante el establecimiento de conexiones virtuales, permitiendo el transporte a alta velocidad en forma segura y confiable. Los conmutadores Frame Relay cuentan con las siguientes características:

- Permiten la conexión a enlaces desde 64 kbps hasta 34 Mbps.
- Soportan interfaces seriales V.35 para conexión WAN (DS0) Y RS232.
- Soportan conexiones WAN mediante enlaces digitales E1, interfaces G.703/G.704
- Permiten la conexión a equipos de voz PBX, mediante enlaces E1 de voz (G.703).
- Permiten la conexión a FRAD´s y enrutadores.
- Permite la conexión a dispositivos de video.

2.2.2 Equipos de acceso a una red Frame Relay

Los equipos a la red Frame Relay tienen la responsabilidad de entregar las tramas a la red un formato pre-establecido. Dentro de los equipos de acceso a una red Frame Relay se encuentran los equipos de acceso FRAD´s y los enrutadores, donde:

- Un FRAD recibe información de voz/datos a través de diferentes interfaces y la integra en tramas de Frame Relay para su transporte a través de la red pública o privada. Comúnmente un FRAD cuenta con las siguientes interfaces.
- Puertos WAN (Red de Área Amplia). Interfaces RS232-C V.35 (DS0).
- Puertos LAN. Puertos Ethernet (10 y 100Mbps) para la conexión a la red LAN (Red de Área Local), comúnmente la integran uno o dos puertos.
- Puertos de voz. Interfaces analógicas que permiten la conexión a extensiones telefónicas o equipos multilínea de voz.
- Un enrutador tiene la función específica de enrutar la información de una LAN a la WAN. Por lo tanto, los dispositivos pueden soportar el mismo tipo de puertos de datos que una FRAD. Algunos enrutadores soportan puertos analógicos de voz.

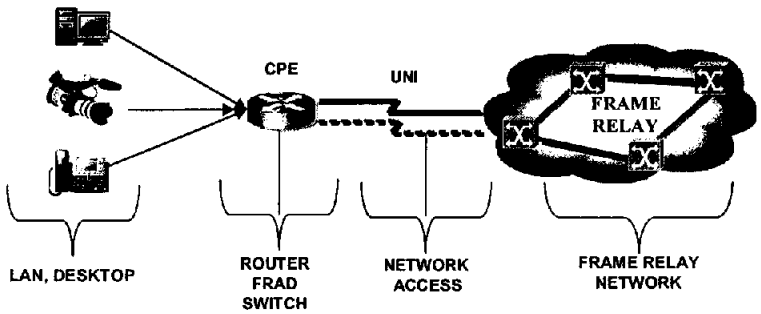


Figura 10. Elementos de una Red Frame Relay.

2.3 Operación de Frame Relay

La tecnología Frame Relay se basa en el concepto de circuitos virtuales o VC´s. Los VC´s son trayectorias entre dos puertos de datos, definidas por un software que actúa como una línea privada. Estos circuitos virtuales pueden ser permanentes (Permanent Virtual Circuit / PVC´s) o conmutados (Switched Virtual Circuit / SVC´s).

Dentro del proceso de envío y transmisión de tramas Frame Relay existen dos puntos importantes:

1. Verificación de la trama. Cuando el equipo de Frame Relay se dispone a enviar la información debe verificar la integridad de la trama utilizando la información contenida en el campo FCS (Frame Check Secuence) de la trama. En caso de que se detecte un error, la trama será eliminada. Existen dos razones principales para eliminar una trama: por detección de errores en los datos y por congestión en la red.

2. Comparación de DLCI´s. Después de verificar la trama se analiza el DLCI creado en el conmutador de Frame Relay. Si no existe un DLCI definido en la tabla para ese enlace, la trama se elimina. Si la trama es valida y el DLCI se encuentra en la tabla de enrutamiento, la trama se envía hacia su destino por el puerto especificado en la siguiente tabla.

DLCI	FUNCIÓN
0	Canal LMI (Interfase de Administración Local), usado para transportar los mensajes LMI para señalización de llamadas e integridad de enlace.
1 - 15	Reservados para uso futuro
16 – 991	Disponibles para Circuitos Virtuales
992 – 1007	Administración de la capa 2 del servicio portador FR. Usados para transmitir información relacionada con la red.
1008 - 1022	Reservados para usos futuros.
1023	Administración en canal de capas, usado para pasar mensajes de interfaces de administración que tienen relación con protocolos de capas superiores a través de la conexión.

Tabla 1. Información de Operación Del DLCI

Ya que:

- DLC'I Identifica un enlace lógico.
- El DLC'I de acceso se asigna manualmente. El de troncal se asigna dinámicamente.
- Debido a su significado local es responsabilidad de la red mapear los DLCI's de acceso a los destinos, este significado local también permite que éstos sean reutilizados en diferentes interfaces.

2.3.1 Circuitos Virtuales Permanentes PVC´s

Los PVC´s se establecen manualmente por el operador de la red mediante un sistema de administración y permiten el establecimiento de una conexión entre dos sitios en forma permanente. Estos enlaces se pueden modificar posteriormente. Dentro de la red la trayectoria del enlace puede variar debido a re-enrutamientos que puedan ocurrir por fallas o alguna otra causa, pero los puntos extremos de la conexión siempre son los mismos. En este sentido el PVC es como una línea dedicada.

Características

- Se utilizan cuando la transferencia de datos entre dispositivos es constante.
- Reducen el uso del ancho de banda asociado con el establecimiento y la terminación de los circuitos virtuales, pero aumentan los costos debidos a la disponibilidad constante del circuito virtual.

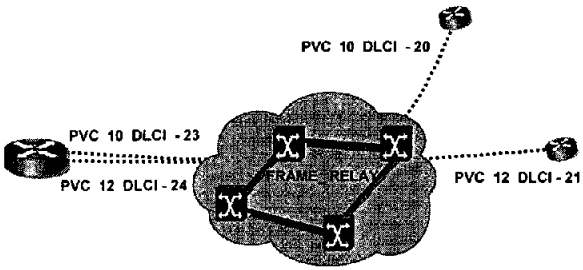


Figura 11. PVC "Circuitos Virtuales Permanentes".

2.3.2 Circuitos Virtuales Conmutados SVC´s

Los circuitos virtuales conmutados se establecen con base a una solicitud de conexión. El usuario especifica una dirección destino, así como los requerimientos de ancho de banda. El manejo de SVC´s es más complicado que el de los PVC´s, sin embargo, este proceso debe ser transparente para el usuario. La red Frame Relay debe atender la solicitud y establecer la conexión en base a la solicitud.

Los SVC's son conexiones temporales que se utilizan en situaciones donde se requiere solamente de una transferencia de datos esporádica entre los dispositivos DTE a través de la red Frame Relay. Para ello la operación de una sesión de comunicación a través de un SVC consta de cuatro estados:

1. Establecimiento de la llamada - Se establece el circuito virtual entre dos dispositivos DTE Frame Relay.
2. Transferencia de datos - Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.
3. Ocioso - La conexión entre los dispositivos DTE aún está activa, sin embargo no hay transferencia de datos. Si un SVC permanece en estado ocioso por un periodo definido de tiempo, la llamada puede darse por terminada.
4. Terminación de la llamada - Se da por terminado el circuito virtual entre los dispositivos DTE.

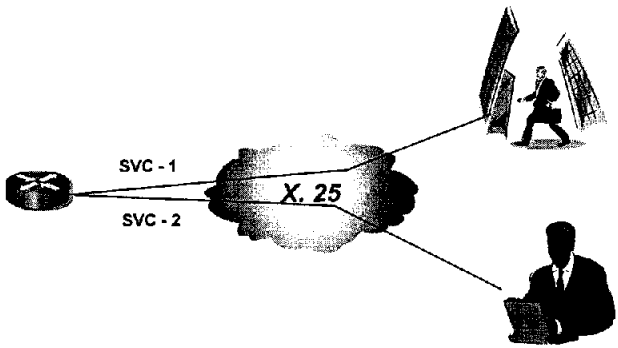


Figura 12. SVC "Circuitos Virtuales Conmutados".

Una vez finalizado un circuito virtual los dispositivos DTE deben establecer un nuevo SVC si hay más datos que intercambiar. Se espera que los SVC's se establezcan, conserven y finalicen utilizando los mismos protocolos de finalización que se usan en ISDN. Sin embargo, pocos fabricantes de equipos DCE Frame Relay soportan SVC's. Por lo tanto, su utilización real es mínima en las redes Frame Relay actuales.

2.3.3 Identificador de conexión de enlace de datos (DLCI)

El DLCI es el número de circuito virtual que corresponde a un destino en particular. Es ésta información la que utilizan los conmutadores Frame Relay para enrutar las tramas al destino correspondiente. El DLCI permite que las tramas que llegan a un conmutador Frame Relay se puedan enviar a través de la red utilizando un procedimiento simple. Un DLCI se encuentra determinado por 10 bits de los 2 bytes que conforma el encabezado de la trama Frame Relay.

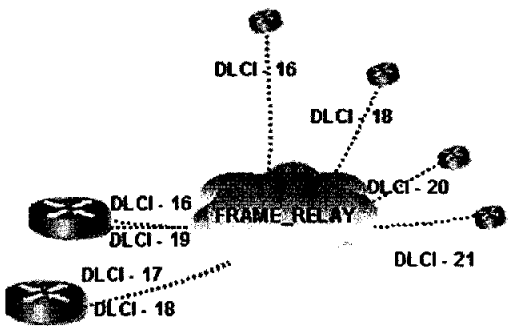


Figura 13. DLCI "Identificador de conexión de datos".

2.4 Parámetros de transmisión de Frame Relay

Frame Relay no tiene un mecanismo de control de flujo, por lo que los usuarios pueden enviar teóricamente todos los datos que deseen a través de una red Frame Relay. Esto significa que el protocolo no tiene ningún medio de prevenir que el ancho de banda sea consumido por un solo usuario. Esta es la razón por la que los servicios de una red pública Frame Relay hayan desarrollado el CIR.
CIR: (Committed Information Rate, o tasa de información comprometida). Es la tasa a la cual la red se compromete en condiciones normales de operación, a aceptar datos desde el usuario y transmitirlos hasta el destino. Puede ser distinto en cada sentido

Cuando se solicita un servicio de Frame Relay y sus correspondientes circuitos virtuales a un proveedor de dicho servicio, se le pedirá que especifique una velocidad de información comprometida (CIR).

La velocidad de información comprometida no tiene porque ser la velocidad de conexión física. Por lo tanto, se podrá tener una conexión física 2.048 Mbs (E1), pero una CIR de sólo 64 kbps. En el caso de que el tráfico enviado por la red supere a la velocidad de información (CIR), se puede proporcionar una velocidad adicional. Esto se debe a que Frame Relay puede recibir una transmisión que supere al CIR. En este caso la red Frame Relay intentará abrir circuitos adicionales para la transmisión, sólo si la red no se encuentra congestionada.

Las ráfagas por encima del CIR se pueden producir únicamente cuando la red no esté congestionada. Existen dos velocidades garantizadas adicionales que se pueden utilizar por encima del CIR.

2.4.1 Parámetros de tráfico

- Bc (Committed Burst Size o ráfaga comprometida). Es la cantidad de bits transmitidos en el periodo T a la tasa CIR (CIR=Bc/T). En las redes Frame Relay se permite al usuario enviar picos de tráfico a la red por encima de CIR, durante intervalos de tiempos muy pequeños, incluidos en el periodo T.

- Be (Excess Burst Size, o ráfaga en exceso). Es la cantidad de bits transmitidos en el periodo T por encima de la tasa CIR. Si la red tiene capacidad libre suficiente admitirá la entrada de este tipo de tráfico en exceso (trama 3 de la Figura 14), marcándolo con DE activo.

- CBR (Velocidad de ráfaga comprometida). Es el valor de la velocidad de datos máxima que el proveedor de la red esta de acuerdo en transferir bajo condiciones normales.

- EBR (Velocidad de ráfaga en exceso). Es la velocidad de datos máxima por encima de la CBR que la red intentara mantener. A los datos de EBR se les pone automáticamente la etiqueta DE.

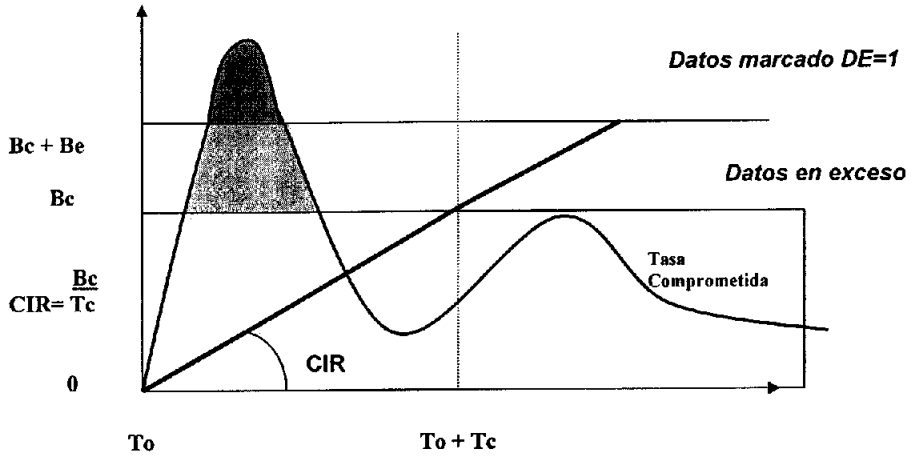


Figura 14. "Parámetros de Tráfico".

2.5 Foro Frame Relay

El foro Frame Relay se formó en enero de 1991, con miembros principalmente de proveedores de equipo para coordinar los desarrollos, acelerar el proceso de elaboración de estándares y efectuar la cooperación sobre trabajos y conformación de pruebas.

El foro Frame Relay es una organización de normalización iniciada por el grupo de los cuatro:

1. - DEC (Digital Equipment Corporation).
2. - Northem Telecom.
3.- Cisco.
4.- Stratacom.

Este foro generó dos interfaces basándose en los estándares que en ese momento estaba desarrollando la ANSI Frame Relay, los estándares que definió el foro Frame Relay fueron:

- Interfaz Uni (User to Network Interface). Este protocolo le permite a los usuarios acceder a una red Frame Relay pública o privada y establecer una trayectoria de comunicaciones hacia otro usuario dentro de la red.

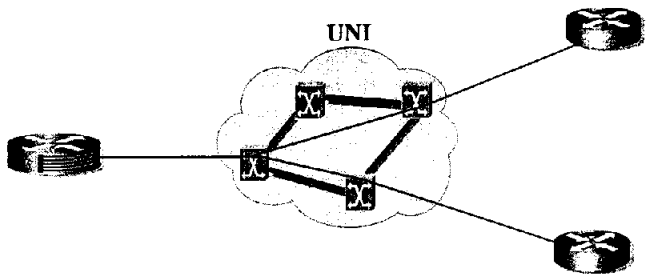


Figura 15. "Conexión usuario a red".

- Interfaz NNI (Network to Network Interface). La interfase de red a red en FR está diseñada para proporcionar una interfaz eficiente entre redes FR y permitir que los usuarios de dichas redes se puedan comunicar entre ellos.

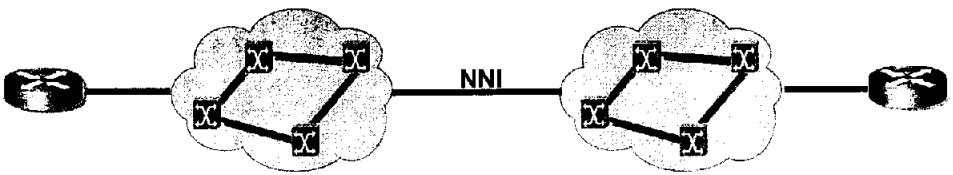


Figura 16. "Conexiones de red a red".

2.6 Ventajas que ofrece una red Frame Relay

Dentro de las principales ventajas que proporciona una red Frame Relay, se encuentran las siguientes:

- Arquitectura Abierta: debido a que existen una gran variedad de proveedores de equipo Frame Relay, se han generado estándares que han sido implantados a nivel mundial, lo cual asegura interoperabilidad entre diferentes equipos. (Frad´s (Motorota), Routers (Cisco, Juniper, Huawei, 3Comm).

- Encabezado reducido: debido a que el tamaño de encabezado de la trama es pequeño, le permite utilizar mejor el ancho de banda para el envío de la información.
- Escalabilidad y Confiabilidad: la red Frame Relay se basa en circuitos virtuales (permanentes/PVC y conmutados /SVC), los cuales pueden establecer una topología de malla o punto a punto.
- Interoperabilidad: Frame Relay pueden Transportar la mayoría de los protocolos tradicionales como X.25, SNA, HDLC, SDLC, tráfico de voz y puede permitir la conexión a redes TCP/IP y ATM.

2.7 Modelo de red Frame Relay

En las siguientes gráficas se puede ver el modelo Frame Relay como se vería en la práctica, tanto a nivel usuario como administrador.

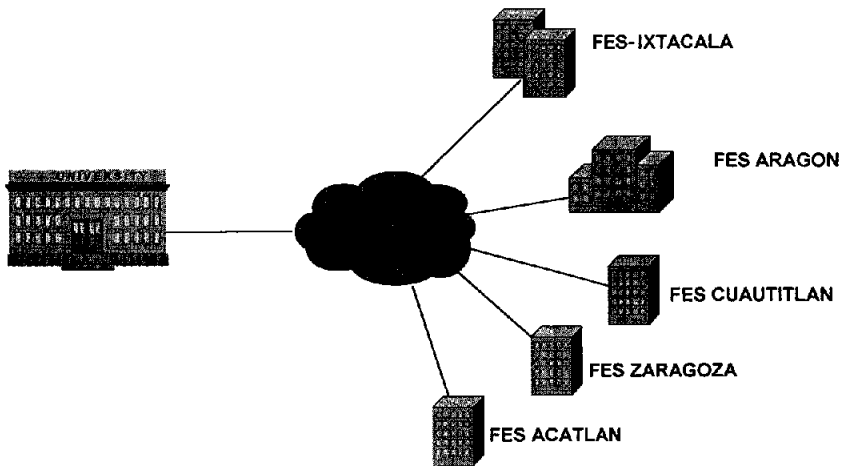


Figura 17. "Visión Externa (Usuario)".

En la figura 17. Se muestra la forma en la que el usuario final observa el entorno de red, en donde simplemente este hace uso de los servicios de esta, sin tomarle importancia en como se lleva a cabo la comunicación entre los distintos puntos de la organización, indicando por lo tanto que tiene un nulo conocimiento de la operación de esta.

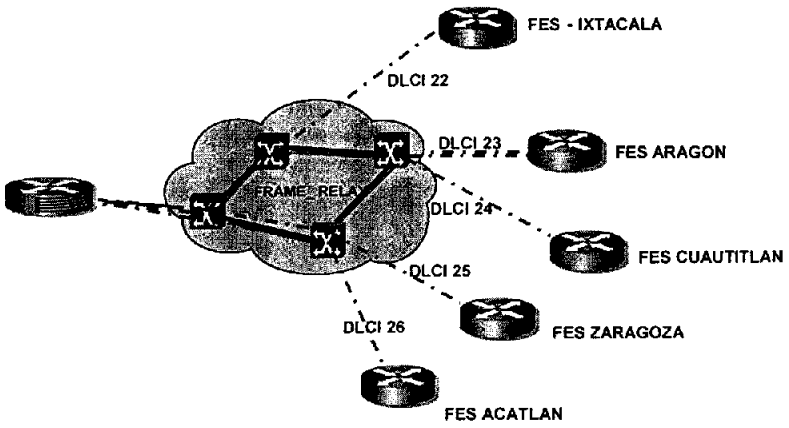


Figura 18. "Visión Interna (Administrador)".

En la figura 18. Muestra la forma en la que el administrador observa la red de la organización, nos referimos con esto a las personas que se encargan de administrar y mantener la operación de la red, este tipo de personas tienen conocimientos detallados para poder solucionar los problemas que se puedan presentar en la red por lo que ellos se encargan de activar, desactivar nodos de la red y configurar o modificar el modo de operación de esta según convenga a la organización.

Cuando se trabaja con la tecnología Frame Relay se asegura la interoperabilidad entre diferentes equipos y protocolos pero para poder crear la conexión de un punto hacia otro es necesario de mecanismos lógicos y físicos "hardware" dedicados al envió y reenvío de paquetes por lo que esto representa mayores gastos, sin embargo, al utilizar una red privada virtual el enlace se puede hacer únicamente a través de mecanismos lógicos por lo que disminuye el costo considerablemente. Esta es la principal característica para implementar un modelo de red privada virtual utilizando el protocolo IPsec el cual se trata a continuación.

3.1 Introducción IPsec

IPSec es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP. Es un protocolo de seguridad de la capa de red que proporciona servicios de encriptación con flexibilidad para soportar combinaciones de autenticación (la información enviada es realmente de quien dice ser), integridad (seguridad de que cualquier alteración de la información será detectada), control de acceso y confidencialidad (la información enviada no será vista por otras personas). Actualmente IPSec es considerado el mejor protocolo de seguridad. Fue creado por el Grupo de Seguridad de la IETF y (por lo tanto aportado en sus estándares) desarrolló mecanismos para proteger al protocolo IP al cual se denomina IP Security Protocol (IPSEC).

Otra característica Importante de IPSec es su carácter de estándar abierto. Entre los beneficios que aporta IPSec, cabe señalar que:

- Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.
- Facilita el comercio electrónico de negocio a negocio al proporcionar una infraestructura segura sobre la que realizar transacciones usando cualquier aplicación, como por ejemplo las extranets.
- Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el costo de líneas dedicadas.
- Ofrece al teletrabajador el mismo nivel de confidencialidad que dispondría en la red local de su empresa, siendo innecesaria la limitación de acceso a la información sensible por problemas de privacidad en tránsito.

3.2 RPV´S en IPsec

Las Redes Privadas Virtuales responden a una necesitad actual y creciente en el mundo de las comunicaciones. Las Redes Privadas Virtuales utilizan Internet como un mecanismo de trasporte mientras se mantiene la seguridad de los datos en la RPV.

La principal motivación para la implantación de las RPV´S es la financiera: los enlaces dedicados son demasiados caros, principalmente cuando las distancias son largas. Por otro lado existe Internet, que por ser una red de alcance mundial, tiene puntos de presencia diseminados por el mundo. Las conexiones con Internet tienen un costo mas bajo que los enlaces dedicados, principalmente cuando las distancias son largas.

El servicio RPV, permite la conexión segura de diferentes delegaciones con la central, permitiendo la transmisión de datos entre las diferentes delegaciones separadas geográficamente de la sede central, y facilita la salida a Internet de todas

las delegaciones si el cliente lo desea. Aprovecha los costes de ADSL para mantener una conexión las 24 horas con una tarifa plana entre las delegaciones y la central. También se puede utilizar la misma conexión ADSL para que todas las delegaciones y la central puedan salir a Internet. Permite la creación de Redes Privadas Virtuales, reduciendo costes y aumentando el rendimiento. El tráfico Corporativo y de Gestión se protege en su tránsito por la Red IP mediante IPSec. Para el tráfico corporativo IPSec en modo transporte como protocolo de tunneling. La salida a Internet de las delegaciones se puede realizar a través de su propia conexión a la red IP con la dirección pública del servicio ADSL.

Actualmente multitud de empresas ofrecen servicios de RPV a través del actual ADSL. Lo que se busca con esto es conseguir una seguridad y para conseguir esta seguridad, usando los estándares IETF, se necesitan soluciones RPV basadas en el protocolo de seguridad a nivel de red IPSec y protocolos de intercambio de claves de alto nivel, como IKE. Pero desde el punto de vista del manejo de claves, esta solución es muy estática, ya que todas las entidades involucradas en la comunicación deben tener previamente almacenada toda la información privada (claves privadas o compartidas) que protege la transmisión de datos. Esto es un grave problema si queremos tener un modelo abierto donde dos entidades quieran comunicarse de un modo seguro, flexible y de bajo costo, y sin conocimiento previo de la otra parte (solamente teniendo en común una jerarquía de confianza). Para solucionar este problema se ha diseñado un marco seguro basado en Redes Privadas Virtuales, infraestructuras de clave pública y el uso de tarjetas inteligentes, que se ha llamado Redes Privadas Virtuales dinámicas.

3.3 Arquitectura y diseño

La arquitectura de IPSec permite definir la precisión con la que el usuario puede especificar su política de seguridad, pudiendo determinar que cierto tráfico sea identificado para recibir el nivel de protección deseado.

IPSec está diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Por defecto hay ciertos algoritmos "estándar" que deberán soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones Hash. El usuario puede determinar el uso de otro tipo de algoritmos, como algoritmos de cifrado de clave simétrica IDEA, Blowfish o el más reciente AES, se consideren los más adecuados para un entorno determinado.

IPSec proporciona una base estable y duradera para proporcionar seguridad de capa de red. Soporta todos los algoritmos criptográficos que se utilizan hoy en día y también puede ajustarse a algoritmos nuevos más potentes que vayan surgiendo.

El protocolo IPSec cubre las siguientes cuestiones de seguridad principales:

Autenticación de origen de datos. Verifica que cada datagrama ha sido originado por el remitente indicado.

Integridad de datos. Verifica que el contenido de un datagrama no se ha cambiado por el camino, ni deliberadamente ni debido a errores aleatorios.

Confidencialidad de datos. Oculta el contenido de un mensaje, normalmente mediante cifrado.

Protección de reproducción. Impide que un agresor pueda interceptar un datagrama y reproducirlo posteriormente.

Gestión automatizada de claves criptográficas y asociaciones de seguridad. Permite utilizar la política VPN en toda la red con poca o ninguna configuración manual.

VPN utiliza dos protocolos IPSec para proteger los datos mientras fluyen a través de la VPN: AH (cabecera de autenticación) y EPS (carga útil de seguridad encapsulada). La otra parte de la habilitación de IPSec es el protocolo IKE (intercambio de claves de Internet) o la gestión de claves. Mientras que IPSec cifra los datos, IKE soporta la negociación automatizada de SA (asociaciones de seguridad) y la generación y la renovación automatizadas de claves criptográficas.

Los principales protocolos IPSec se listan a continuación

- Protocolo de autentificación Authentication Header (AH).
- Protocolo de encriptación Encapsulating Security Payload (ESP). Ambos son protocolos de seguridad de tráfico.
- Protocolo y procedimiento para el manejo de llaves encriptadas. Internet Key Exchange (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

Figura 19. Encabezado IPsec.

3.3.1 Protocolo AH (Authentication Header)

Este protocolo garantiza la integridad y autenticación de los datagramas IP. Proporciona un medio al receptor de los paquetes IP para autenticar el origen de los

datos y para verificar que dichos datos no han sido alterados en tránsito. Sin embargo, no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros.

Consiste en una cabecera de autenticación que se inserta entre la cabecera IP estándar (tanto IPv4 como IPv6) y los datos transportados, que pueden ser un mensaje TCP, UDP o ICMP, o incluso un datagrama IP completo.

3.3.2 Protocolo ESP (Encapsulating Security Payload)

Su función primordial es proporcionar confidencialidad, para ello especifica el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH.

El formato de la cabecera es más complejo. Consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo IP (por ejemplo, TCP, UDP o ICMP, o incluso un paquete IP completo).

Aquí se muestra la estructura de un datagrama ESP, en la que se observa cómo el contenido o carga útil viaja cifrado. Por encima de esta cabecera iría la cabecera IP. La distribución de claves de forma segura y el acuerdo en el algoritmo de cifrado o de Hash y como en el resto de parámetros comunes que utilizan es un requisito escencial tanto para el funcionamiento de ESP como de AH. La principal diferencia entre la autenticación provista por AH y ESP tiene que ver con la cobertura. AH autentifica los campos de la cabecera IP (en concreto los que no son variables) y ESP no autentifica la cabecera IP. No obstante, en el caso de que se esté utilizando el modo túnel, ESP protege los datos IP, debido a que estos están encapsulados en el campo datos del datagrama y por tanto se codifican. ESP encripta los datos y por tanto son secretos, les provee de confidencialidad.

3.4 Asociaciones de seguridad (SA: Security Association)

Una SA es una clase de conexión que permite establecer los servicios de seguridad del tráfico. En cada SA los servicios de seguridad pueden hacer uso de AH o ESP pero no de ambos. Para utilizar los dos se deberá establecer dos SA. Una SA es particularmente identificada por tres valores:

- SPI (Index Parameter Security).
- Dirección IP.
- Identificador de protocolo de seguridad (AH o ESP).

Se pueden definir dos tipos de SA:

1. Modo transporte: Se trata de una SA entre dos host.
2. Modo túnel: Se trata de una SA aplicada a un túnel IP.

3.4.1 Modo Transporte

Es el que usa un anfitrión que genera los paquetes. En modo transporte, las cabeceras de seguridad se añaden antes que las cabeceras de la capa de transporte (TCP, UDP), y también de que la cabecera IP sea añadida al paquete. En otras palabras, un AH añadido al paquete cubrirá el resumen criptográfico de la cabecera TCP y algunos campos de la cabecera IP extremo-a extremo, y una cabecera ESP cubrirá el cifrado de la cabecera TCP y los datos, pero no la cabecera IP extremo-a-extremo.

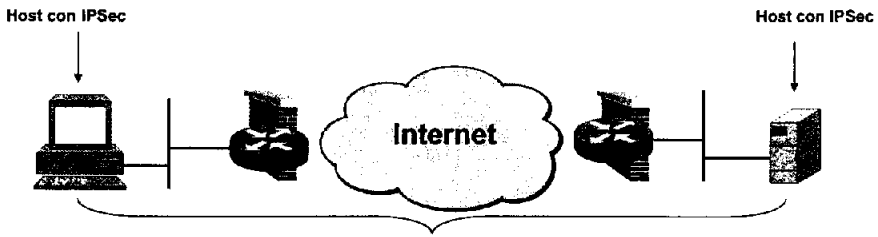


Figura 20. SA "Modo Transporte".

3.4.2 Modo Túnel

En este modo existen dos encabezados IP, uno que es el externo: que especifica los datos para llegar al destino del túnel y otro interno a éste que detalla el destino final. El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos de modo que funcionalmente aparezcan conectados.

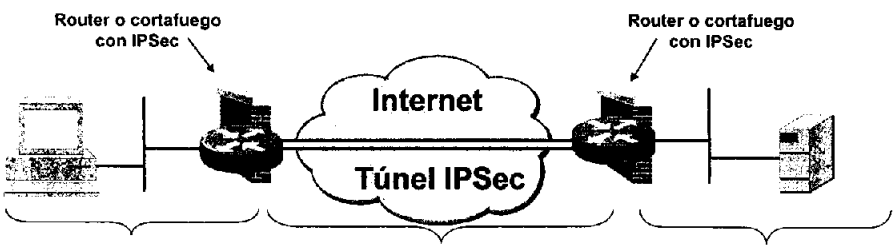


Figura 21. SA "Modo Túnel".

El modo Túnel se usa cuando la cabecera IP extremo-a-extremo ya ha sido adjuntada al paquete, y uno de los extremos de la conexión segura es solamente una pasarela. En este modo, las cabeceras AH y ESP se usan para cubrir todo el paquete, incluida la cabecera extremo-a-extremo, y se añade una nueva cabecera IP al paquete que cubre sólo el salto al otro extremo de la conexión segura (aunque eso puedan ser varios saltos de distancia).

3.5 Combinaciones de Asociaciones de Seguridad

Un host debe soportar ambos modos, un Gateway de seguridad sólo debe soportar modo túnel. Los diferentes SA pueden iniciarse y finalizar en los mismos puntos o no y se pueden combinar de dos formas:

3.5.1 Transporte adyacente

Se trata de aplicar más de un protocolo de seguridad a un mismo datagrama sin invocar un modo túnel, aprovechando la combinación de AH y ESP.

Figura 22. "Transporte Adyacente".

3.5.2 Túnel iterado

En este caso son también varias SA pero implementadas a través de modo túnel, y se puede llevar a cabo a través de tres formas:

1. Host, Host Host, Host: Ambos extremos de las SA son los mismos. Cada túnel podría emplear AH o ESP.

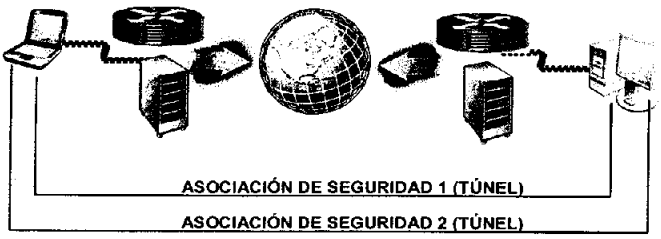


Figura 23. "Túnel Iterado Host, Host, Host, Host".

2. Host, Host Gateway, Host: Un extremo de las SA es el mismo y el otro no.

Figura 24. "Túnel Iterado Host, Host, Gateway, Host".

3. Y Cualquiera de las propuestas anteriores puede ser combinada con otras, generando empaquetados de SA mixtos.

3.6 Casos de Combinaciones

Hay cuatro casos básicos de estas combinaciones que deben ser soportados por todo Host o Gateway de seguridad que implemente IPSec, estos son:

1. Seguridad de extremo-a-extremo entre dos host a través de Internet,(Host1, Host2).

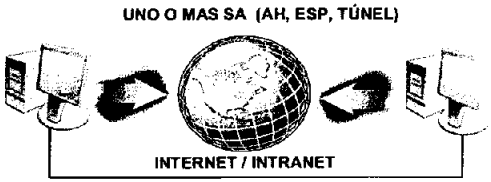


Figura 25. "Seguridad Extremo a Extremo".

2. Soporte con simple RPV.

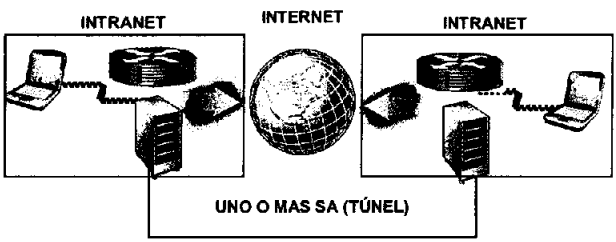


Figura 26. "Soporte con RPV".

3. Combinación de las dos anteriores.

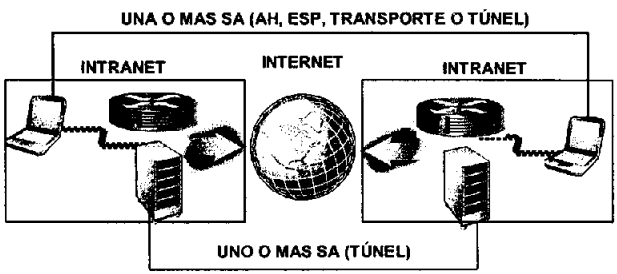


Figura 27. "Combinación".

4. Host remoto a través de Internet: Sólo el modo túnel puede ser empleado entre el host 1 y el Gateway de seguridad, y entre los host cualquiera de ellos.

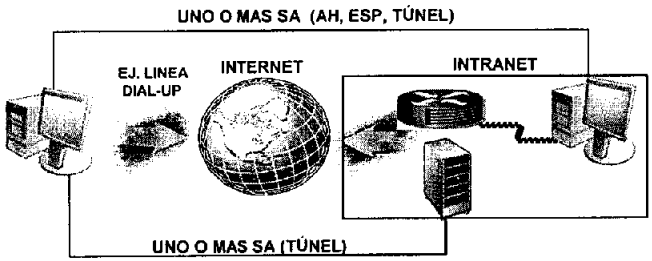


Figura 28. "Host Remoto".

3.7 Protocolo IKE (Internet Key Exchange)

Es un protocolo de control que se encarga de poner en contacto y negociar los algoritmos, claves y demás elementos para la comunicación segura con IPSec entre 2 nodos.

El IETF ha definido el protocolo IKE para realizar tanto esta función de gestión automática de claves como el establecimiento de las SA'S correspondientes. La utilidad del protocolo IKE no se limita a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos, como, por ejemplo, OSPF o RIPv2. IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios: ISAKMP y Oakley. SAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

3.8 Negociación IKE

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec. Dicha negociación se lleva a cabo en dos fases:

- Establecimiento de un canal seguro y autentificado: Esta fase es común a cualquier aplicación. Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se

derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de los nodos para ello es necesario un paso adicional de autenticación.

- Métodos de autenticación: el primer método de autenticación se basa en el conocimiento de un secreto compartido que es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones Hash cada extremo demuestra al otro que conoce el secreto sin revelar su valor, así los dos se autentican mutuamente. Debe configurarse un secreto distinto para cada par de nodos, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de nodos.

- El segundo método es el de certificados digitales. Está indicado para la interconexión de muchos nodos. IPSec está previsto del uso de un método de autenticación que se basa en utilizar certificados digitales X509v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere de la aparición de un elemento más en la arquitectura IPSec, la PKI (Infraestructura de Clave Pública).

- Negociación de los parámetros de seguridad específicos de IPSec a través del Canal seguro: durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

3.9 Seguridad en las RPV´S

Un punto fundamental de seguridad en las RPV´S es el particionamiento de las redes públicas o de uso compartido para implementar las RPV'S que son disjuntas. Esto se logra mediante el uso de túneles que no son ni más ni menos que técnicas de encapsulado del tráfico. Las técnicas que se utilizan son: GRE, que permite que cualquier protocolo sea transportado entre dos puntos de la red encapsulado en otro protocolo, típicamente IP; L2TP que permite el armado de túneles para las sesiones PPP remotas, y por último IPSec para la generación de túneles con autenticación y encriptado de datos.

La seguridad engloba la confidencialidad de la comunicación y la integridad de los datos, que para muchas compañías y entornos de negocio puede ser un requisito mucho más crítico que la confidencialidad. Esta integridad es proporcionada por IPSec como servicio añadido al cifrado de datos o como servicio independiente.

3.10 Aspectos básicos de túneles

Trabajar en un sistema de túnel es un método de utilizar una infraestructura de la red para transferir datos de una red sobre otra; los datos que serán transferidos (o carga útil) pueden ser las tramas (o paquetes) de otro protocolo.

En lugar de enviar una trama a medida que es producida por el nodo promotor, el protocolo de túnel la encapsula en un encabezado adicional. Éste proporciona información de entubamiento de manera que la carga útil encapsulada pueda viajar a través de la red intermedia.

Con esto, se pueden enrutar los paquetes encapsulados entre los puntos finales del túnel sobre la red (la trayectoria lógica a través de la que viajan los paquetes encapsulados en la red se denomina túnel). Cuando las tramas encapsuladas llegan a su destino sobre la red se desencapsulan y se envían a su destino final; nótese que este sistema de túnel incluye todo este proceso (encapsulamiento, transmisión y desencapsulamiento de paquetes).

Existen muchos otros ejemplos de túneles que pueden realizarse sobre intranets corporativos. Y aunque la Red de redes (Internet) proporciona una de las intranets más penetrantes y económicas, se puede reemplazar por cualquier otra intranet pública o privada que actúe como de tránsito.

3.11 Protocolos de túneles

Para que se establezca un túnel, tanto el cliente de éste como el servidor deberán utilizar el mismo protocolo de túnel.

La tecnología de túnel se puede basar en el protocolo de túnel de Nivel 2 o de Nivel 3 (estos niveles corresponden al Modelo de referencia de interconexión de sistemas abiertos OSI).

Los protocolos de Nivel 2 corresponden al Nivel de Enlace de datos, y utilizan tramas como su unidad de intercambio. PPTP y L2TP y el envio de Nivel 2 (L2F) son protocolos de túnel de Nivel 2, ambos encapsulan la carga útil en una trama de Protocolo de punto a punto (PPP) que se enviará a través de la red.
Los protocolos de Nivel 3 corresponden al nivel de la red y utilizan paquetes. IP sobre IP y el modo de túnel de seguridad IP (IPSec) son ejemplos de los protocolos

de túnel de Nivel 3, éstos encapsulan los paquetes IP en un encabezado adicional antes de enviarlos a través de una red IP.

3.11.1 Protocolo de túnel de punto a punto (PPTP)

Permite que se encripte el tráfico IP, IPX o NetBEUI, y luego se encapsule en un encabezado IP para enviarse a través de una red corporativa IP o una red pública IP, como Internet.

PPP se diseñó para enviar datos a través de conexiones de marcación o de punto a punto dedicadas. Encapsula paquetes de IP, IPX y NetBEUI dentro de las tramas del PPP, y luego transmite los paquetes encapsulados del PPP a través de un enlace punto a punto. Es utilizado entre un cliente de marcación y un NAS.

Existen cuatro fases distintivas de negociación en una sesión de marcación del PPP, cada una de las cuales debe completarse de manera exitosa antes de que la conexión del PPP esté lista para transferir los datos del usuario.

Fase 1: Establecer el enlace del PPP

PPP utiliza el Protocolo de control de enlace (LCP) para establecer, mantener y concluir la conexión física. Durante la fase LCP inicial, se seleccionan las opciones básicas de comunicación. Nótese que durante la fase de establecimiento de enlace (Fase 1), se seleccionan los protocolos de Autenticación, pero no se implementan efectivamente hasta la fase de Autenticación de conexión (Fase 2). De manera similar, durante el LCP se toma una decisión respecto a que si dos iguales negociarán el uso de compresión y/o encriptación. Durante la Fase 4 ocurre la elección real de algoritmos de compresión/encriptación y los otros detalles.

Fase 2: Autenticar al usuario

En la segunda fase, la PC cliente presenta las credenciales del usuario al servidor de acceso remoto. Por su parte, un esquema seguro de Autenticación proporciona protección contra ataques de reproducción y personificación de clientes remotos. (Un ataque de reproducción ocurre cuando un tercero monitoriza una conexión exitosa y utiliza paquetes capturados para reproducir la respuesta del cliente remoto, de manera que pueda lograr una conexión autenticada.

La personificación del cliente remoto ocurre cuando un tercero se apropia de una conexión autenticada.

La gran parte de la implementaciones del PPP proporcionan métodos limitados de Autenticación, típicamente el Protocolo de autenticación de contraseña (PAP), el

Protocolo de autenticación de saludo Challenge (CHAP) Y Microsoft Challenge Handshake Authentication Protocol (MSCHAP).

Protocolo de autenticación de contraseña (PAP). El PAP es un esquema simple y claro de autenticación de texto: el NAS solicita al usuario el nombre y la contraseña y el PAP le contesta el texto claro (no encriptado).

Obviamente, este esquema de autenticación no es seguro, ya que un tercero podría capturar el nombre y la contraseña para tener seña del usuario y utilizarlo en un acceso subsecuente al NAS y todos los recursos que proporciona el mismo cuando se ha escrito la contraseña del usuario, PAP no proporciona protección contra ataques de reproducción o personificación de cliente remoto.

Protocolo de autenticación de saludo Challenge (CHAP). El CHAP es un mecanismo encriptado que evita la transmisión de contraseñas reales en la conexión. El NAS envía un Challenge, que consiste de una identificación de sesión y una extensión arbitraria al cliente remoto. Por su parte, el cliente remoto deberá utilizar el algoritmo de control unidireccional MD5 para devolver el nombre del usuario y una encriptación del challenge, la identificación de la sesión y la contraseña del cliente.

El CHAP es una mejora sobre el PAP en cuanto a que no se envía la contraseña de texto transparente sobre el enlace. En su lugar, se utiliza la contraseña a fin de crear una verificación encriptada del challenge original. El servidor conoce la contraseña del texto transparente del cliente y, por tanto, puede duplicar la operación y comparar el resultado con la contraseña enviada en la respuesta del cliente.

El CHAP protege contra ataques de reproducción al utilizar una extensión challenge arbitraria para cada intento de autenticación. Asimismo, protege contra la personificación de un cliente remoto al enviar de manera impredecible challenges repetidos al cliente remoto a todo lo largo de la duración de la conexión.

Microsoft ChallengeHandshake Aut 1 identication Protocol (MSCHAP). Es un mecanismo de autenticación encriptado muy similar al CHAP. Al igual que en este último, el NAS envía un challenge, que consiste en una identificación de sesión y una extensión challenge arbitraria, al cliente remoto. El cliente remoto debe devolver el nombre del usuario y una verificación MD4 de la extensión challenge, el identificador de sesión y la contraseña MD4 verificada.

Este diseño, que manipula una verificación del MD4 de la contraseña, proporciona un nivel adicional de seguridad, debido a que permite que el servidor almacene las contraseñas verificadas en lugar de contraseñas con texto transparente.

MSCHAP también proporciona códigos adicionales de error, incluido un código de Contraseña ya expirado, así como mensajes adicionales cliente-servidor encriptado que permite a los usuarios cambiar sus contraseñas. En la implementación de Microsoft del MSCHAP, tanto el Cliente como el NAS, de manera independiente, una

llave inicial para encriptaciones posteriores de datos por el MPPE.
El último punto es muy importante, ya que explica la forma en que se requiere la autenticación del MSCHAP, a fin de permitir la encriptación de datos con base en MPPE.

Durante la fase 2 de la configuración del enlace del PPP, el NAS recopila los datos de autenticación y luego valida los datos contra su propia base de datos del usuario o contra un servidor central para la autenticación de base de datos, como el que mantiene un Controlador del dominio primario Windows NT, un servidor de Servicio remoto de usuario con marcación de autenticación (RA, DIUS).

FASE 3: Control de iteración del PPP

La implementación de Microsoft del PPP incluye una fase opcional de control de interacción. Esta fase utiliza el protocolo de control de iteración (CBCP) inmediatamente después de la fase de autenticación.

Si se configura para interacción, después de la autenticación, le desconectan tanto el cliente remoto como el NAS. En seguida, el NAS vuelve a llamar al cliente remoto en el número telefónico especificado, lo que proporciona un nivel adicional de seguridad a las redes de marcación.

El NAS permitirá conexiones a partir de los clientes remotos que físicamente residan sólo en números telefónicos específicos.

FASE 4: Invocar los protocolos a nivel de red

Cuando se hayan terminado las fases previas, PPP invoca los distintos Protocolos de control de red (NCP), que se seleccionaron durante la fase de establecimiento de enlace (Fase i) para configurar los protocolos que utiliza el cliente remoto. Por ejemplo, durante esta fase el Protocolo de control de IP (IPCP) puede asignar una dirección dinámica a un usuario de marcación.

En la implementación del PPP de Microsoft, el protocolo de control de compresión se utiliza para negociar tanto la compresión de datos (utilizando MPPC) como la encriptación de éstos (utilizando MPPE), por la simple razón de que ambos se implementan en la misma rutina.

Fase de transferencia de datos. Una vez que hayan concluido las cuatro fases de negociación, PPP empieza a transferir datos hacia y desde los dos iguales. Cada paquete de datos transmitidos se envuelve en un encabezado del PPP, que elimina el sistema receptor. Si se seleccionó la compresión de datos en la Fase 1 y se negoció en la Fase 4, los datos se comprimirán antes de la transmisión. Pero si se seleccionó y se negoció de manera similar la encriptación de datos, estos (comprimidos opcionalmente) se encriptarán antes de la transmisión.

3.11.2 Protocolo de túnel de Nivel 2 (L2TP)

Permite que se encripte el tráfico IP, IPX o NetBEUI, y luego se envíe sobre cualquier medio que dé soporte a la entrega de datagramas punto a punto, como IP, X.25, Frame Relay o ATM.

Es una combinación del PPTP y L2F. Sus diseñadores esperan que el L2TP represente las mejores funciones del PPTP y L2E, L2TP que es un protocolo de red que encápsula las tramas de PPP que viajan sobre redes IP, x.25, Frame Relay, o modo de transferencia ATM.

Cuando está configurado para utilizar al IP como su transporte de datagrama, L2TP se puede utilizar como un protocolo de túnel sobre Internet. También se Puede utilizar directamente sobre varios medios WAN (como Frame Relay), sin nivel de transporte IP.

El L2TP sobre las redes IP utiliza UDP y una serie de mensajes para el mantenimiento de túnel. Asimismo, emplea UDP para enviar tramas del PPP encapsuladas del L2TP como los datos enviados por el túnel; se pueden encriptar y/o comprimir las cargas útiles de las tramas PPP encapsuladas.

3.11.3 Modo de túnel de seguridad IP (IPSec)

Permite que se encripten las cargas útiles IP y luego se encapsulen en un encabezado IP para enviarse a través de una red corporativa IP o una red pública IP como Internet.

El modo de túnel IP tiene las siguientes funciones y limitaciones:

- Sólo da soporte a tráfico IP.
- Funciona en el fondo de la pila IP por tanto, las aplicaciones y los protocolos de niveles más altos heredan su comportamiento.
- Está controlado por una Política de seguridad (un conjunto de reglas que se cumplen a través de filtros). Esta política de seguridad establece los mecanismos de encriptación y de túnel disponible en orden de preferencia, así

- como los métodos de autenticación disponibles, también en orden de preferencia. Tan pronto como existe tráfico, ambos equipos realizan una autenticación mutua, y luego negocian los métodos de encriptación que se utilizarán. Posteriormente, se encripta todo el tráfico, y luego se envuelve en un encabezado de túnel.

Tanto el PPTP como L2TP utilizan el PPP para proporcionar una envoltura inicial de los datos, y luego incluir encabezados adicionales a fin de transportarlos a través de la red. Aunque ambos protocolos son muy similares, existen diferencias entre ellos: El PPTP requiere que la red sea de tipo IP, y el L2TP requiere sólo que los medios del túnel proporcionen una conectividad de punto a punto orientada a paquetes. Se puede utilizar L2TP sobre IP (utilizando UDP), circuitos virtuales permanentes (PVC), circuitos virtuales X25 (VC) o VC ATM.

El PPTP sólo puede soportar un túnel único entre puntos terminales, y el L2TP permite el uso de varios túneles entre puntos terminales. Con el L2TP es posible crear diferentes túneles para diferentes calidades de servicio.

L2TP proporciona la compresión de encabezados. Cuando se activa la compresión de encabezado, el L2TP opera sólo con 4 Bytes adicionales, comparado con los 6 Bytes para el PPTP.

L2TP proporciona la autenticación de túnel, no así el PPTP. Sin embargo, cuando se utiliza cualquiera de los protocolos sobre IPSec, se proporciona la autenticación de túnel por el IPSec, de manera que no sea necesaria la autenticación del túnel Nivel 2.

3.12 Funcionamiento de los túneles

Para las tecnologías de túnel de Nivel 2 como PPTP y L2TP, un túnel es similar a una sesión; los dos puntos finales deben estar de acuerdo respecto al túnel, y negociar las variables de la configuración, como asignación de dirección o los parámetros de encriptación o de compresión.
En la mayor parte de los casos, los datos que se transfieren a través del túnel se envían utilizando protocolos basados en datagramas, se utiliza un protocolo para mantenimiento del túnel como el mecanismo para administrar al mismo.
Por lo general, las tecnologías del túnel de Nivel 3 suponen que se han manejado fuera de banda todos los temas relacionados con la configuración, normalmente a través de procesos manuales, sin embargo, quizá no exista una fase de mantenimiento de túnel. Para los protocolos de Nivel 2 (PPTP y L2TP) se debe crear, mantener y luego concluir un túnel.
Cuando se establece el túnel, es posible enviar los datos a través del mismo. El cliente o el servidor utilizan un protocolo de transferencia de datos del túnel a fin de preparar los datos para su transferencia.

Por ejemplo, cuando el cliente del túnel envía una carga útil al servidor, primero adjunta un encabezado de protocolo de transferencia de datos de túnel a la carga útil. Luego, el cliente envía la carga útil encapsulada resultante a través de la red, la

que lo enruta al servidor del túnel. Este último acepta los paquetes, elimina el encabezado del protocolo de transferencia de datos del túnel y envía la carga útil a la red objetivo. La información que se envía entre el servidor del túnel y el cliente del túnel se comporta de manera similar.

3.12.1 Los protocolos y los requerimientos básicos del túnel

Puesto que se basan en protocolos PPP bien definidos, los protocolos de Nivel 2 (como PPTP v L2TP) heredan un conjunto de funciones útiles, como se señala más adelante, estas funciones y sus contrapartes de Nivel 3 cubren los requerimientos básicos de la RPV

Autenticación de usuario. Los protocolos de túnel Nivel 2 heredan los esquemas de autenticación del usuario de PPP.

Muchos de los esquemas de túnel de Nivel 3 suponen que los puntos finales han sido bien conocidos (y autenticados) antes de que se estableciera el túnel. Una excepción es la negociación IPSec ISAKMP que proporciona una autenticación mutua de los puntos finales del túnel.

Nótese que la mayor parte de las implementaciones IPSec dan soporte sólo a certificados basados en equipo, más que en certificados de usuarios; como resultado, cualquier usuario con acceso a uno de los equipos de punto final puede utilizar el túnel. Se puede eliminar esta debilidad potencial de seguridad cuando se conjunta el IPSec con un protocolo de Nivel 2, como el L2TP.

3.12.1.1 Soporte de tarjeta de señales

Al utilizar el Protocolo de autenticación ampliable (EAP), los protocolos de túnel Nivel 2 pueden ofrecer soporte a una amplia variedad de métodos de autenticación, incluidas contraseñas de una sola vez, calculadores criptográficos y tarjetas inteligentes. Los protocolos de túnel Nivel 3 pueden utilizar métodos similares, por ejemplo IPSec define la Autenticación de los certificados de llaves públicas en su negociación ISAKMP/Oakley.

3.12.1.2 Asignación de dirección dinámica

El túnel de Nivel 2 da soporte a la asignación dinámica de direcciones de clientes basadas en un mecanismo de negociación de protocolos de control de la red en general los esquemas del túnel de nivel 3 suponen que ya se ha asignado una dirección antes de la iniciación del túnel.

3.12.1.3 Compresión de datos

Los protocolos de túnel Nivel 2 proporcionan soporte a esquemas de compresión basados en PPP, por ejemplo las implementaciones de Microsoft tanto de PPTP como L2TP utilizan Microsoft Point to Point Compression (MPPC). La IETF está investigando mecanismos similares (como la compresión IP) para los protocolos de túnel Nivel 3.

3.12.1.4 Encriptación de datos

Los protocolos de túnel Nivel 2 dan soporte a mecanismos de encriptación de datos basados en PPP. Por su parte, la implementación de Microsoft de PPTP da soporte al uso opcional de Microsoft Point to Point Encription (MPPE), basado en el algoritmo RSA/RC4. Los protocolos de túnel Nivel 3 pueden utilizar métodos similares, por ejemplo IPSec define varios métodos de Encriptación opcional de datos que se negocian durante el intercambio ISAKMP/Oakley.

La implementación de Microsoft del protocolo L2TP utiliza la encriptación IPSec para proteger el flujo de datos del cliente al servidor del túnel.

3.12.1.5 Administración de llaves

MPPE, un protocolo de Nivel 2, se basa en las claves iniciales generadas durante la Autenticación del usuario y luego las renueva en forma periódica. IPSec negocia explícitamente una llave común durante el intercambio ISAKMP y también las renueva de manera periódica.

3.12.1.6 Soporte de protocolo múltiple

El sistema de túnel de Nivel 2 da soporte a protocolos múltiples de carga útil, lo que facilita a los clientes de túnel tener acceso a sus redes corporativas utilizando IP, IPX, NetBEUI, etc.

En contraste, los protocolos de túnel Nivel 3, como el modo de túnel IPSec, por lo común dan soporte sólo a redes objetivo que utilizan el protocolo IP.

3.13 Ventajas de las RPV´S

Dentro de las numerosas ventajas que proporciona este protocolo la más destacable sería que permite construir una red segura, sobre redes públicas, eliminando la gestión y el coste de las líneas dedicadas, ofreciendo al trabajador que se encuentra fuera de la sede de la empresa la misma seguridad que si trabajase sobre una red de área local de una empresa. Este protocolo es independiente de la tecnología física empleada y es transparente a la aplicación, esto se debe a que se añade a los protocolos de la capa IP.

Entre las ventajas de IPSec destacan que, se integra en la versión actual de IP (IP versión 4) y, lo que es todavía más importante, se incluye por defecto en IPv6.

- Integración de las comunicaciones de datos entre los nodos, dispersos geográficamente, funcionando como una única red.
- Información centralizada simplificando el proceso de actualización, al mismo tiempo que asegura que todos disponen de la misma versión.
- Control y planificación de los gastos gracias a la tarifa plana del servicio. Coste fijo por nodo independiente del tráfico cursado y la distancia entre los nodos.
- La incorporación de nuevos nodos se realiza de forma rápida y sencilla.
- IPSec crea el cable o túnel virtual a través de la red común sin tener que disponer de ningún dispositivo ni de ningún software complejo. Este avance ha permitido que una persona con un portátil o pc y una conexión a la red pudiera operar con total tranquilidad sin temer que su información altamente confidencial pueda ser vista o alterada.

3.13.1 Desventajas de las RPV´S

Las VPN han representado una magnífica solución para las empresas en cuanto a seguridad, confidencialidad de integridad de los datos, por esto se han vuelto tan importantes para las empresas, ya que reduce el costo de la transferencia de datos de un lugar a otro, un inconveniente importante es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no está bien definido pueden existir consecuencias serias como las siguientes:

- No se garantiza disponibilidad (NO Internet NO VPN).
- No se garantiza el caudal (red pública).
- Gestión de claves de acceso y autenticación delicada y laboriosa.
- La fiabilidad es menor que en una línea dedicada.
- Mayor carga en el cliente VPN (Encapsulación y cifrado).
- Mayor complejidad en la configuración del cliente (Proxy, servidor de correo,).
- Una VPN se considera segura, pero no hay que olvidar que la información sigue viajando por Internet (no seguro y expuestos a ataques).

Como se ha visto IPsec es un protocolo sencillo de configurar e implementar lo cual garantiza que los datos lleguen seguros a su destino tomando en cuenta que puede manejar distintos grados de encriptación que lo hacen un protocolo muy versátil en cuanto a la seguridad de la información es por eso que se toma como referencia para la elaboración de este trabajo el cual se basa en la implementación de una red privada virtual sobre un modelo superpuesto utilizando como base IPsec para lograr la comunicación entre entidades sin tener riesgo alguno utilizando como medio de transporte Internet.

IMPLEMENTACIÓN DE UNA RPV (RED PRIVADA VIRTUAL) SOBRE UN MODELO RPV - SUPERPUESTO

Como se ha estado tratando en los capítulos anteriores, el tema de la seguridad en una red toma un lugar importante en el desarrollo de ésta, pues de este punto depende el buen funcionamiento de todos los servicios que se brinden.

Hoy en día, la información se ha convertido en el elemento más importante en una organización, sobre todo para aquellas que poseen sucursales, clientes y socios comerciales distribuidos a lo largo de la ciudad e incluso a nivel internacional, los cuales necesitan tener acceso a las bases de datos y procesos en línea que tiene la organización.

Frecuentemente este tipo de organizaciones cuentan con conexiones dedicadas las cuales resultan muy costosas, sobre todo cuando se trata de grandes distancias, y esta situación resulta, en la mayoría de los casos, difícil de mantener.

En tal sentido, la tecnología de Red Privada Virtual surge como un medio para utilizar el canal público de Internet y así poder comunicar datos privados utilizando llamadas locales, proporcionando además seguridad a través de técnicas de encriptación y encapsulamiento.

4.1 ANÁLISIS DEL PROBLEMA

Se utilizara como escenario a una organización "X" la cual para poder tener una comunicación continua entre sus sucursales cuenta con conexiones Frame Relay hacia todos sus puntos distribuidos en las principales ciudades de la republica, teniendo de esta manera acceso a todos los recursos compartidos de la organización (impresoras, fax, www (internet), correo electrónico (mail), consulta y actualización de bases de datos, etc.) además de poder utilizar la red de voz IP con la que cuenta esta organización.

Así mismo esta organización cuenta con socios comerciales internacionales los cuales debido a la relación comercial que los une desean tener acceso a los mismos recursos de las sucursales de la organización (voz y datos).

4.1.1 SITUACIÓN ACTUAL

La forma en la que se comunica la organización con sus otras sedes es utilizando en el nodo central tres enlaces "punto a punto y multipunto" con un ancho de banda que oscila entre 2Mb y 512Kbps operando con una tecnología Frame Relay a nivel nacional. Esta organización también cuenta con 2 conexiones tipo E1 las cuales proporcionan el servicio de internet de toda la organización (mail, www).

En toda la organización se utiliza para la conexión de sus distintos nodos enrutadores "Cisco", los cuales cuentan con una interfaz serial la cual tiene conexión hacia el enlace WAN y una interfaz Fast Ethernet que crea la conexión hacia la red interna de la organización.

Para la parte de Internet se utiliza un equipo "Cisco 2620" el cual soporta todo el tráfico de Internet de la organización, este equipo cuenta con 2 enlaces tipo E1 en donde por uno de ellos se transporta el trafico hacia Internet (www y http) y por el otro hacia el correo electrónico (mail) quedando de esta manera balanceado el trafico por cada una de puertos.

Figura 29. Enrutador Cisco 2620.

Para la transmisión de datos el nodo central cuenta con un equipo "Cisco 3640" el cual cuenta con las siguientes características: un puerto Fast Ethernet con el cual se puede operar en la Red LAN a una velocidad de 100Mbps en modo full-Duplex, así mismo cuenta con 6 slots en donde solo se utilizan 2 para las tarjetas de conexión hacia el enlace WAN las cuales soportan 2 conexiones seriales de 2Mbps por cada una teniendo un total de 4 puertos seriales suficientes para las sucursales que se tienen.

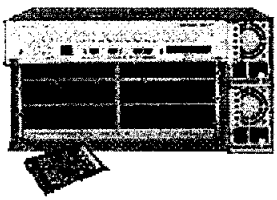


Figura 30. Enrutador Cisco 3640.

También se cuenta con un PBX IP el cual interactúa con un Server que opera con el Protocolo SIP sirviendo de Gateway para toda la Red otorgando el servicio de voz sobre IP.

Así mismo todas estas aplicaciones están interconectadas a un equipo switch "Cisco Catalyst 3500" el cual otorga el servicio de VLAN´s separando el trafico de voz, datos y video de la organización e interconexión hacia el equipo Firewall el cual protege a la red de los accesos maliciosos de Internet.

Para los nodos nacionales se cuenta con enrutadores "Cisco 1751" los cuales tienen solo un puerto hacia la WAN y hacia la parte LAN, siendo estos suficientes para poder soportar todas las aplicaciones "voz y datos" de cada sucursal.

Figura 31. Enrutador Cisco 1751.

En el nodo central se cuenta también con un equipo Firewall marca NetScreen JUIPER el cual protege a la red de intrusos que quieran dañar la integridad de la organización.

Figura 32. Firewall NetScreen-100A.

Todos estos sitios cuentan con teléfonos IP los cuales solo tiene que conectarse directamente a la red LAN de cada nodo logrando con esto comunicarse a través de la red sin costo alguno.

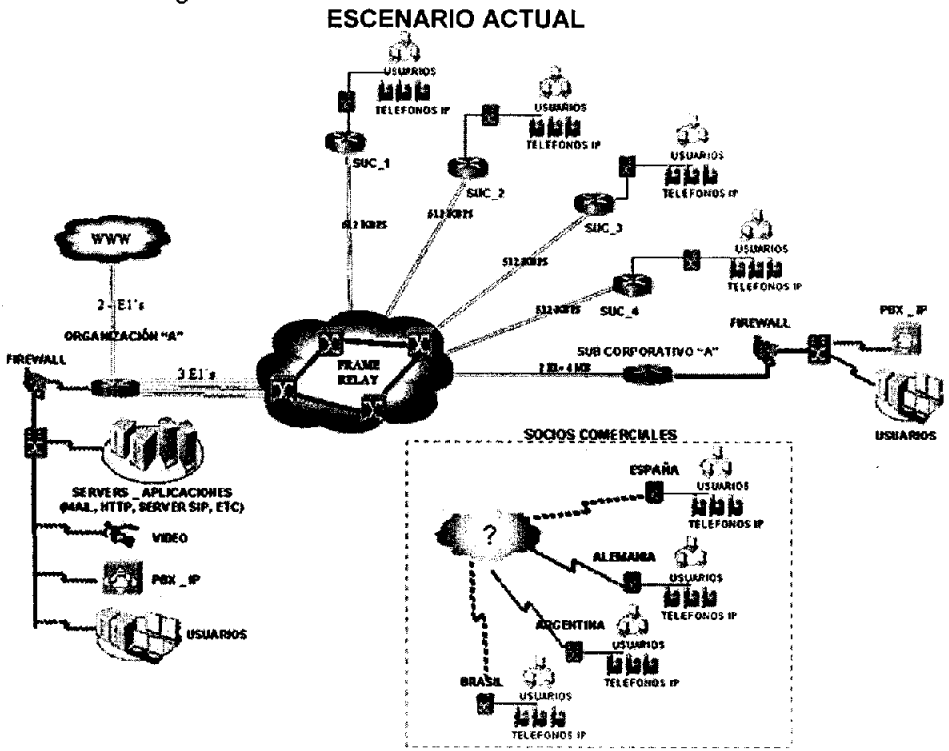


Figura 33. Red Frame Relay.

4.2 PLANEAMIENTO DEL PROBLEMA

El problema que se plantea en esta organización es que es necesario buscar la manera para poder interconectar a los socios internacionales al nodo que funge como central en la CD. De México, todo esto debido a que les resulta muy costoso el poder comunicarse e intercambiar información hacia el corporativo y entre sus sucursales

Como primera opción para poder lograr esta conectividad se pensó en contratar otro enlace con tecnología Frame Relay pero una de las limitantes fue su costo el cual se anexa en la siguiente tabla.

Gastos de Instalación: **FRAME RELAY PUERTO EXTENDIDO** **PAGO UNICO**

Sitios	Concepto	Precio	Desc. 1 Año	Desc. 3 Años	Desc. 5 Años
Corporativo México **AV12**	1 Puerto Frame Relay a 64 Kbps	$ 0.00	$ 0.00	$ 0.00	$ 0.00
	1 Data Enlace de 64 Kbps	$ 12,908.00	$ 12,908.00	$ 6,454.00	$ 0.00
Sucursal Guadalajara **AV12**	1 Puerto Frame Relay a 64 Kbps	$ 0.00	$ 0.00	$ 0.00	$ 0.00
	1 Data Enlace de 64 Kbps	$ 12,908.00	$ 12,908.00	$ 6,454.00	$ 0.00
Total		$ 25,816.00	$ 25,816.00	$ 12,908.00	$ 0.00

TOTAL GASTOS DE INSTALACION: Sin descuento $ 25,816.00
TOTAL GASTOS DE INSTALACION: Con descuento a 5 años **$ 0.00**
(incluye 2 sitios)

POLITICAS DE DESCUENTO: TELMEX - UNINET

- 100 % de descuento, en 5 años y 50% de descuento en 3 años para gastos de instalación. En los Lada enlaces

Renta Mensual: **FRAME RELAY PUERTO EXTENDIDO**

Sitios	Concepto	Precio
Corporativo México **AV12**	1 Puerto Frame Relay a 64 Kbps	$ 1,893.00
	1 Data Enlace de 64 Kbps	$ 907.00
Sucursal Guadalajara **AV12**	1 Puerto Frame Relay a 64 Kbps	$ 1,893.00
	1 Data Enlace de 64 Kbps	$ 907.00
	1 Circuito Virtual de 48 Kbps	$ 1,150.00
Total		$ 6,750.00

TOTAL RENTA: (incluye 2 sitios) $ 6,750.00

Tabla. 2 Costos de enlaces Frame Relay

Teniendo todos estos datos de por medio resulta muy difícil poder contratar este tipo de tecnología por lo que la segunda opción la cual es interconectar estos sitios por medio de una tecnología de redes privadas virtuales resulta mas atractivo cuando los sitios se encuentran fuera del país.

Para poder aplicar este tipo de tecnología solo es necesario tener un acceso a Internet en cada punta (nacional e internacional) y un equipo que proporcione la conectividad "Server (software), firewalls (hardware)" por lo que la comunicación seria de una manera más sencilla y menos costosa.

En la siguiente tabla se anexan los precios de las conexiones de Internet solo a nivel nacional debido a que en cada país varia el costo dependiendo del proveedor de servicios local.

TELMEX (INTERNET)

INFINITUM 128 –512	$ 599
INFINITUM 512 – 1280	$ 999
INFINITUM 2MBPS	$ 4599
COSTO EXTRA - IP FIJA	$ 1000

Tabla. 3 Costos de enlaces Internet

Se anexa también una tabla con los precios de algunos equipos firewalls basados en hardware.

Juniper NetScreen 204	$ 7,709
NetScreen – 100A	$ 6,500

Cisco Pix 506E 3DES/AES Firewall	$ 7,920

Tabla. 4 Costos Firewalls

Existen varias soluciones comerciales y no comerciales para poder conectar a estos sitios hacia su organización central siendo las siguientes las más importantes:

Soluciones comerciales.

- Por medio de Servidores dedicados utilizando WIN_2000 Server o WIN_2003_Server los cuales tienen el software necesario para poder crear túneles de RPV utilizando el protocolo IPSec.

- Por medio de Firewalls basados en Hardware del fabricante los cuales utilizan un S.O. propio usualmente en UNIX y que tienen una o más características especiales que los basados en Software.

Soluciones no comerciales

- FreeS/WAN es una implementación de IPSec en Linux , por eso el uso de IPSec cobra mayor relevancia a la hora de crear una VPN, ya que existen muchos otros sistemas operativos que tienen implementado IPSec, y además es sumamente seguro, esto permite que con Linux se puedan establecer túneles cifrados contra otras redes que tengan sistemas operativos diferentes.

En este caso se implemento la solución por medio de Firewall´s basados en hardware ya que el nodo central cuenta con este tipo de equipo solo seria necesario comprar estos equipos para los puntos internacionales.

4.2.1 CREACIÓN DE TÚNELES UTILIZANDO UN FIREWALL BASADO EN HARDWARE

La primer instancia que se debió tener en cuenta para el sitio que fungirá como servidor central de los túneles, fue que deberá tener una salida hacia internet por medio de una IP pública, tomando como base de que el direccionamiento privado no puede ser anunciado en la red pública de internet, por lo cual no puede ser rastreado desde otro punto que también se encuentre conectado a "Internet" lo cual provocaría que jamás se lograran conectar estos sitios.

Para los sitios remotos no existen problemas con el direccionamiento, ya que en ellos no habrá conexiones entrantes si es así también se tendría que requerir un direccionamiento público.

Para nuestro caso se cuenta con direccionamiento público por lo cual se procederá a la creación de los túneles que comunicarán a la organización con sus subsedes internacionales.

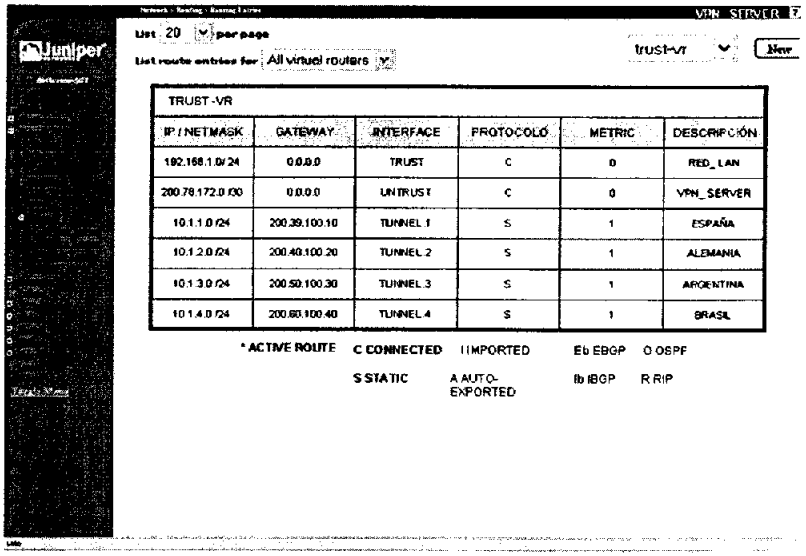
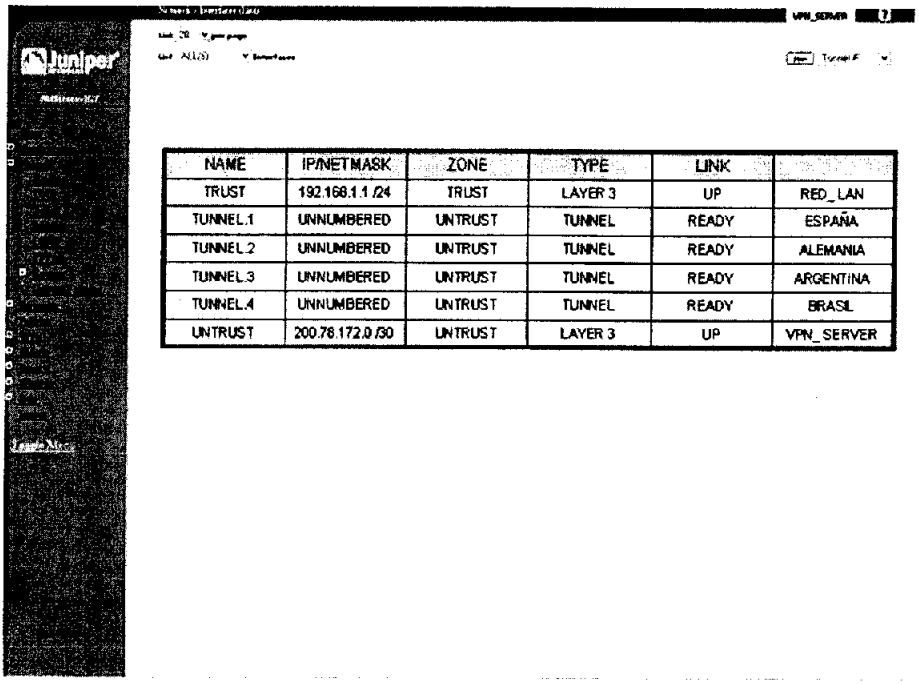


Figura 34. Conexiones Vía Túnel hacia los nodos Internacionales.

En la figura 34, se muestra la configuración del nodo central y sus conexiones hacia los distintos nodos internacionales utilizando los túneles encriptados con el protocolo IPsec, también se muestra el direccionamiento tanto para la parte LAN como para la parte WAN de cada nodo internacional de la organización, así como, el que funge como nodo central o concentrador .



NAME	IP/NETMASK	ZONE	TYPE	LINK	
TRUST	192.168.1.1 /24	TRUST	LAYER 3	UP	RED_LAN
TUNNEL.1	UNNUMBERED	UNTRUST	TUNNEL	READY	ESPAÑA
TUNNEL.2	UNNUMBERED	UNTRUST	TUNNEL	READY	ALEMANIA
TUNNEL.3	UNNUMBERED	UNTRUST	TUNNEL	READY	ARGENTINA
TUNNEL.4	UNNUMBERED	UNTRUST	TUNNEL	READY	BRASIL
UNTRUST	200.76.172.0 /30	UNTRUST	LAYER 3	UP	VPN_SERVER

Figura 35. Estado de los Túneles hacia nodo concentrador.

En la figura 35, se muestra el estado de cada túnel creado hacia los distintos puntos internacionales de la organización, en esta pantalla se puede observar si el túnel se encuentra activo o inactivo, si en dado caso el túnel se encontrara inactivo su estado cambiaría a *Standby* lo que significaría que esta en espera de recibir una conexión RPV entrante de Internet.

Después de que los túneles se hayan establecido y se encuentren en estado de *ready* (quiere decir que la comunicación hacia la organización se encuentra activa), por lo que se podrá hacer uso de todos los recursos a los que se haya otorgado su acceso, En este caso sería acceso a los Server´s de Base de datos y de telefonía IP, esto con el fin de lograr comunicarse entre los usuarios de la misma organización sin utilizar llamadas de larga distancia.

A continuación se muestra la forma más simple para entender cómo se realiza esta conexión de túneles por medio de un Firewall.

1- El sitio remoto que se encuentra conectado a Internet ejecuta su conector RPV (conectoid) el cual en nuestro caso se realiza por medio de un Firewall el cual envía la solicitud de conexión hacia el nodo central.

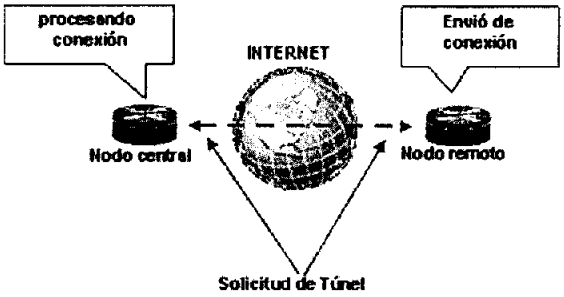


Figura 36. Solicitud de conexión.

2- El Firewall central empieza a procesar la conexión remota validando en sus políticas que tipo de acceso requiere conectarse a él (conexión RPV).

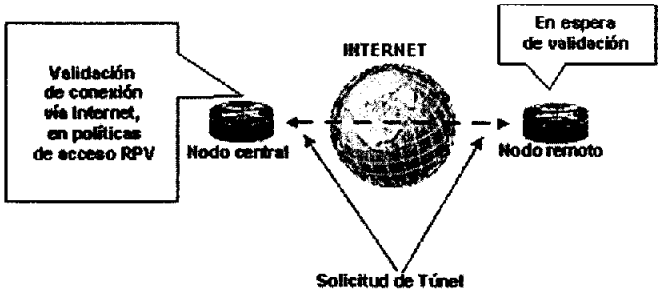


Figura 37. Validación de políticas.

3- Cuando el Firewall central RPV recibe la solicitud de su sitio remoto RPV empieza un proceso de negociación para poder establecer una comunicación segura. Esto quiere decir que antes de pasar a un nivel superior (cliente y servidor) se autentifica que la conexión de este usuario remoto sea válida.

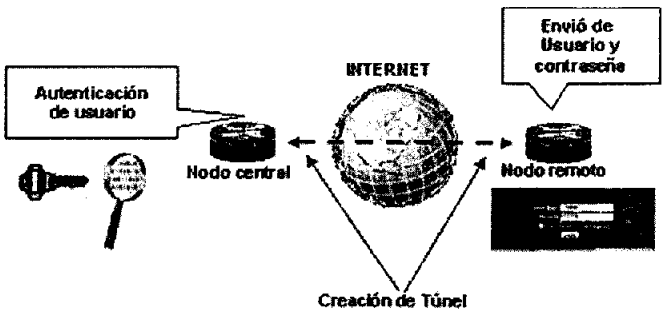


Figura 38. Auntentificación de usuario.

4- Cuando ambas partes ya se han autentificado se establece el "túnel de encriptación". Esto quiere decir que mantienen una comunicación constante entre estos dos puntos.

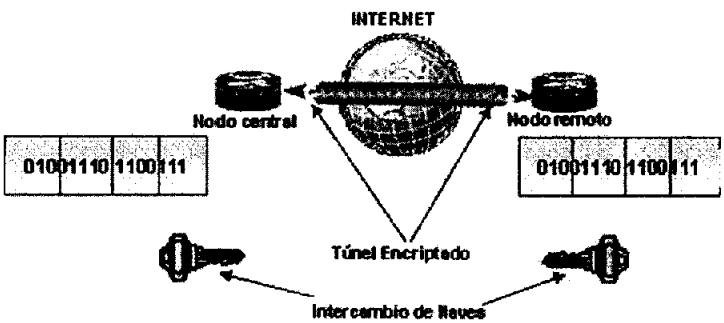


Figura 39. Establecimiento de túnel encriptado.

5- Con el establecimiento del "túnel encriptado" la organización remota RPV se autentifica en la red a la que esta accesando. Este proceso dependerá de la plataforma de red que exista en nuestra empresa, una vez que el servidor RPV sabe que esta organización tiene los derechos de acceso otorgados permite su ingreso.

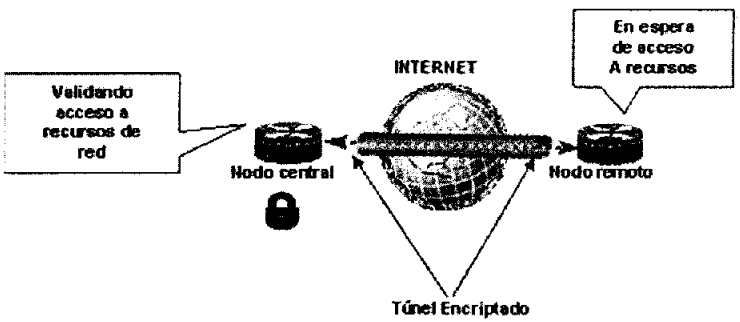


Figura 40. Privilegios de usuario.

6- La organización remota ya puede hacer uso de todos los recursos disponibles en la red de la empresa (voz, datos, video).

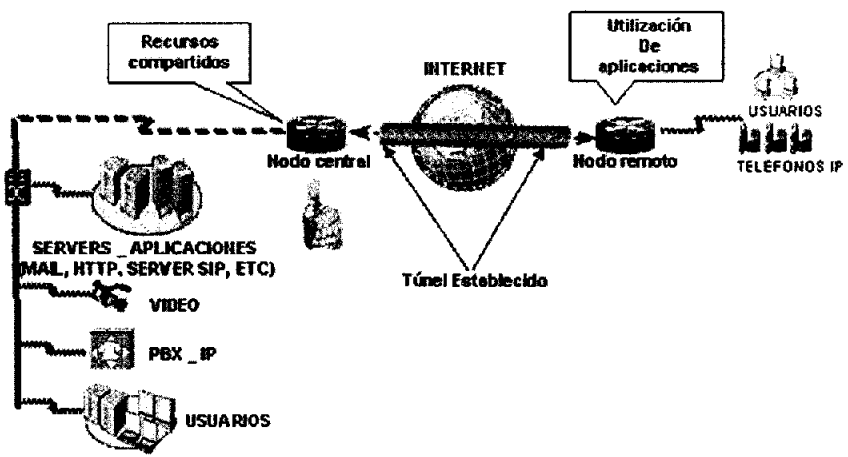


Figura 41. Acceso a los recursos permitidos.

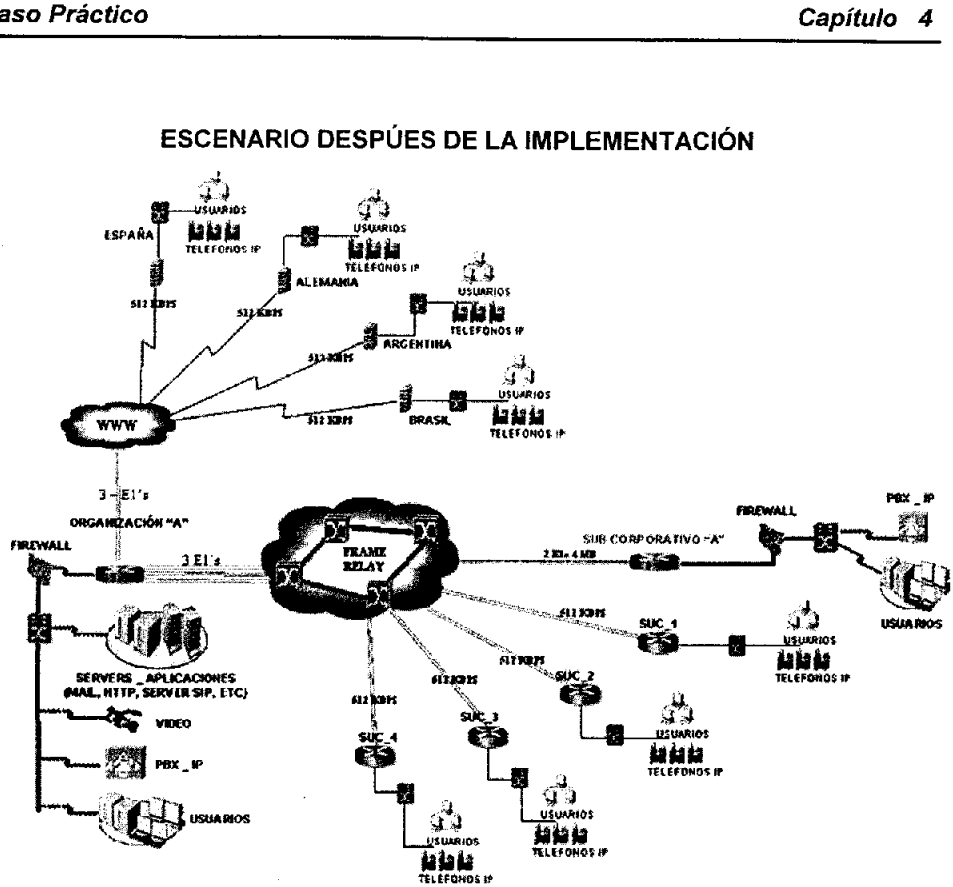


Figura 42. Red Frame Relay - IPsec.

La forma de operar de la organización después de haber implementado una RPV sobre el protocolo IPSec seria de la siguiente manera.

Cuando un host local envía información a otro remoto que pertenece a la misma organización, los datos tienen que atravesar el primer Gateway en este caso el Firewall que está antes de salir a la red pública (Internet), y luego a través del segundo Gateway en cuyo caso sería el Firewall que se configuró como servidor de acceso, el cual proporcionará la entrada a la red local remota en la que está el host receptor de la información.

El sistema protegerá dicha información de forma automática encriptándola, haciéndola de tal forma incomprensible a terceras partes. Los gateways (Firewalls) pueden asimismo hacer una doble función, al actuar también como cortafuegos que denieguen el acceso de datos generados por hackers o virus informáticos.

Las necesidades y exigencias del mundo moderno son cada vez mayores por lo que las tecnologías que se utilizan para el desarrollo de una red tienen que enfocarse a la sencillez de su administración y sobre todo asegurando que no se deje de lado la seguridad de la información ya que juega un papel importante para el óptimo desempeño de una red.

La elección del tema se hizo tomando en cuenta la necesidad de una tarea que permitiera demostrar la capacidad de gestión de recursos tecnológicos en función de una realidad nacional y mundial para lograr un producto viable, factible y realmente útil.

Por todo esto, en este trabajo se aborda la aplicación de mecanismos de seguridad a través de protocolos como IPSec, aplicando soluciones a las problemáticas de las organizaciones que se atreven a cambiar su forma de transmitir su información a través de la red Internet. Así mismo se explicaron las implicaciones que surgen al implementar este tipo de tecnología en una empresa, sus costos, sus beneficios y también sus desventajas.

El cambio de tecnología que se planteó en este trabajo está direccionado para utilizar herramientas de punta en hardware y software, haciendo uso de los medios de transferencia de información más económicos y universales como Internet y con los protocolos de seguridad y comunicaciones propios de este medio; garantizando la estabilidad de la plataforma mediante la correcta integración de tecnologías.

El estudio que se realizó incluyó los protocolos que implica IPSec, tipo de túneles, cifrado, autenticación, etc. y se detalló como este tipo de conexión asegura solamente al tráfico que circula a través del túnel, es decir, IPSec es un protocolo punto a punto, que establece una comunicación segura entre dos puntos únicamente, y no es un protocolo end-to-end, es decir, no hay protección de sistema a sistema, o de usuario a usuario.

Para comprender los beneficios que se obtienen al implementar una RPV superpuesta se explicó el desarrollo de este cambio, así como los equipos que opcionalmente pueden ser utilizados; el escenario se proyecta de manera que existirán organizaciones que se puedan comunicar en red desde puntos lejanos usando como medio de transporte Internet y estas a su vez utilizar el mismo medio para poder comunicarse con otras organizaciones todo esto con el único fin de intercambiar información entre empleados, clientes y socios comerciales.

BIBLIOGRAFÍA

Textos

- McQuerry, Steve, **"Interconexión de dispositivos de red Cisco"**, Ed. Pearson Educación, S.A. Madrid, 2001
- Schwartz, Mischa, **"Telecommunication Networks Protocols"**, Addison Wesley, 1994 (versión en español)
- Stallings, William., ***"Local Area Networks"***, Prentice-Hall, Second Edition, 1997
- Tanenbaum, Andrew S., **"Computer Networks"**, Ed. Prentice-Hall, E.U. 2002
- Thomas A, Stephen, ***"IPng and the TCP/IP protocols, implementing the next generation Internet"***, Ed. John Wiley & Sons, Inc. E.U. 2001
- Academia de Networking de Cisco Systems: GUÍA DEL SEGUNDO AÑO. Tercera edición Editorial Ciscopress (Pearson Educación, S.A.)

Mesografia

http://teleline.terra.es/personal/jralcala/web/redes/vpn/vpn1.htm

http://www.rediris.es/rediris/boletin/54-55/ponencia2.html

http://www.maillist-archive.de/security-basics.htm

http://cpi.ictnet.es/ICTnet/cv/documentos.jsp?area=tecInf&cv=intranet

http://ditec.um.es/laso/docs/tut-tcpip/3376c22.html#address

http://www.mundopc.net/ginformatico/g/gateway.php

http://www.virtual.uamericas.cl/faci/foro/viewtopic.php?t=1973

http://www.informatica.uv.es/it3guia/TD/practica-pix2.**pdf**

http://www.uniboyaca.edu.co/facingenieria/**ipsec.pdf**

www.monografias.com/trabajos12/mon**vpn**/mon**vpn**.shtml

- **3DES**.- Triple data encryption standard
- **ADSL**.- Línea de abonado digital asimétrica
- **AES**.- Algoritmo de encriptación avanzado
- **AH**.- Authentication header
- **ANSI**.- American national standards institute
- **ATM**.- Modo de transferencia asíncrono
- **BC**.- Ráfaga comprometida
- **BE**.- Ráfaga en exceso
- **BRIDGE**.- Puente dispositivo de interconexión de redes de ordenadores
- **CBCP**.- Protocolo de control de iteración
- **CBR**.- Velocidad de ráfaga comprometida
- **CE**.- Customer edge
- **CHAP**.- Protocolo de autenticación de saludo challenge
- **CIR**.-Tasa de información comprometida
- **CPE**.- Customer premises equipment
- **CRC**.- Código de verificación de redundancia cíclica
- **DCE**.- Data communication equipment
- **DES**.- Data encryption standard
- **DLCI**.- Identificador de conexión de enlace de datos
- **DS0**.- Servicio de línea privada
- **DTE**.- Data Terminal Equipment
- **E1**.- Línea digital con velocidad de 64kbps hasta 2 mbps
- **E3**.- Línea digital con velocidad de 34 mbps
- **EAP**.- Protocolo de autenticación ampliable
- **EBR**.- Velocidad de ráfaga en exceso
- **ESP**.- Encapsulating security payload
- **FCS**.- Frame check secuence
- **FRADS**.- Familia de equipos de acceso frame relay
- **G.703/704**.-Interfase con capacidad de 2mbps y conectores bnc y/o rj-45
- **GRE**.- Generic routing encapsulation, protocolo
- **HASH**.- Protocolo que garantiza la integridad de los textos
- **HDLC**.- High-level data link control
- **HMAC**.- Hash message authentication codes
- **ICMP**.- Protocolo de mensajes de control y error de Internet
- **IETF**.- Grupo de trabajo en ingeniería de Internet.
- **IKE**.- Internet key exchange
- **IP**.- Protocolo de internet
- **IPCP**. - Protocolo de control de IP
- **IPSEC**.- Protocolo de seguridad IP
- **IPX**.- Internetwork Packet Exchange

- **ISAKMP**.- Asociación de seguridad del protocolo de gestión de claves de asociaciones de seguridad en Internet
- **ISDN**.- Red digital de servicios integrados
- **ISP**.- Proveedor de servicio de Internet
- **L2F**.- Layer 2 forwarding
- **L2TP**.- Layer 2 tunneling protocol
- **LCP**.- Protocolo de control de enlace
- **LMI**.- Interfase de administración local
- **MD4**.- Algoritmo para la comprobación de la integridad de ficheros
- **MD5**.- Algoritmo para la comprobación de la integridad de ficheros binarios
- **MPLS**.- Multiprotocolo de intercambio de etiquetas
- **MPPC**.- Microsoft point to point compression
- **MPPE**.- Microsoft point to point encription
- **MSCHAP**.- Microsoft challenge handshake authentication protocol
- **NAS**.- Servidor de acceso a la red
- **NCP**.- Protocolo de control de red
- **NETBEUI**.- Protocolo de red ideado por microsoft
- **NNI**.- Network to Network Interface
- **OAKLEV**.- Metodo de autenticación de certificados de llaves públicas
- **PAD**.- Packet assembly and disassembly
- **PAP**.- Protocolo de autenticación de contraseña
- **PBX**.- Private branch exchante, sistema telefónico al interior de la empresa
- **PE**.- Provider edge.
- **PKI**.- Infraestructura de clave pública
- **PPP**.- Point-to-point protocol protocolo de conexión punto a punto
- **PPTP**.- Point-to-point tunneling protocol
- **PVC**.- Permanent virtual circuit
- **RIPV2**.- Versión mejorada de Rip v1. Comparte muchas de las mismas funciones que RIP v1. RIP v2, también es un protocolo de vector-distancia
- **RPV**.- Red Privada Virtual
- **RS232-C**.- Interfase serial estándar para comunicación con PC u otros equipos
- **RSA/RC4**.- El cifrado estándar se aplica al tráfico, y la autenticación de los usuarios
- **SA**.- Asociaciones de seguridad
- **SDLC**.- Protocolo para el control de enlace de datos
- **SHA-1**.- Secure Hash Algorithm, uno de los algoritmos más usados para firmar documentos electrónicos
- **SNA**.- *Standard Network Architecture*, es el protocolo de red utilizado por IBM para conectividad con sus hosts o mainframes
- **SP**.- Proveedor de servicios

- **SPI**.- Index parameter security
- **SVC**.- Switched virtual circuit
- **TCP**.- Protocolo de control de transporte
- **TCP/IP**.- Protocolo de control de transporte / Internet Protocol
- **TDM**.- Múltiplexacción por división de tiempo
- **UDP**.- Protocolo no orientado a la conexión
- **UNI**.- User to network interface
- **V.35**.- Conexión física de datos
- **VC**.- Virtual Circuit
- **X.25**.- Estándar para redes de paquetes recomendado por CCITT
- **XDSL**.- Línea Digital Asimétrica

- **3DES**.- Usa tres claves de 56 bits, un total de 168 bits. DES es un tipo de cifrado de los conocidos como Red Feistel Tradicional.
- **Blowfish**.- Es un algoritmo de encriptación que puede usarse como sustituto de DES y de IDEA. Es simétrico y encripta bloques, con una clave de longitud variable, desde 32 bits hasta 448 bits. Fué diseñado en 1993 por Bruce Schneier como una alternativa a los algoritmos existentes entonces, y con procesadores de 32 bits en mente, lo que lo hace significativamente más rápido que DES.
- **Capa 1**.- Nivel físico del modelo de interconexión de sistemas abiertos
- **Capa 2**.- Enlace de datos del modelo de interconexión de sistemas abiertos
- **Datagrama**.- Paquete de ip que contiene toda la información de control de la conexión y el segmento de datos tcp/udp
- **DES**.- (Data Encryption Standard) es un método de encriptación de clave privada muy usado. Es un método de encriptación simétrico, lo que obliga a que tanto el emisor como el receptor han de conocer la clave privada. DES aplica una clave de 56 bits a cada bloque de 64 bits de datos. El proceso se puede ejecutar en diferentes modos e implica 16 turnos de operaciones. Aunque está considerado como un algoritmo de encriptación fuerte, muchas organizaciones usan "triple DES", o sea aplicar 3 claves de forma sucesiva.
- **Dial-up**.- Acceso por la red telefónica
- **Enrutador**.- Dispositivo hardware y software de interconexión de que opera en la capa 3 del modelo osi
- **Ethernet**.- Protocolo por el cual se comunican las computadoras en un entorno local
- **Extranet**.- Red que tiene acceso limitado y que esta disponible únicamente a usuarios específicos
- **Firewall**.- Sistema o grupo de ellos enfocados hacia una política de control de acceso entre la red de la organización e internet.
- **Frame Relay**.- Tecnología de conmutación rápida de tramas, basada en estándares internacionales
- **Gateway**.- Puerta de enlace
- **HDLC**.- (High-level Data Link Control) es un grupo de protocolos para la transmisión de datos entre nodos, o puntos de una red. En HDLC, los datos se organizan en unidades o frames y son enviadas a través de una red hasta un nodo de destino que verifica la llegada correcta del frame. El protocolo HDLC también gestiona el flujo al que se envían los datos.
- **Host**.- Ordenador dentro de una red
- **IDEA.-** (Internacional Data Encryption Algorithm) es un algoritmo de encriptación desarrollado en el ETH de Zurich (Suiza) por James Massey y Xuejia Lai. Usa criptografía de bloque con una clave de 128 bits, y se suele

considerar como muy seguro. Está considerado como uno de los algoritmos más conocidos.

- **IETF.- (Internet Engineering Task Force)** es la organización que define los protocolos estándares de funcionamiento de Internet, como por ejemploTCP/IP. Es supervisada por la IAB (Internet Society Internet Architecture Board). Los miembros de la IETF son escogidos entre los miembros de la Internet Society y de las organizaciones que la conforman.
- **IKE**.- (Internet Key Exchange) es un servicio de negociación automático y de gestión de claves, usado en los protocolos IPsec.
- **Intranet**.- Es un entorno interno diseñado para ser utilizado en el interior de una organización
- **IPsec**.- (Internet Protocol Security) es un estándar en desarrollo para garantizar la seguridad de las comunicaciones al nivel de red. Será especialmente útil para el desarrollo de redes privadas virtuales (RPVs).
- **LAN**.- Red de área local
- **MPLS**.- (Multiprotocol Label Switching) es una tecnología para acelerar el tráfico de red y hacerlo más sencillo de gestionar. MPLS configura un camino específico para una secuencia dada de paquetes de información, identificados por una etiqueta insertada en cada paquete. De esa forma, el router se ahorra el tiempo necesario para buscar la dirección siguiente a la que debe enviar el paquete. MPLS se denomina multiprotocolo puesto que funciona con los diferentes protocolos de red IP (Internet Protocol), ATM (Asynchronous Transport Mode) y frame relay. Respecto al modelo OSI, MPLS permite a la mayoría de los paquetes ser reenviados en el nivel 2 (switching) en lugar de en el nivel 3 (routing). Además de acelerar el movimiento del tráfico de datos, MPLS hace más sencillo gestionar una red para dar una determinada calidad de servicio (QoS, quality of service).
- **Osi**.- Modelo de referencia de interconexión de sistemas abiertos
- **Ospf**.- Protocolo de red que tiene por significado abrir primero la trayectoria más corta
- **PPP**.- (Point-to-Point Protocol), es un protocolo diseñado para establecer la comunicación entre dos ordenadores a través de un puerto serie, PP usa el protocolo IP (Internet Protocol), aunque está diseñado para poder usar otros.
- **RADIUS**.- (Remote Authentication Dial-In User Service) es un protocolo clienteservidor que permite a servidores de acceso remoto (concentradores VPN en este caso) comunicarse con un servidor central para autentificar a usuarios externos (dial-in) y permitirles el acceso a los servicios requeridos. RADIUS permite que una organización mantenga los perfiles de usuarios en una base Redes Privadas Virtuales

- **Switches**.- Llamado también conmutador interconecta dos o más segmentos de red y opera en la capa 2 del modelo OSI
- **Tunneling**.- Usado esencialmente para crear interfaces virtuales tipo túnel
- **WAN**.- Red de área amplia. Red que conecta ordenadores distantes.