IMPLEMENTACIÓN DE UN PROTOTIPO DE VPN EN INSTITUCIONES EDUCATIVAS DEL MUNICIPIO DE MADRID.

MARIA AZUCENA FONSECA LOZANO
LUZ AMANDA MORALES RODRIGUEZ
MARTHA PATRICIA CHAPARRO BELTRAN
WILLIAM JANSZOON GONZALEZ TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE CIENCIAS BASICAS E INGENIERIA
PROGRAMA DE INGENIERIA DE SISTEMAS
BOGOTÀ, D.C.
2004

IMPLEMENTACIÓN DE UN PROTOTIPO DE VPN EN INSTITUCIONES EDUCATIVAS DEL MUNICIPIO DE MADRID.

MARIA AZUCENA FONSECA LOZANO
LUZ AMANDA MORALES RODRIGUEZ
MARTHA PATRICIA CHAPARRO BELTRAN
WILLIAM GONZALEZ TORRES

PROYECTO

DIRECTORA
JEANETH HERRERA CUESTA
INGENIERA DE SISTEMAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE CIENCIAS BASICAS E INGENIERIA
PROGRAMA DE INGENIERIA DE SISTEMAS
BOGOTÀ, D.C.
2004

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____
Jurado

_____
Jurado

Bogotá, 24 de septiembre de 2004

	A nuestras familias por haber creado valores de integridad, constancia y perseverancia en nosotros. A toda la comunidad estudiantil del Municipio de Madrid por haber recibido el aporte de este proyecto como algo clave dentro de su proceso de formación. A las futuras generaciones de estudiantes de la Universidad Nacional abierta y a Distancia "UNAD" para que la referencia de este proyecto les sirva como punto de partida dentro de las investigaciones de este tipo.

AGRADECIMIENTOS

A Dios y su corte celestial por darnos la vida e iluminarnos el camino.

A nuestros padres, hermanos por su constante e incondicional apoyo

A nuestros hijos por su inmensa paciencia

A Norman Estupiñan, Licenciado en filosofía y letras, magíster en admón. Educativa, magíster en desarrollo educativo y social, candidato a doctor en Educación, por sus grandes ideas y enseñanzas

A la Fundación Pilares de Desarrollo en cabeza de la Rectora del Colegio Gabriel Echavarría, Jeaneth Parada, Psicóloga, por apoyar y creer siempre en esta propuesta

A la Rectora del Colegio Tecnológico de Madrid en cabeza de la Rectora Cecilia Matíz, Licenciada en Pedagogía, por argumentar la implementación de este proyecto ante el estado.

A nuestros tutores por su orientación.

A la Ingeniera de Sistemas Jeaneth Herrera y al Ingeniero de Sistemas Adriano Rodríguez, por trascender mas halla de ser tutores.

A la Universidad Nacional Abierta y a Distancia "UNAD", por generar espacios de crecimiento profesional y personal.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

ACL (Access Control List): asocia cada recurso con una lista ordenada de qué usuarios pueden tener acceso al recurso y cómo esos usuarios pueden accederlo

ANCHO DE BANDA: es el rango de frecuencias sobre el cual un dispositivo transmitirá información.

ALINEACIÓN: para crear un acoplamiento acertado, todo el equipo relacionado se debe asociar a sus accesorios o equipo respectivos.

ALGORITMO DE CIFRADO SIMÉTRICO: preferido para la llave: Este indica el algoritmo de cifrado que el propietario del certificado prefiere para que su información sea encriptada. Los algoritmos soportados son CAST, IDEA y 3DES

AMPLITUD: la magnitud de una forma de onda cuando está medida del punto mediano al pico de la onda.

ANÁLOGO: una señal en la forma de una cantidad que varia continuamente tal como voltaje, frecuencia o fase.

ANTENA: el dispositivo utilizado para concentrar y dirigir la energía de una señal en un haz apretado. Parabólicas o plato, rejilla, y Yagi son diversas variedades de antenas.

ANTENNA GAIN: (L A GANANCIA DE LA ANTENA) la relación entre la energía irradiada por una antena en una dirección específica frente a la energía requerida para producir la misma fuerza si se utilizase una antena isotrópica

ATENUACIÓN: la medida de la pérdida de energía en una señal de microonda en la medida en que viaja entre dos puntos. Se mide en decibelios (DB).

ATENUADOR: los atenuadores simulan antenas durante pruebas de bench.

AZIMUTH: ésta es la dirección de la antena apuntando relativo al verdadero norte.

BANDA: una porción del espectro electromagnético de la frecuencia.

BASTILLE: Estación de trabajo que permite agregar y quitar programas.

BIT: una abreviatura para los dígitos binarios.

BIT ERROR RATE (TASA DE ERROR BIT): es una medida del número de errores del numero de errores en una transmisión digital. Típicamente dado como un número exponencial que representa la relación de errores con respecto al total de bit. Ejemplo: 1E-03 = 0.001 = 1.0 x 10-3 and 1.0E-6 = 0.000001 = 1.0 x 10-3. Un solo elemento en un codigo binario.
BRIDGE (PUENTE): la función de un puente es conectar redes separadas. Este dispositivo funciona en la capa de DataLink del modelo de OSI. Los puentes conectan diversos tipos de la red (tales como Ethernet rápida y Ethernet) o redes del mismo tipo. Los puentes permiten solo permiten el tráfico necesario para pasar a través de segmentos señalados. Cuando el puente recibe un paquete, este determina los segmentos de la destinación y de la fuente. Si los segmentos son iguales, se cae, o se filtra el paquete. Si los segmentos son diferentes, entonces el paquete "se remite" al segmento correcto. Además, los puentes no remiten los paquetes malos o mal alineados. Los puentes también se llaman los dispositivos de almacenar y avanzar "store-and-forward" porque miran el paquete entero de Ethernet antes de tomar decisiones de la filtración o de la expedición. El filtrar paquetes y regenerar paquetes en proceso le permite a la tecnología de puentes el desagregar una red en dominios de colisión separados.

BRI (DEL INGLÉS BASIC RATE INTERFACE) : Tipo básico de servicio RDSI. Consiste de dos canales B de 64 kbit/s y un canal D de 16 kbit/s para un total de 144 kbit/s. Este servicio está orientado a brindar capacidad de conexión para usuarios residenciales.

BYTE: octeto Una unidad de datos que consiste en ocho bit.

CABLE: un medio de la transmisión del alambre de cobre o de la fibra óptica envuelta en una cubierta protectora.

CANAL: una banda de frecuencia especifica designada para un propósito especifico. El sendero de datos entre dos nodos.

CLASE: el entender esta metodología es difícil, aun para los clientes. Por lo tanto, déjenos explican esto en términos más fáciles. El primer octeto (o los octetos) define la "clase" (indicada por la palabra "red" en este ejemplo) de la dirección, que es el único método para decir el tamaño de la red (cómo es grande) y a

donde pertenece el internet address. Los octetos restantes indican la disponibilidad para el equipo de la red (es decir, la computadora o el otro equipo de la red). Las tres clases principales son: Clase A, clase B. y clase C.

CLASE A: red, nodo, nodo, nodo 255.0.0.0 (los tres octetos pasados están disponibles para el equipo).
CLASE B: red, red, nodo, nodo 255.255.0.0 (los dos últimos octetos están disponibles para el equipo).

CLASE C: red, red, red, nodo 255.255.255.0 (el ultimo octeto está disponible para el equipo)

CABLE COAXIAL: el tipo de línea de la transmisión que consiste en un alambre conductor central recubierto por un material de aislamiento que a su vez esta recubierto por un protector conductor hecho de hoja de metal o de trenza del alambre. Frecuentemente utilizado para conectar el sistema RF y la unidad del módem de un sistema sin hilos.

CODE DIVISION MULTIPLE ACCESS (CDMA): un sistema en el cual todos los usuarios ocupan el mismo ancho de banda. Los códigos sin correlación se utilizan para permitir una ocupación más alta del de banda. Esto también se conoce como el sistema de la expansión del espectro.

COMMON MANAGEMENT INFORMATION PROTOCOL (CMIP): es un protocolo de administración de red que es consistente con un modelo de red de comunicación de interconexión de sistemas abiertos.

COMPANY NAME (NOMBRE DE LA EMPRESA): esto es el nombre de la compañía que posee o mantiene la radio dada al terminal.

CONSOLA: este dispositivo permite que usted se comunique a través del cliente del telnet para tener acceso al software de la configuración.

DRAK CONF: Estación de trabajo que permite la configuración de mandrake como tal.

ESPACIAMIENTO DE CANAL: la cantidad de señales espaciales que pueden fluir.

ENTUNELAMIENTO (TUNNELING): los paquetes de datos son enrutados por la red pública, tal como Internet o alguna otra red comercial, en un túnel privado que simula una conexión punto a punto.

GENERIC ROUTING ENCAPSULATION -GRE: Protocolo de Encapsulamiento Ruteado Genérico

IP TABLE: Estación de trabajo que permite el manejo de tablas para la configuración de reglas de seguridad.

IPSEC: Protocolo de seguridad creado para establecer comunicaciones que proporcionen confiabilidad e integridad en los datos.

LA UNIDAD DE SERVICIO DEL SERVICIO UNIT/DATA DEL CANAL (CSU/DSU): maneja la transmisión digital y supervisa las señales para los problemas. Realiza muchas funciones similares a un módem a excepción de convertir señales análogas a digitales dados que los dispositivos de transmisión son digitales.

L2TP: Protocolo con el cual se tiene acceso a una red privada a través de internet o de otra red pública mediante una conexión de red privada virutal (VPN). Con el protocolo de túnel de nivel 2 (L2TP).

MAKDEV: Estación de trabajo que permite la configuración de dispositivos.

PPP: Protocolo que a su vez ya vienen incriptados en un paso previo para poderlos enviar a través de la red.

PPTP: Protocolo diseñado para permitir el transporte (encapsulado) de protocolos diferentes al TCP/IP a través de INTERNET. Lo que hace es encapsular los paquetes del protocolo PPP (point to point).

PRI (del inglés Primary Rate Interface): Tipo básico de servicio RDSI. Un enlace PRI está orientado a usuarios que requieren un mayor ancho de banda

RADIUS: es un protocolo muy ligero, basado en UDP, fue desarrollado por Livingston Enterprise, ahora una división de Lucent Technologies. Servidor de acceso en el cual se esta autenticando todas las conexiones.

RAS (REMOTE ACCESS SERVER): servidor de acceso remoto

ROUTER: este dispositivo es una combinación de una direccionador (router) y de un puente en un producto.

RESUMEN

Dentro de los temas más relevantes a tratar en el presente trabajo están:

- ✓ Estudio de Factibilidad: Se presentan las diferentes alternativas de soluciones de comunicación existentes hoy en día en el mercado de las telecomunicaciones. Se seleccionó la mas acorde de acuerdo a los requerimientos de este proyecto, para nuestro caso un ISP.

- ✓ Los enlaces privados antes de la aparición de las Redes Privadas Virtuales, Presenta un breve enfoque de las tecnologías WAN tradicionalmente implementadas, tanto dedicadas como conmutadas, entre las que se encuentran Clear Channel, Frame Relay, ATM, líneas análogas y líneas digitales RDSI.

- ✓ Redes Privadas Virtuales – VPNs: Presenta una descripción de la tecnología, asi como sus diferentes escenarios y sus componentes básicos.

- ✓ Arquitecturas VPN: Amplia cada una de las diferentes soluciones que se pueden implementar con las VPNs, tales como Acceso Remoto, LAN to- LAN y Extranets.

- ✓ Autenticación y Cifrado: Presenta los conceptos de seguridad sobre los cuales se basan todas las tecnologías existentes que sirven para implementar una VPN.

- ✓ Tecnologías VPN: Es la esencia del trabajo. Comprende las tecnologías existentes mas usadas para crear túneles y enlaces encriptados sobre redes privada y públicas. Comprende temas como PPTP, L2TP, IPSec y MPLS.

- ✓ Páginas Web: Se presenta el Diseño, construcción e implementación de un sitio web para los Colegios: Tecnologico de Madrid y Gabriel Echavarria.

INTRODUCCIÓN

En La actualidad las telecomunicaciones son parte fundamental en el proceso de desarrollo de la cultura de esta generación; de ahí nace la importancia de llevar esta tecnología desde el punto de partida en la educación del ser humano hasta su formación integral.

Este proyecto nació con el propósito de participar con nuestros conocimientos adquiridos en el diseño e implementación de una tecnología que contribuyera a lograr ese fin.
Gracias al trabajo conjunto y a la cooperación de muchas personas se logro diseñar un proyecto, que diera herramientas a la población estudiantil para mejorar su infraestructura tecnológica. Por esto se seleccionaron dos colegios que sirvieran de pilotos: El colegio Gabriel Echavarría y Tecnológico de Madrid; ambas instituciones se caracterizan por tener unos principios, ideales semejante, dar a sus estudiantes valores, desarrollar sus capacidades para tomar decisiones y enfrentar desafíos. Sus estudiantes son jóvenes creativos, investigadores honestos y seguros de si mismos.

El proyecto "**IMPLEMENTACIÓN DE UN PROTOTIPO DE VPN EN INSTITUCIONES EDUCATIVAS DEL MUNICIPIO DE MADRID.**" consistió en el diseño e implementación de una red privada "VPN" como canal que permitiera compartir información virtual, aprovechando de esta forma la sinergia de los jóvenes. Las directivas de las instituciones Gabriel Echavarría y Tecnológico de Madrid comprendieron la importancia de adquirir el servicio de internet para apoyar el desarrollo de este proyecto.

Además de implementar las redes virtuales, se diseñaron e implementaron las páginas Web para cada unos de los colegios; permitiendo que la comunidad en general conozca y pueda consultar las diferentes actividades académicas y culturales desarrolladas en cada uno de ellos.
Falta mucho por avanzar en este campo, sin embargo el continuo mejoramiento siempre será la meta por obtener. Estamos seguros que la implementación de este proyecto sumado al carácter de liderazgo de ambas instituciones permitirá a los jóvenes vivenciar nuevas tecnologías pensando siempre en el desarrollo de un mejor proyecto de vida.

1. PROBLEMA

1.1 Planteamiento y Descripción del problema a Investigar:

En el municipio de Madrid - Cundinamarca (Colombia), los colegios Gabriel Echavarría y Tecnológico no cuentan con una red que los comunique; al no estar comunicados estos colegios están desaprovechando todo el potencial informático con el que contamos hoy día.

Siendo estos colegios de educación básica primaria y secundaría; en este momento no cuentan con una conexión que les permitan tener una salida al exterior como lo es Internet, correo electrónico, página web entre otros, desaprovechando estos recursos.

Por tal motivo, se quiere llegar a la solución mas conveniente para que las instituciones educativas ya mencionadas utilicen todo el potencial informático que los conduzca a mejorar la plataforma con la que cuentan actualmente.

1.2 ANÁLISIS DE VARIABLES:

Dentro del proceso de análisis de variables se tomo como punto de partida tres grandes factores para cada uno de los colegios involucrados en este proyecto que son: Plataforma Informática, Aspecto económico y Aspecto Social.

1.2.1. Plataforma Informática:

1.2.2.1 Hardware

A continuación se realiza una descripción de los Equipos de cómputo de los colegios Gabriel Echevarria y Tecnológico de Madrid:

INVENTARIO DE EQUIPOS DE COMPUTO							
COLEGIO GABRIEL ECHAVARRIA							
Serial	**Producto**	**Compañia Propietaria**	**Categoria**	**Disco duro**	**Memoria**	**Procesador**	**Velocidad**

NA	Clon Desktop	Colceramica	Machines	20	128	CELERON	900
NA	Clon Desktop	Colceramica	Machines	1	16	P	133
NA	Clon Desktop	Colceramica	Machines	6	32	P	NA
F636BBQ10489	Compaq Deskpro	Colceramica	Machines	4	32	P	120
NA	Clon Desktop	Colceramica	Machines	40	64	CELERON	400
NA	Clon Desktop	Colceramica	Machines	4	32	P	120
NA	HP Desk Jet 610C	Colceramica	Impresora	NA	NA	NA	NA
07520750281	Lexmark X73	Colceramica	Impresora	NA	NA	NA	NA
NA	Clon Desktop	Colceramica	Machines	15	64	P3	550
K69866020004	Scanner Symbol LF2104	Colceramica	Scanner	NA	NA	NA	NA
CDUY154051	Epson LX 300	Colceramica	Impresora	NA	NA	NA	NA
NA	Clon Desktop	Colceramica	Machines	40	256	P3	1100
NA	Clon Desktop	Colceramica	Machines	20	562	CELERON	800
F713HVU60210	Compaq Deskpro	Colceramica	Machines	4	32	P	NA
NA	Clon Desktop	Colceramica	Machines	20	264	CELERON	800
F543HMW60527	Compaq Deskpro 575	Colceramica	Machines	1	32	P	NA
NA	Clon Desktop	Colceramica	Machines	8	16	P	200
NA	Clon Desktop	Colceramica	Machines	4	16	P	NA
NA	Clon Desktop	Colceramica	Machines	20	262	CELERON	800
MX9681V109	HP Desk Jet 710C	Colceramica	Impresora	NA	NA	NA	NA
CDUY187644	Epson LX 300	Colceramica	Impresora	NA	NA	NA	NA
US8481W06S	HP Desk Jet 692C	Colceramica	Impresora	NA	NA	NA	NA
0010259222	Epson LX 800	Colceramica	Impresora	NA	NA	NA	NA
NA	Clon Desktop	Colceramica	Machines	NA	NA	NA	NA
SG7C41D0J9	HP Desk Jet 692C	Colceramica	Impresora	NA	NA	NA	NA
NA	Clon Desktop	Colceramica	Machines	2	16	P	150
78NWAZN	IBM PC350	Colceramica	Machines	6	64	NA	NA
NA	Clon Desktop	Colceramica	Machines	NA	NA	NA	NA
F805BK550053	Compaq Deskpro	Colceramica	Machines	8	32	P	NA
0E11332697	Epson FX 1050	Colceramica	Impresora	NA	NA	NA	NA
CN93G120VM	HP Desk Jet 695C	Colceramica	Impresora	NA	NA	NA	NA
MX95D141WB	HP Desk Jet 695C	Colceramica	Impresora	NA	NA	NA	NA

Tabla 1. Descripción de Equipos de Cómputo colegio Gabriel Echavarria

EQUIPOS DE CÓMPUTO Y ACCESORIOS. COLEGIO Tecnológico de Madrid		
Servidor Compaq Proliant 800	Bueno	1 (Uno)
Monitor Compaq Modelo PE1100 de 14" a color con base, cable de poder y de datos (servidor)	Bueno	1 (Uno)

Mouse Compaq PS/2 de dos botones modelo M-S34	Bueno	16 (dieciséis)
Teclado Compaq para Windows 95, Latin American 166516-166, PS/2, español	Bueno	16 (dieciséis)
Par de parlantes modelo SP-120C	Bueno	14 (dieciséis)
Par de parlantes modelo SP-120C	Malo	2 (dos)
Filtro para monitor	Bueno	16 (dieciséis)
Pad Mouse	Malo	16 (dieciséis)
Forro para teclado	Bueno	16 (dieciséis)
Forro para Servidor	Bueno	1 (Uno)
Forro para Monitor (Server)	Bueno	1 (Uno)
Forro para PC (workstation)	Bueno	15 (Quince)
Monitor a color Compaq Modelo PE1112, 15", base, cable de poder y datos (workstation)	Bueno	15 (Quince)
WorkStation Compaq Deskpro con cable de poder modelo EPC466	Bueno	15 (Quince)
Micrófono de cabeza modelo HP-116C	Regular	16 (dieciséis), empaque
OTROS ACCESORIOS WORKSTATIONS		
Tapa "Compaq Deskpro" para posición vertical	Nuevo	15 (Quince, empacadas)
Juego de pieza metálica y un tornillo	Nuevo	12 (Doce, empacados)
Juego de pieza metálica y dos tornillos	Nuevo	3 (Tres, empacados)

PERIFERICOS ESPECIALES		
Impresora Lexmark Optra E+ con cable de poder y cable de datos	Bueno	1 (Una)
Escáner Agfa modelo Snapscan Touch con cable USB, adaptador de poder y siete manijas	Bueno	1 (Uno)
Cámara de fotografía digital Epson modelo PhotoPC 850Z con los siguientes accesorios: • Cargador de baterías Ni-MH modelo EU-38 con cable de poder • Cuatro pilas recargables EPSON • Tarjeta de memoria CompactFlash de 48 MB • Cable de video • Cable para puerto serial • Cable para puerto USB • Cable para Mac/impresión directa • Adaptador de lentes • Correa	Bueno	1 (Una)
Televisor LG 20"	Bueno	1
Combo VHS – DVD LG	Bueno	1
Soporte para TV y VHS anclado en la pared	Bueno	1
CABLEADO ESTRUCTURADO CAT 5		
Canaleta de cableado estructurado y red eléctrica	Bueno	Distribuida por las paredes
Rack cerrado 19", dos llaves	Bueno	1 (Uno)

Patch Panel 24 RJ45 Cat 5 marca Lucent	Bueno	1 (Uno)
Hub Netgear Modelo DS524	Bueno	1 (Uno)
Router 3Com Lan Modem, modelo 3C886	Bueno	1 (Uno)
Toma lógica Cat 5	Bueno	22 (veintidós)
Tomacorriente doble Leviton	Bueno	44 (Cuarenta y cuatro)
Caja de alumbrado de 12 tacos con tres circuitos principales y dos para extractores.	Bueno	1 (Una)
Tablero eléctrico de sobreponer, dos llaves	Bueno	1 (Uno)
Regulador Energex Modelo AV-650p	Bueno	1 (Uno)
UPS PowerCom modelo KIN-1000AP	Bueno	1 (Una)
Patch Cord RJ-45 Cat 5 Lucent de 1m aprox.	Bueno	22 (Veintidós, 16 en uso)
Patch Cord RJ-45 Cat 5 Lucent de 3m aprox.	Bueno	22 (Veintidós, 16 en uso)

SOFTWARE Y DOCUMENTACIÓN		
Enciclopedia Multimedia Salvat, edición de 1998	Nuevo	12 (Doce, sin destapar)
Enciclopedia Multimedia Salvat, edición de 1998	Bueno	3 (Tres)
Caja de Enciclopedia Multimedia Salvat, edición de 1998	SIN CD	1 (Una)
CD drivers impresora Lexmark	Bueno	1 (Uno)
CD Restore Compaq Deskpro	Bueno	15 (Quince)
Guía de usuario impresora Lexmark	Bueno	1 (Uno)
CD drivers ATI Rage Pro (server video card)	Bueno	1 (Uno)
CD drivers Lan Modem 3Com	Bueno	1 (Uno)
CD Utilitarios Lan Modem 3Com	Bueno	1 (Uno)
Set Drivers en disquette impresora Lexmark	Nuevo	1 (Uno, tres discos)
CD copia antivirus McAfee	Bueno	1 (Uno)
Paquete “Guía de Usuario” Monitor Compaq V45	Nuevo	1(Uno)
Guía de Solución de Problemas Compaq, manual y CD	Nuevo	15 (Quince, sin destapar)
Paquete “Guía de Usuario” Monitor Compaq S500	Nuevo	15(Quince, sin destapar)
Introducción a Microsoft Windows 98, paquete de libro, folleto y CD	Bueno	14 (Catorce)
Instrucciones de seguridad Cargador de baterías de la Epson PhotoPC 850Z	Nuevo	1 (Uno)
Guía rápida de referencia Epson PhotoPC 850Z	Nuevo	1 (Uno)
Guía del Usuario Epson PhotoPC 850Z	Nuevo	1 (Uno)
CD Drivers y aplicaciones Epson PhotoPC 850z	Nuevo	1 (Uno)
Plegable Epson Ink Jet Papers	Nuevo	1 (Uno)
Mapa de Navegación del SnapScan Agfa (pleable de tres secciones y una hoja sencilla)	Nuevo	1 (Uno)
Instalación del escaner y del software snapscan	Nuevo	1 (Uno)
CD drivers snapscan con plegable de instalación con portaCD para 3 discos y cubierta de protección	Nuevo	1 (Uno)
CD Corel Print House Magic con tarjeta de registro	Nuevo	1 (Uno)
CD Page Keeper Standard	Nuevo	1 (Uno)
Manual de Microsoft: El Camino de la Tecnología	Nuevo	1 (Uno)
Manual de Microsoft: Productividad en el Salón de Clases	Nuevo	1 (Uno)
DVD Predators of the Animal World	Bueno	1 (Uno)
Paquete Microsoft Office 2000 Premium, consta de: • Estuche de cuatro CD´s	Nuevo	1 (Uno)

• Cuadernillo "Garantía Limitada" • Plegable "Información de subsidiarias de Microsoft" • Tarjeta "Microsoft Office Update" • Tarjeta de Registro • Manual "Descubra Microsoft Office 2000"		
Sistema Operativo Microsoft Windows NT 4.0 Server, consta de: • Caja de 2 CD´s con cuadernillo: - Instalación de Windows NT Server - Microsoft FrontPage 98 • Caja de 2 CD´s sin cuadernillo: - Service Pack 4 - Windows MT Option Pack • Disquettes de instalación (tres) • Cuadernillo "Garantía Limitada" • Plegable "Información de subsidiarias de Microsoft" • Tarjeta de Registro • Tarjeta de "Orden de Instalación" • Manual: "Introducción"	Nuevo	1 (Uno)

Tabla 2. Descripción de Equipos de Cómputo colegio Tecnológico de Madrid

Descripción servidores

Servidor	**Producto**	**Compañia Propietaria**	**Serie**	**Disco duro**	**Memoria**	**Procesador**	**Velocidad**
Ubicado en el colegio Gabriel Echevarria	Clon	Fundación Pilares de Desarrollo	S/N	20 gigas	Ram: 256 Mb	Celeron	Mhz.
Ubicado en el Colegio Tecnológico de Madrid	Clon	Colegio Tecnológico de Madrid	S/N	20 gigas	Ram: 128 Mb.	Celeron	Mhz.

Tabla 3. Descripción de Servidores

1.2.2 Software

Dentro de la investigación realizada se tomo la plataforma de software libre con los siguientes protocolos que se tienen en cuenta para la implementación de VPNs:

IPSEC Protocolo de seguridad creado para establecer comunicaciones que proporcionen confiabilidad e integridad en los datos.

PPTP Protocolo diseñado para permitir el transporte (encapsulado) de protocolos diferentes al TCP/IP a través de INTERNET. Lo que hace es encapsular los paquetes del protocolo PPP (point to point).
PPP Protocolo que a su vez ya vienen incriptados en un paso previo para poderlos enviar a través de la red.

L2TP Protocolo con el cual se tiene acceso a una red privada a través de internet o de otra red pública mediante una conexión de red privada virutal (VPN). Con el protocolo de túnel de nivel 2 (L2TP).

1.2.2 Aspecto Económico:

Se contó con apoyo económico de la empresa privada al igual que en el gobierno municipal.

Los costos generados para el desarrollo de este proyecto son:

Canal dedicado de 128k de ancho de banda (anual), para los Colegios (Gabriel Echavarría y Colegio Tecnológico de Madrid	$ 12.000.000
Dominio para los Colegios (Gabriel Echavarría y Colegio Tecnológico de Madrid, por dos (2) años.	$ 150.000
Asesoría y varios (18 meses)	$ 3.000.000

1.2.2.1 Costo / Beneficio

Partiendo de las diferentes soluciones dadas en nuestro proyecto encontramos que la más viable es tomar como plataforma LINUX; debido a que el software es de libre uso. La parte ingenieril es realizada por los ingenieros Maria Azucena Fonseca Lozano, Luz Amanda Morales Rodríguez. Martha Patricia Chaparro Beltrán y William González Torres quienes forman parte del Proyecto **IMPLEMENTACIÓN DE UN PROTOTIPO DE VPNs EN INSTITUCIONES EDUCATIVAS DEL MUNICIPIO DE MADRID**, además se recibe apoyo de los colegios Gabriel Echevarria, Tecnológico de Madrid y de la Empresa Privada.

Cuadro comparativo Costo/Beneficio

COSTOS	SQL	ORACLE	LINUX	IFX
Licencias	$2.000.000	$3.000.000	Software Libre	
Hora Ingeniero	$ 160.000	$220.000	COSTO /BENEFICIO	
Alquiler del Canal Para acceder a Internet				$1.000.000 mensual por diez equipos

Tabla 3. Cuadro Comparativo Costo/Beneficio

1.2.3 Aspecto Social:

Durante la investigación realizada para llevar a cabo este proyecto se tuvo en cuenta los dos tipos de población existente en el municipio de Madrid; esta el Colegio Gabriel Echevarria que forma parte de la Fundación Pilares de desarrollo, y da un 80% de ayuda a éste. De otro lado encontramos el Colegio Tecnológico de Madrid, que es un Colegio estatal el cual cuenta con un presupuesto muy limitado y va dirigido a una población de escasos recursos económicos.

El beneficio dado a una parte de la población de Madrid se da primordialmente en aprovechar mejor sus recursos tecnológicos con la salida a Internet, las páginas Web y de esta forma poder compartir información entre el Colegio Gabriel Echevarria y el Colegio Tecnológico de Madrid.

1.2.3.1 Tipos de solución

Se diseña e implementa un prototipo de red para que las dos instituciones se comuniquen a través de una VPN con los beneficios de una página web para cada uno de los colegios, Gabriel Echevarria y Tecnológico de Madrid, para poder realizar esta solución se contrata un proveedor de servicios de internet. En este caso se realizó con IFX.

1.3. Formulación

¿En que medida se hace necesario el diseño de una red que comunique los colegios Tecnológico y Gabriel Echavarría, teniendo como solución la salida a Internet, cuentas de correo, dos páginas web e implementación de VPNs y que a la vez sirvan como prototipo para el resto de colegios del municipio de Madrid?

1.4 Delimitación

Diseñar e implementar una red VPN en cada uno de los Colegios Gabriel Echevarria, Colegio Tecnológico de Madrid con su respectiva salida a Internet; utilizando plataforma de Software libre, y diseñando en cada Colegio una página Web para publicación de información de acuerdo con las exigencias de cada colegio.

2. OBJETIVOS

2.1 Objetivo General

Diseñar e implementar un prototipo de Red Wan utilizando redes privadas virtuales "VPN" para los colegios Gabriel Echavarría y Tecnológico, ubicados en el municipio de Madrid – Cundinamarca (Colombia), con el fin de compartir información académica, cultural y dar a conocer a la comunidad cibernética estas instituciones a través de un sitio Web.

2.2 Objetivos Específicos

- ✓ Levantar información en las salas de informática, identificando la topología de la red, el cableado estructurado, hardware y equipos activos con su respectivo software e Investigar el tipo de solución tecnológica viable de acuerdo a los costos, beneficios y ubicación geográfica de los Colegios Gabriel Echavarría y Tecnológico de Madrid (Cundinamarca).

- ✓ Diseñar e implementar una red VPN y las páginas Web de los Colegios (Gabriel Echavarría y Tecnológico de Madrid.) con salida a Internet de acuerdo a la investigación realizada.

- ✓ Realizar pruebas de conectividad en cada uno de los Colegios (Gabriel Echavarria y Tecnológico de Madrid, de acuerdo a la solución implementada.

- ✓ Publicar las páginas que han sido implementadas.

3. JUSTIFICACIÓN

El momento actual esta atravesado por los procesos de comunicación, tanto es así que a esta era se le ha bautizado como la era de la información[1]. Esto es evidente en el comercio, la navegación, la industria, la educación, entre otras actividades. En el caso de la educación se espera que las nuevas tecnologías hagan parte sustancial de su que hacer, lo anterior esta reclamando que los procesos tecnológicos de la informática circulen por todo el andamiaje de los centros educativos para que este tipo de tecnología sea aprovechado por todos los usuarios de los planteles. Esto requiere que para su mejor aprovechamiento los colegios no solamente establezcan salas de informática en su interior sino que se comuniquen unos con otros para así aprovechar el mayor potencial que estos nuevos escenarios educativos ofrecen.

Los colegio Gabriel Echavarría y el Tecnológico, cuentan con una sala de informática cada uno, las cuales se encuentra en una red de area local. No cuentan con una salida a Internet, y a nivel informatico no estan comunicados con otros colegios, lo cual es clave hoy en día para el intercambio de información permita un mejor aprendizaje del niño en las aulas.

Se busca incentivar en los alumnos y maestros la mentalidad de interacción con todo el entorno tecnológico que los rodea, por lo cual se hace necesario la implementación de una red que permita utilizar el recurso de Internet y que puendan compartir información mas halla de lo que la educación tradicional les pueda ofrecer; ya que Internet permite proporcionar a colegios, bibliotecas, empresas y hogares acceso universal a una información de calidad que eduque, informe y entretenga.

Las Redes Privadas Virtuales (VPNs) son una alternativa práctica, segura y eficiente de los enlaces privados que en la actualidad son usados para interconectar redes corporativas y brindar acceso a trabajadores teleconmutados.

Este trabajo de grado tiene como objetivo primario dar a conocer esta tecnología y brindar las pautas necesarias, apoyándose en conceptos técnicos y prácticos, para una adecuada implementación.

[1] La era de la Información Manuel Castells

4. MARCO HISTÓRICO

Madrid es una población ubicada a 20 kilómetros de la capital de Colombia. Ésta cuenta con 60.000 habitantes; allí hay una población estudiantil de 15.641 repartidas en 54 planteles educativos. Para nuestro caso en particular hemos tomado dos planteles:

Colegio Gabriel Echevarria, este plantel fue fundado hace 40 años; creado por la Fundación Pilares de desarrollo para los hijos de los empleados de esta empresa y actualmente brinda sus servicios a toda la comunidad madrileña, cuenta con una jornada de 7:00 a.m. a 3:00 p.m. tiene 514 alumnos repartidos así: 241 de primaria y 273 de bachillerato distribuidos en 14 cursos.

Colegio Tecnológico Creado mediante Acuerdo No. 033 de Octubre 30 de 1996, Jornada Única calendario A, de carácter oficial, Género Mixto Resoluciones No. 017777 Noviembre 2 de 2000 y No. 02552 de Diciembre de 2001 Básica Secundaria y Media Vocacional, Bachillerato Clásico y Certificado de estudios Especializados DANE No. 12543000740". Los cuales cuentan cada uno con una sala de informática, En esta sala se dictan clases de Office, programas educativos entre otros.

4.1 Antecedentes

Para este proyecto se tomo una experiencia realizada en: [2]"El Instituto de Educación Saavedra de Capdepera (Mallorca) tiene unos 400 alumnos, Ciclos Formativos y Garantía Social, que tienen acceso a 2 aulas de informática de 14 ordenadores cada una. Ocasionalmente utilizan también algunos ordenadores de la biblioteca y de las aulas de apoyo.

Conectar los ordenadores de las aulas a Internet ha sido un gran avance, y todavía recordamos hace tan sólo unos años, el único ordenador con módem de 56 Kb que tardaba tanto! Sin embargo el uso que se hace de Internet se puede convertir fácilmente en abuso:

[2] pagina Web. European Academic and Research Netword

Algunos alumnos que se conectan a páginas porno en cuanto el profesor se da la vuelta o se ausenta. Otros que con el pretexto de buscar información para un trabajo, se bajan las últimas canciones del triunfito de moda. Alumnos que no pueden ponerse a trabajar si antes no han comprobado su correo, operación que dura la mitad de la clase. chat .etc.. Todo esto puede hacer que ciertos profesores se desanimen y vean Internet como un problema y no como una herramienta educativa, mostrándose reacios a utilizar el aula de informática. Está claro que el profesor no puede vigilar la actividad de todos los ordenadores todo el tiempo, y tampoco se trata de ir al aula de informática para acabar haciendo de policía.
Así pues sería deseable controlar el acceso a Internet de manera automática a fin de:

- Evitar páginas web inadecuadas mediante un filtro.
- Registrar las páginas visitadas desde cada ordenador.
- Establecer un horario para que Internet esté disponible únicamente en las horas en que realmente haga falta.

LA SOLUCIÓN

Las funciones requeridas se pueden conseguir mediante el filtro SquidGuard, que usa una base de datos con miles de direcciones web clasificadas en grupos (porno, violencia, publicidad...). Hay múltiples opciones de configuración:
Bloqueo por grupo o por palabra clave, identificación del cliente por su dirección IP o por nombre de usuario, creación de horarios, actualización de la base de datos por un robot,...etc... SquidGuard funciona asociado al proxy Squid que nos va a permitir registrar las páginas web visitadas en ficheros .log y además hace de caché acelerando el acceso a las páginas visitadas recientemente.

Otra posibilidad de SquidGuard es limitar el acceso a Internet permitiendo únicamente ciertos dominios. Esto nos puede servir si tenemos un grupo de alumnos especialmente difícil pero que tiene que hacer uso puntual de Internet para hacer algo concreto.
Por ejemplo, en mi instituto los alumnos del grupo PAC van al aula 1 y necesitan Internet sólo para leer el correo electrónico en Hotmail. Sin embargo, aprovechan el menor descuido del profesor para navegar por otros sitios. Para limitar el acceso sólo al correo de Hotmail, debemos crear un grupo de direcciones que llamaremos, por ejemplo, únicas. Hay que señalar que para leer el correo de Hotmail, no sólo se debe dar acceso a hotmail.com sino también a otros dominios y direcciones IP asociados.

SquidGuard ofrece muchas posibilidades de configuración. Para otras opciones no explicadas en este artículo, existe una documentación bastante completa en la web de SquidGuard. De todas maneras, probablemente no convenga complicarse demasiado, ya que la gestión de actualizaciones, horarios,... puede llevar mucho tiempo.

Siguiendo a Díaz Guerra (1994) las redes las podemos clasificar en tres grandes grupos: de telefonía, redes de datos y redes de distribución de televisión. Aunque es una clasificación que obedece a criterios de origen de la señal y no de impacto en el usuario, nos clarifican el uso que de ellas puede hacer el docente, especial interés tendrán las redes de datos, que con potencia audiovisual permitirán al docente organizarlos y trabajar con ellos.

Dada la complejidad de la información que cada red tiene y tomando como referencia al menos las redes más conocidas: EARN (European Academic and Research Network), Internet, por su gran impacto internacional y la derivada del programa IRIS, nos proporcionan elementos para reflexionar sobre el desafío que el uso racional y frecuente de las mismas pueden tener para la formación del Profesorado.

Así en la Formación Inicial la propuesta de capacitación y construcción de conocimiento profesional ha de estar ligada a una nueva visión de la cultura pedagógica en la que integrar el uso y la elaboración creadora de las Nuevas Tecnologías en la práctica educativa, tal como hemos presentado en otros trabajos (Medina y Domínguez, 1989) (Rodríguez Diéguez y Sáez, 1995), en los que se evidencia la creación de un modelo de reflexión en el que incorporar el empleo innovador de los nuevos espacios telemáticos.

El empleo e integración de las nuevas tecnologías en la Formación Inicial y Permanente del Profesorado ha de realizarse de acuerdo con la concepción que de la formación del profesorado tengamos, gráficamente lo representamos:

El modelo que presentamos se apoya en las tres grandes aportaciones de los paradigmas consolidados en formación del profesorado, con toda su línea y procesos de investigación: Paradigma del Pensamiento del Profesorado, Paradigma de la indagación en la acción, Paradigma emergente de la Colaboración en las Instituciones educativas.

La formación tiende a consolidarse en conmitancia con el principio de Educación Permanente en la consolidación de una línea propia de Desarrollo Profesional, que sitúa a cada docente y equipo de colegas en un espacio de reflexión y mejora continua de las concepciones y actuaciones curriculares en el aula y centro.

La aportación más destacada es evidenciar que la formación tecnológica del Profesorado y su actualización permanente tiene sentido en la medida en que se coordina en una perspectiva más general y argumentada de los modelos y bases para formarnos con los docentes. La visión colaboración pone en el candelero que "los docentes poco pueden aprender de los asesores" si no se configura un espacio de diálogo y de indagación, en colaboración, que respetando los esquemas mentales de los docentes, sus múltiples habilidades profesionales (analítico-sintéticos, prácticos, creativos, etc.) y su estilo de enseñanza. El modelo pretende que la formación tecnológica en la comprensión, adaptación e integración de las redes en la formación del profesorado, en el intercambio habitual, tenga un primer eje: "La visión profesional y global" y desde ella incorporar a cada docente a su propia actualización profesional.

La incorporación sistemática y formativa de las redes a la actualización profesional es un camino complejo, que sólo puede desbrozarse si tenemos claro qué docente formamos y cuál es el lugar que en esta formación ha de alcanzar la cultura tecnológica y singularmente el uso de las redes? Tan compleja es esta integración, como necesaria, pero sobre todo hemos de partir del sentido virtual y de la aportación que la red puede tener para la actualización de cada docente.

Desde las perspectiva del pensamiento y construcción de teorías de enseñanza, la red ha de contribuir a resolver las siguientes necesidades de formación:

- Descubrir el valor intrínseco de la red, como espacio de comunicación, base de datos, lugar de encuentro de innovaciones, facilitación de las relaciones, etc.

- Valorar la actitud que tenemos ante la incorporación de un medio de estas características, estimando sus implicaciones en todo el proceso de enseñanza-aprendizaje y en un uso más innovador de todas las tecnologías a ella incorporada.

- Estimar el nivel de familiarización con la red, de sus posibilidades y limitaciones educativas, desde las cuales desarrollar la concepción y práctica educativa de cada docente.

- Adaptar la red a las necesidades actuales y futuras que vive cada docente en el centro y aulas.

- Seleccionar la información más pertinente con la concepción de enseñanza, los problemas vividos en las aulas y centros propuestos estime que la red puede apoyar.

- Ampliar las opciones personales y valorar los esquemas mentales que mantenemos en relación con el uso, adaptación y aprovechamiento de la red en nuestra vida profesional.

- Aprovechar la red para el contraste de nuestras concepciones e innovaciones educativas con otras aportaciones de equipos y colegas.

La red sirve a los docentes para profundizar en los procesos de disonancia, en el análisis de las concepciones educativas y en la valoración de las aportaciones de otros colegas a la concepción y práctica educativas.

Las redes incrementarán el contacto entre los docentes, profundizando y valorando las teorías, conceptos, habilidades, principios de la acción, etc., que caracterizan la práctica educativa, avanzándose en la diferenciación de cada equipo de docentes, pero a la vez en el afianzamiento de las concepciones y procesos formativos que cada docente va elaborando en la formación inicial y actualizando en la continua.

La red apoyará el pensamiento innovador al posibilitar una nueva comunicación ágil, multidireccional y contrastada con otros colegas, impulsando a los educadores a explicitar y compartir su concepción educativa. Este intercambio público, pero respetuoso con la intimidad de los participantes, incrementa el saber personal y hace posible que construyamos líneas fundamentadas de reflexión y acercamiento profesional.

El Paradigma del Pensamiento del Profesor, criticado por su limitación reduccionista, encuentra en la red un apoyo para la reflexión personal, para la consolidación del conocimiento profesional y para comprender, en interacción con otros colegas, las claves de su pensamiento y acción.

Pensar en voz alta, una exigencia del conocimiento compartido, será una demanda de la "comunicación por red", cada profesor y profesora podrá verter a la red los procesos de acción, sus concepciones, dudas y problemas de sus prácticas innovadoras, que permitirá que otros colegas los conozcan, sirviéndole para entender mejor su actuación en las aulas y centros. El equilibrio entre la explicitación de creencias, teorías, fundamentos y principios de la acción, etc., hace que se logre un proceso de formación bien construido, así al compartir las metáforas e imágenes, por ejemplo, que cada uno mantenemos de la actuación educativa se configura un espacio riguroso de saber educativo, de actitudes abiertas y de nuevos valores de sinceridad y humildad, que frente al aislamiento tradicional en el que nos movemos los docentes nos auxilia para ser el docente que necesitamos ser y consolidarnos como tal.

La dimensión Indagadora es la que encuentra en las redes su más directo apoyo, ya que como hemos adelantado, cada docente aprende de su práctica cuando cree en ella y busca continuamente las razones de sus acciones y las claves de los problemas que encuentra en su vida profesional con estudiantes, colegas y la sociedad en su conjunto.

Los centros educativos tenderán a ser espacios de relación y de intercomunicación, al emplear junto al concepto de aula de informática, "aulas abiertas al mundo, en las que además de las tareas propias y específicas de la instrucción del grupo, se abra diariamente la ventana al mundo, que nos posibilitan las redes". El s. XXI nos demanda un nuevo concepto del espacio, la comunicación y las relaciones humanas, a él hemos de tender y desde este nuevo estilo de acción nos hemos de plantear el sentido y la proyección de las acciones educativas. Cada red es una puerta abierta a innumerables puertas, aprendamos a abrir y no a cerrar tantas puertas.

Las redes según Salinas (1995) crean distintos espacios: "campus virtual", "campus electrónico", "campus en línea", que implican un nuevo modo de ver y vivir la aldea global en la que nos estamos situando. Cuáles serán las posibilidades en la próxima década 2.000? La imaginación y la creatividad se han de estimular ante estos retos, sin olvidar lo mucho que necesita avanzar el ser, como persona humana".

4.2 MARCO COCEPTUAL

4.2.1 Enlaces Privados

Los enlaces privados se caracterizan por brindar seguridad en la transmisión de datos de extremo a extremo. Se valen siempre de una red de transmisión (en algunos casos también existe una red de conmutación) para conectar las partes. Estos enlaces pueden ir desde los 9600bps (en el caso de una conexión conmutada usando un modem análogo de 9600bps) hasta el orden de los Gigabps (usando redes ópticas, con equipos de transporte de última generación o multiplexores DWDM).

4.2.2 Enlaces Dedicados

Los enlaces dedicados, como su nombre lo indica, son conexiones permanentes punto-punto, o punto-multipunto, que se valen de una infraestructura de transporte (Capa 1) o de transporte y conmutación (Capa 1 y 2). Los primeros son comúnmente llamados enlaces Clear Channel y los segundos son enlaces Frame Relay o ATM.

4.2.3 Enlaces Conmutados

Los enlaces conmutados se dividen en dos tipos: los análogos y los digitales. Los primeros llegan hasta ratas de 53 kbit/s para el downlink y hasta de 48 kbit/s para el uplink, los segundos transmiten y reciben a 64 kbit/s o 128 kbit/s. Estos últimos son conocidos como enlaces RDSI (o ISDN, en inglés) que son las siglas de Red Digital de Servicios Integrados.

4.2.3.1 Enlaces Conmutados Análogos

Fue quizá la primera tecnología de transmisión de datos que usó el hombre para construir redes privadas entre dos sitios remotos. Esto lo hizo aprovechando la Red de Telefonía Pública Conmutada – RTPC (PSTN, en inglés), dicha red ha tenido muchos desarrollos en los últimos 20 años. El servicio tradicional que la RTPC ha

prestado ha sido comunicación de voz, y solo recientemente se empezó a usar para soportar un creciente mercado de transferencia de datos.

El rango de frecuencia de la voz humana va desde los 20Hz hasta los 20Khz, pero casi toda la energía espectral se encuentra entre los 300Hz y 3.4Khz, por ende, la ITU ha definido un canal de voz (speech channel) para telefonía en esta banda. Por cuestiones prácticas, y para evitar efectos aliasing se maneja el canal desde los 0Hz hasta los 4KHz, dejando unos pocos Hz como bandas de guarda.

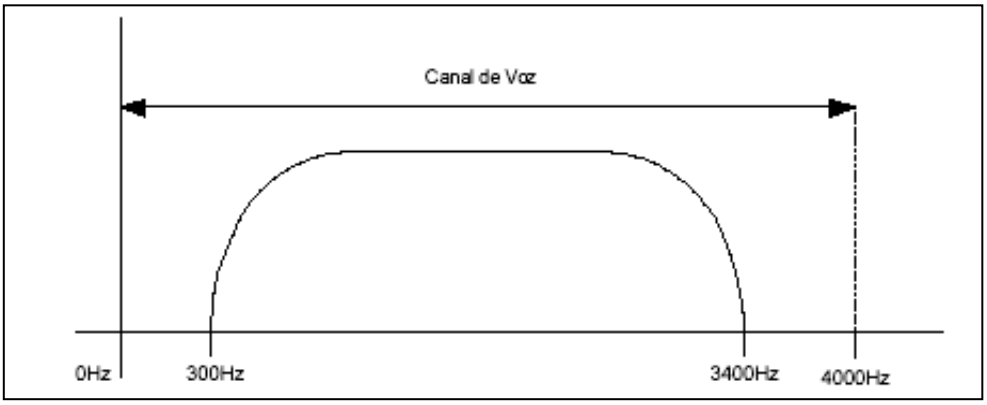


Figura 1. Ancho de banda de un Canal convencional de voz humana

De este criterio partió todo el desarrollo que se ha hecho sobre las redes de telefonía, todos los equipos fueron diseñados para transmitir señales en este rango. Las investigaciones que se hicieron en el campo de las comunicaciones han demostrado que transportar cualquier señal, incluso la voz, en formato digital tiene inmensas ventajas comparado con una transmisión análoga, de allí que nuestra voz sea convertida en una señal digital en las centrales telefónicas y transportada de la misma manera entre ellas.

4.2.3.2 Enlaces Conmutados Digitales – RDSI

RDSI o Red Digital de Servicios Integrados, es un sistema de telefonía digital que se desarrollo hace más de una década. Este sistema permite transmitir voz y datos simultáneamente a nivel global usando 100% conectividad digital.

En RDSI, la voz y los datos son transportados sobre canales B (del inglés Bearer) que poseen una velocidad de transmisión de datos de 64 kbit/s, aunque algunos switches ISDN limitan esta capacidad a solo 56 kbit/s. Los canales D (o canales de datos) se usan para señalización y tiene ratas de 16 kbit/s o 64 kbit/s dependiendo del tipo de servicio.

Los dos tipos básicos de servicio RDSI son: BRI (del inglés Basic Rate Interface) y PRI (del inglés Primary Rate Interface). Un enlace BRI consiste de dos canales B de 64 kbit/s y un canal D de 16 kbit/s para un total de 144 kbit/s. Este servicio está orientado a brindar capacidad de conexión para usuarios residenciales.
Un enlace PRI está orientado a usuarios que requieren un mayor ancho de banda. En Estados Unidos la estructura básica de canales es 23 canales B y 1 canal D, todos de 64 kbit/s, para un total de 1536 kbit/s. En Colombia donde se ha adoptado el estándar internacional de la ITU-T, y que además es el estándar ETSI europeo, un PRI consiste de 30 canales B y 2 canales D, todos de 64 kbit/s, para un total de 2048 kbit/s. Para accesar a un servicio BRI, es necesario tener una línea RDSI. Si solo se desean comunicaciones de voz es necesario tener teléfonos digitales RDSI, y para transmitir datos es necesario contar con un adaptador de Terminal – TA (del inglés Terminal Adapter) o un enrutador RDSI. La norma RDSI Colombia trabaja con interfaces BRI S/T, a diferencia de la americana que entrega en las premisas del usuario en interfaz BRI U. La figura 2 ilustra los diferentes tipos de interfaz y equipos terminales RDSI.

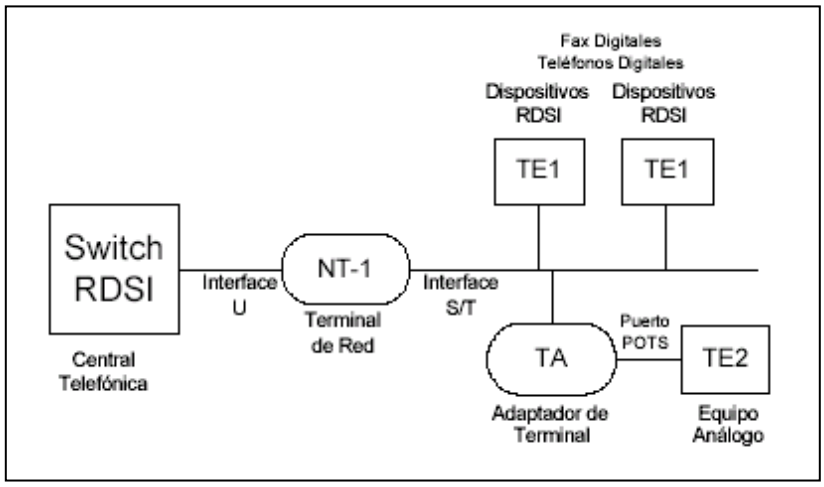


FIGURA 2. Diagrama de Interfaces y equipos en una conexión RDSI BRI

A diferencia de las conexiones conmutadas análogas en una conexión RDSI el camino es 100% digital desde la central hasta el sitio del abonado, por lo cual no existe ningún tipo de conversiones A/D o viceversa, lo que facilita la obtención de velocidades de 64 kbit/s o 128 kbit/s, lo cual se logra convirtiendo los dos canales B de 64 kbit/s o en un canal lógico de 128 kbit/s. Esta característica es usada solo en transmisión de datos y depende de la facilidad que tenga el equipo terminal de realizar esto. Típicamente esta característica tiene el nombre de Multilink. La tecnología RDSI no llega al municipio de Madrid.

4.2.4 ARQUITECTURAS VPN

4.2.4.1 INTRANET VPN LAN-TO-LAN

Tradicionalmente, para conectar dos o más oficinas remotas de una misma compañía se han necesitado contratar enlaces dedicados Clear Channels o Circuitos Virtuales Permanentes (PVCs) Frame Relay. Las empresas adoptan diferentes topologías de red WAN para interconectar todos sus sitios remotos, entre estas se encuentran: Enlaces punto-a-punto, de estrella, de malla parcial y de malla completa. Las figuras 3, 4, 5 y 6 detallan cada una de las topologías anteriormente mencionadas.

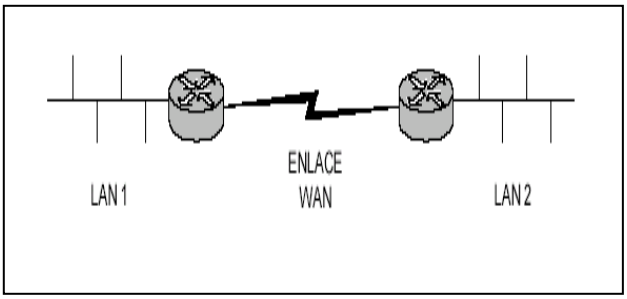


Figura 3. Enlace Punto a Punto

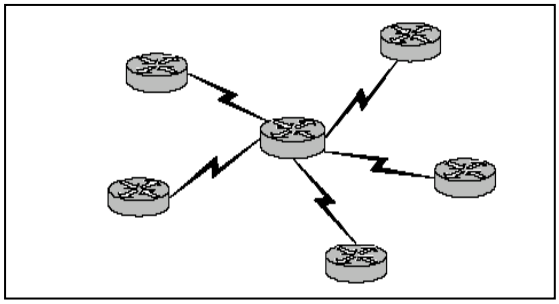


Figura 4. Topología Estrella

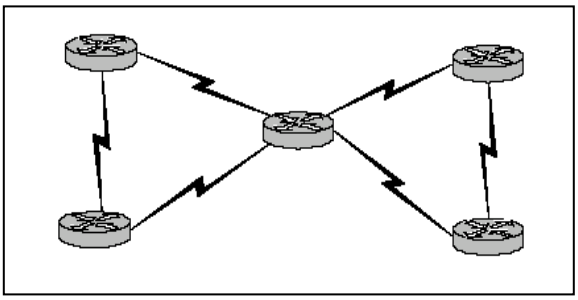


Figura 5. Topología de Malla Parcial

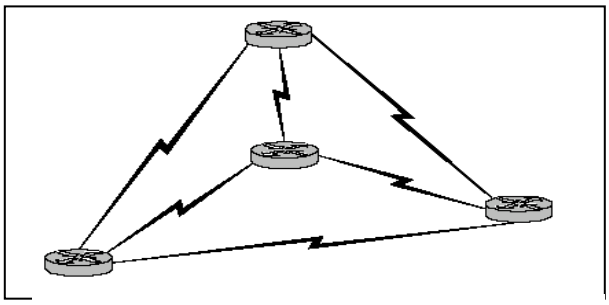


Figura 6. Topología de Malla Completa

En general, cuando se necesita concentrar tráfico en al menos un nodo, es preferible usar tecnologías como Frame Relay pues solo se necesita un último kilómetro por el cual viajan todos los PVCs contratados con el proveedor de servicio; pero económicamente sigue siendo igual de costosa porque las compañías que prestan el servicio de interconexión Frame Relay cobran por PVC activado, así usen la misma solución de último kilómetro. Si se observa bien, la mayoría de escenarios de enlaces WAN corporativos tienen más de dos nodos interconectados, por tanto habrá al menos un nodo donde existan al menos dos

PVCs compartiendo un último kilómetro, esto sería por ejemplo, en la topología de estrella. Si cambiamos a malla completa o parcial, el número de PVCs aumentará considerablemente y con ellos los costos de la solución de transporte de datos. En la figura 7. se observa con más detalle una solución Frame Relay usando topología de estrella.

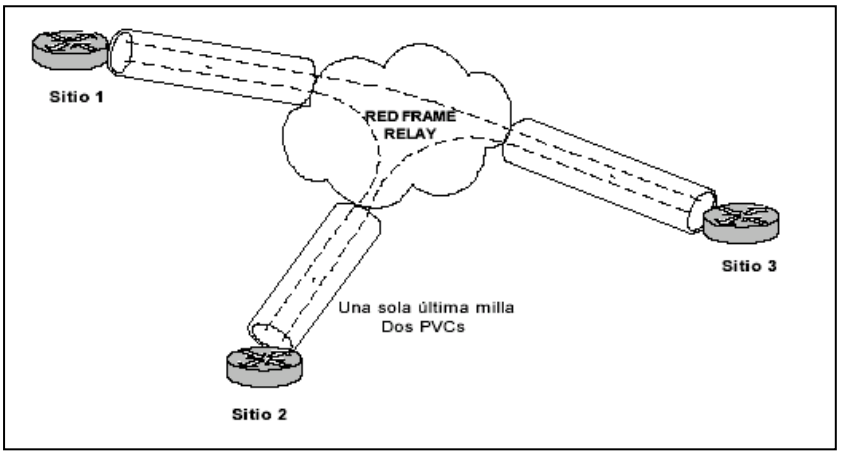


Figura 7. Detalle de 4 nodos en estrella con 2 PVCs

A parte del alto precio que tiene una solución Frame Relay o Clear Channel, hay otros factores a tener en cuenta para decidir cambiar este tipo de tecnologías a una solución usando VPNs, y son entre otras, la disponibilidad, la seguridad, la eficiencia en el manejo del ancho de banda y la amplia cobertura que ha logrado Internet.

La ventaja que han sustentado los tradicionales enlaces dedicados es la disponibilidad, sin embargo, estos enlaces también son susceptibles de caídas, y su montaje, en cuanto a hardware se refiere, es tan complejo que es prácticamente imposible cambiar a otro proveedor mientras el enlace se reestablece. Con un escenario LAN-to-LAN VPN, cuando un enlace a Internet de la ISP que le presta el servicio a la empresa que tiene montada la VPN se cae, la conmutación a otro proveedor es prácticamente transparente para la empresa, ya que el enrutador de frontera de la ISP (que sirve de gateway de toda la red) se encarga de seleccionar otro enlace que se encuentra arriba.[3]
La figura 8 ilustra la conexión de tres oficinas de una misma compañía usando una arquitectura LAN-to-LAN VPN. Nótese que los túneles VPN que aparecen señalados

[3] Para esto es necesario que el enrutador de frontera de la ISP que provee de Internet a la compañía que establece la VPN sea capaz de trabajar con protocolos de enrutamiento dinámicos como BGP o EIGRP, y que la ISP también cuente con enlaces de respaldo a Internet.

no son enlaces físicos sino lógicos que viajan por Internet. El único equipo que tiene que adquirir la compañía para cada oficina a conectar es un gateway VPN que tiene, por lo general, un puerto LAN (Ethernet o Fast Ethernet) para conectarse a la LAN Corporativa, y un puerto LAN o WAN para conectarse hacia la ISP. Muchos de estos gateways VPN trabajan como firewalls y tiene un switch 10/100 incorporado de 4 u 8 puertos, debido a esto son llamados dispositivos Todo en Uno.
Solo se necesita un último kilómetro por oficina, por ahí viajan todos los túneles VPN que se necesiten.

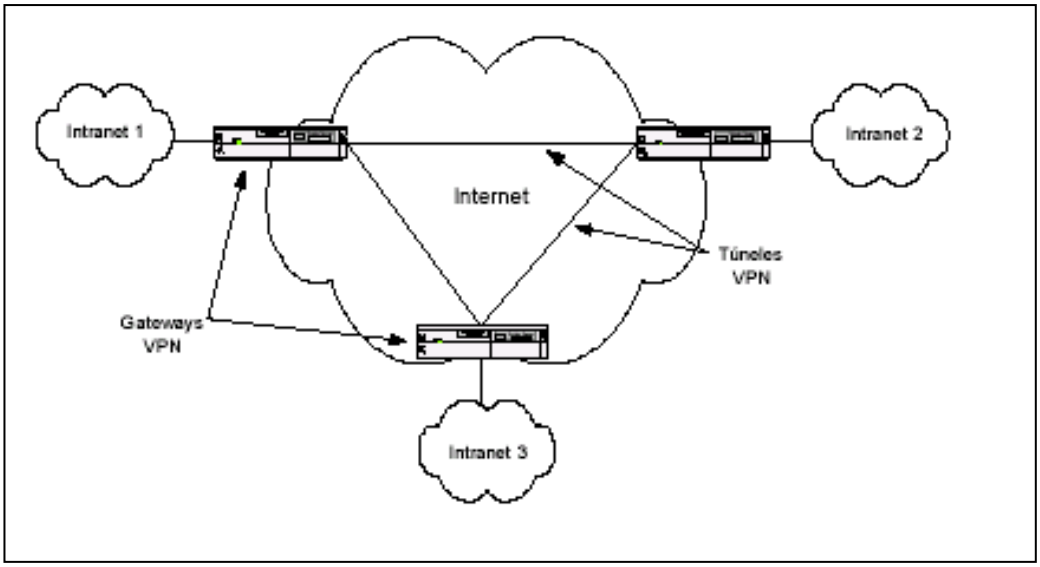


Figura 8. Esquema de una solución Intranet VPN (LAN-to–LAN VPN)

Si el enlace hacia Internet de la compañía no es dedicado sino conmutado, el mecanismo para cambiar de proveedor es mucho más sencillo, basta con configurar el gateway dial-up VPN con el número telefónico de otra ISP. Si se cuenta con un servicio de cable módem o ADSL solo se necesita conectar el cable de la otra ISP al CPE.

Con una arquitectura Intranet VPN (o LAN-to-LAN VPN) se puede lograr el mismo objetivo de interconectar dos o más sitios y a un costo mucho menor. La economía se ve reflejada tanto en equipos que se tienen que adquirir o arrendar para el montaje inicial de la topología, como en cargos fijos que se tienen que pagar mes a mes.
Otro factor decisivo que ha hecho que las empresas comiencen a ver en las VPNs otra opción para el montaje de sus redes WAN usando esta tecnología es la

aparición de los NAPs (o Puntos de acceso a la Red), que son lugares donde varias redes autónomas de sitios cercanos se conectan para intercambiar tráfico a alta velocidad, y así evitar que paquetes de información que se cruzan entre sitios en un mismo lugar geográfico tengan que ir hasta otros países o continentes, disminuyendo así los costos. En Colombia, el NAP más grande que existe es el NAP de la CCIT (Cámara Colombiana deInformática y Telecomunicaciones), también llamado NAP Colombia. La aparición de este NAP hizo que el tráfico que tenía como origen y destino nuestro país usara solo canales locales o nacionales, evitando así a las ISPs conectadas a este, tener que adquirir más ancho de banda internacional.

4.2.4.2 ACCESO REMOTO VPN

Fue la primera aplicación que se le dio a la emergente tecnología de las VPNs. Consiste en usar cualquier RAS que preste servicio de conexión a Internet como punto de acceso a una red corporativa también conectada a Internet por medio de un gateway VPN.

Esta solución nació de la necesidad de poder acceder a la red de una empresa desde cualquier ubicación, incluso a nivel mundial. Con el Acceso Remoto VPN, los RAS corporativos quedaron olvidados, pues su mantenimiento era costoso y además las conexiones que tenían que hacer los trabajadores de planta externa, como vendedores y personal de soporte técnico, cuando viajaban fuera de la ciudad, y más aun, a otros países eran demasiado costosas.

El acceso remoto VPN se vio claramente impulsado por el auge de la Internet que ha hecho que prácticamente en todas partes del mundo se obtenga fácil acceso a la misma.

La figura 9 muestra la creación de un túnel conmutado VPN usando un cliente PPTP instalado en el computador del trabajador remoto. Nótese que se realizan dos conexiones, una PPP a la ISP, y una PPTP al gateway VPN de la compañía que se encuentra conectado a Internet. La conexión PPP puede ser análoga o digital RDSI.

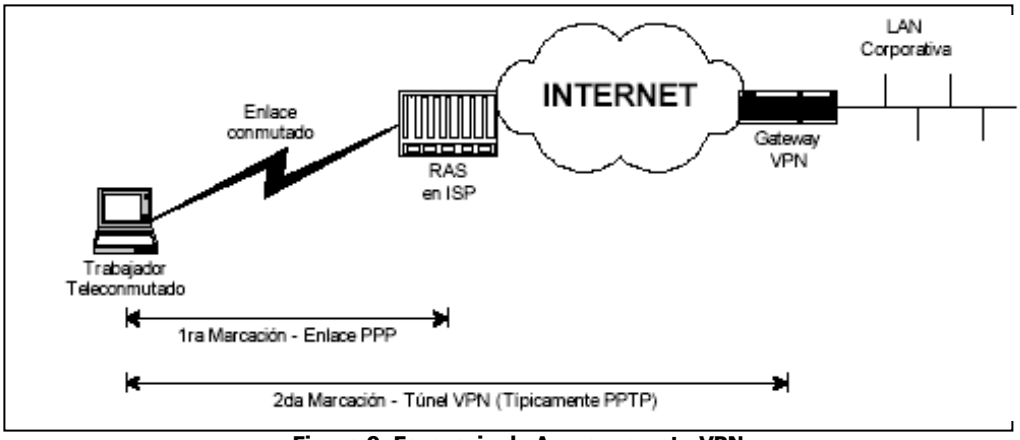


Figura 9. Escenario de Acceso remoto VPN.

Otra de las grandes ventajas del acceso remoto VPN sobre el tradicional acceso remoto es poder usar tecnologías de acceso de banda ancha como xDSL y cable módem. Para una empresa seria costoso e inconveniente tener un concentrador xDSL en sus instalaciones para permitirle a sus trabajadores teleconmutados el acceso a su red. Mientras que las VPNs usan la infraestructura existente de los proveedores del mercado para accesar a gran velocidad a la red corporativa.
El mejor intento de una empresa por tener su propia infraestructura de acceso tradicional (no VPN) sería montar un RAS con capacidad para recibir conexiones RDSI-BRI, es decir velocidades de 64 kbit/s o 128 kbit/s, además si la llamada la origina un trabajador en otra ciudad o país se tienen que sumar los cargos de esas llamadas.

La figura 10 ilustra dos tipos de accesos remotos VPN, uno de banda ancha, donde el usuario remoto que crea el túnel tiene una conexión cable módem (también aplica xDSL) hacia la ISP; y otro acceso por medio de un módem análogo común, en este caso el usuario remoto podría estar en otra ciudad o incluso en otro país.

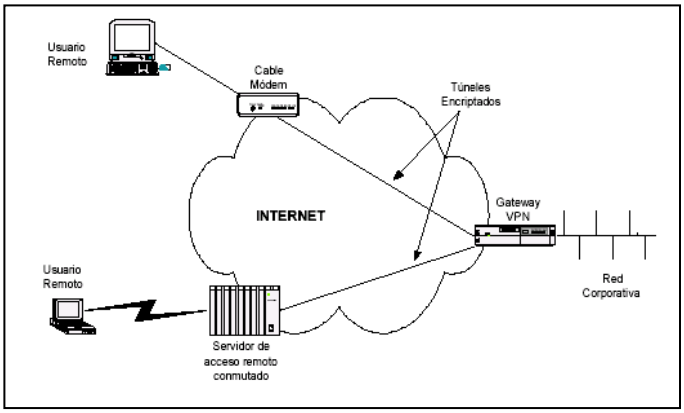


Figura 10. Dos Montajes típicos de un acceso remoto VPN.

4.2.4.3 EXTRANET VPN

Las empresas necesitan intercambiar información y realizar transacciones no solamente entre sitios de su misma organización sino también con otras compañías. Implementar una topología Extranet VPN implica incrementar la complejidad de los sistemas de control de acceso y de autenticación. Adicionalmente la tendencia de los mercados hacen que un cambio en la topología se pueda realizar fácilmente, para esto una Extranet VPN debe poder adicionar y eliminar dinámicamente acceso seguro a otras compañías.

Tal reconfiguración dinámica es difícil cuando se cuenta con circuitos cerrados dedicados. La presencia de una compañía en Internet y el uso de la arquitectura de Extranet VPN, hace posible crear conexiones dinámicas seguras a otras redes sin necesidad de cambiar la infraestructura física.

4.2.5 MODELOS DE ENTUNELAMIENTO

En las VPN los sitios de terminación (terminadores) de los túneles son aquellos donde se toman las decisiones de autenticación y las políticas de control de acceso y donde los servicios de seguridad son negociados y otorgados. En la práctica hay tres tipos posibles de servicios de seguridad que dependen de la ubicación de los terminadores. El primer caso es aquel donde el terminador está en el host mismo, donde los datos se originan y terminan.

En el segundo caso el terminador está en el gateway de la LAN corporativa donde todo el tráfico converge en un solo enlace. El tercer caso es aquel donde el terminador está localizado fuera de la red corporativa, es decir en un Punto de Presencia (POP) de la ISP.

Dado que un túnel VPN se compone de dos terminadores, se pueden obtener seis tipos de modelos de seguridad derivados de la posible combinación de las diferentes localizaciones: End-to-End, End-to-LAN, End-to-POP, LAN-to- LAN, LAN-to-POP y POP-to-POP, en la figura 11 se notan cada uno de ellos.

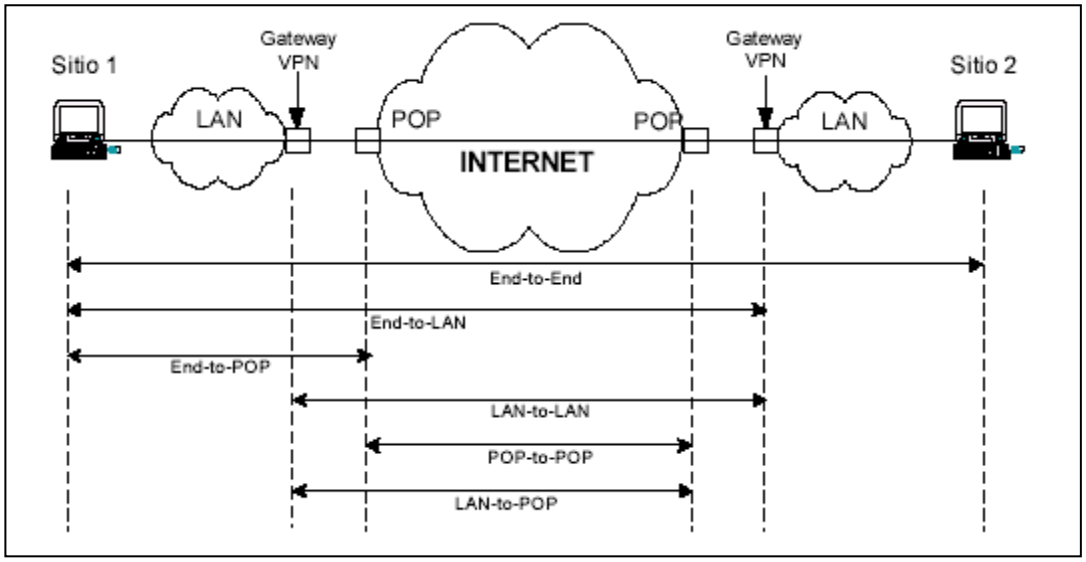


Figura 11. Modelos de entunelamiento VPN

En el modelo End-to-End el túnel va desde un extremo hasta el otro del sistema. Por lo tanto, los servicios de seguridad son negociados y obtenidos en la fuente y en el destino de la comunicación. Este escenario presenta el más alto nivel de seguridad dado que los datos siempre están seguros en todos los segmentos de la red, bien sea pública o privada. Sin embargo, el total de túneles que pueden haber en una empresa grande, dificulta el manejo de los servicios de seguridad requeridos por dichos host. Este modelo de seguridad es comúnmente visto en implementaciones de capas superiores, como es el caso de SSL (Secure Sockets Layer). Tales implementaciones no son consideradas como modelos de entunelamiento.

En el modelo End-to-LAN, el túnel comienza en un host y termina en el perímetro de Una LAN en la cual reside el host destino. Un dispositivo VPN localizado en el perímetro de la red es el responsable de la negociación y obtención de los servicios de seguridad de los host remotos. De esta manera, la seguridad de un gran número de dispositivos en una red corporativa puede ser manejada en un único punto, facilitando así la escalabilidad del mismo.

Dado que la red corporativa es considerada un sitio seguro, comúnmente no hay necesidad de encriptar la información que transita dentro de ella. La mayoría de implementaciones de acceso remoto VPN trabajan con este modelo.
El modelo de entunelamiento End-to-POP es aquel en el cual un host remoto termina el túnel en un POP de la ISP. Un dispositivo VPN o un equipo con

funciones de terminador VPN y que se encuentra en la red de la ISP es el responsable por la negociación y concesión de los servicios de seguridad. La entrega de los datos desde el POP hasta el host destino es por lo general asegurada con infraestructura física, la cual separa el tráfico del resto de la red pública. Por lo general en este caso el ISP administra los permisos y controla el acceso según las directivas de los administradores de red de las empresas clientes. La arquitectura de acceso remoto VPN también usa este modelo.

En el modelo LAN-to-LAN ambos hosts usan dispositivos VPNs situados en la frontera de la red corporativa para negociar y conceder servicios de seguridad. De esta manera, las funciones de seguridad no necesitan ser implementadas en los hosts finales donde los datos son generados y recibidos. La implementación de los servicios de seguridad es completamente transparente para los hosts. Esta implementación reduce drásticamente la complejidad en el manejo de las políticas de seguridad. La arquitectura Intranet VPN encaja en este modelo.

En el caso de LAN-to-POP el túnel comienza en un dispositivo VPN localizado en la frontera de la red corporativa y termina en un dispositivo VPN el cual se encuentra en un POP de la ISP. En la actualidad prácticamente este modelo de entunelamiento no es aplicado.

Finalmente, en el modelo POP-to-POP ambos dispositivos VPN son localizados en la propia red de la ISP. Por lo tanto los servicios de seguridad son completamente transparentes para los usuarios finales del túnel. Este modelo permite a los proveedores de servicio implementar valores agregados a los clientes sin que éstos alteren la infraestructura de sus redes.

De los seis modelos anteriores el End-to-LAN y el LAN-to-LAN son los más extensamente usados en las soluciones VPN. Sin embargo, el POP-to-POP o modelo de seguridad basado en red, ha cobrado vigencia últimamente dado que permite a las ISPs implementar servicios de valores agregados para sus clientes.

4.2.6 AUTENTICACIÓN

La autenticación es el acto de verificar la identidad de alguien o algo en un contexto definido. En un mundo de seis billones de personas no es suficiente simplemente declarar que se es quien se dice ser, se debe probarlo.
La autenticación involucra usualmente la interacción entre dos entidades: el objeto de la autenticación (un usuario o un cliente) que afirma su identidad y un

autenticador realizando la verificación de la identidad. El usuario entrega información de autenticación la cual incluye la identidad proclamada y la información que soporta dicha identidad al autenticador. En la labor de verificación, el autenticador aplica una función de autenticación F que le entrega información y luego compara el resultado de esta operación con el resultado esperado. Si el resultado de la función F concuerda con el resultado esperado, la identidad del usuario se considera verificada.

La información de autenticación puede ir desde un simple password a un juego completo de parámetros y mensajes. De igual manera, la función F puede ser una simple función como en el caso de la comparación de claves, o la aplicación de complejos algoritmos criptográficos, como en el caso de firmas digitales.

Si la información de autenticación y la función de autenticación F están totalmente bajo el control de las dos entidades, el esquema de autenticación es llamado Esquema de Autenticación Compartido (two-party). Sin embargo, en muchos casos es más seguro y escalable ayudarse de una tercera parte (o de más) para la autenticación. Esos esquemas son llamados de confianza en terceras partes (trusted third-party).

Otro factor a tener en cuenta es la integridad y confidencialidad de la información de autenticación. Es importante que la información usada para la autenticación sea segura y no sea obtenida de participantes no autorizados.

Esas medidas de seguridad no solo deben ser tomadas en el establecimiento del túnel, sino durante el transcurso del intercambio de datos. En el caso de las VPNs esto es muy importante ya que la información de autenticación es transmitida a través de Internet.

4.2.6.1. LAS AMENAZAS DE SEGURIDAD EN LAS REDES DE DATOS

En ambientes de redes la seguridad de los datos y las comunicaciones dependen de tres cosas: Autenticación, Confidencialidad e Integridad de Datos. La Autenticación significa que la persona o entidad con la cual se está comunicando es realmente quien dice ser. La Confidencialidad es asegurarse que alguien no autorizado pueda escuchar las comunicaciones, es decir, que nadie pueda entender los datos que han sido interceptados. De igual manera, la garantización de la integridad de los datos significa que ningún dato ha sido alterado en ninguna

parte de la transmisión. Desafortunadamente, el conjunto de protocolos TCP/IP no fueron diseñados originalmente para brindar seguridad a los datos. A continuación se describirán las amenazas de seguridad más comunes en redes públicas como Internet.

4.2.6.1.1 Spoofing

Las redes IP usan direcciones numéricas para cada dispositivo conectado a la misma. Las direcciones del host fuente y destino son incluidas en cada paquete trasmitido en una red IP, spoofing aprovecha este hecho y así un intruso puede usar alguna de esas direcciones IP y pretender ser el destinatario.

Después de que un intruso identifica una pareja de computadores, A y B por ejemplo, que están comunicándose uno con el otro como en una topología cliente – servidor, intenta establecer una conexión con el computador B de tal forma que B cree que está en una conexión con A, cuando en realidad la conexión se ha establecido con el computador del intruso.

El establecimiento de una conexión entre A y B implica un intercambio de mensajes de control, en estos mensajes de control tanto A como B envían sus direcciones de origen. Cuando A recibe un mensaje de B, B tiene que responder con un mensaje de reconocimiento el cual incluye una secuencia de números para garantizar el correcto orden en el recibo de los paquetes. Esas secuencias de números son únicas entre las dos máquinas.

Para completar la configuración de la sección entre A y B, B esperaría de A un reconocimiento en la secuencia de números de B antes de proceder con cualquier tipo de intercambio de operación. Pero para que un atacante se haga pasar como A el tendría que detectar la secuencia de números que B usará. Sabiendo lo anterior, no es muy difícil identificar las secuencias de números en una conexión entre dos hosts. De esta manera un atacante podría hacerse pasar como cualquiera de los dos hosts y así poder ganar privilegios no autorizados

4.2.6.1.2 Hijacking

Hijacking es una amenaza de seguridad que se vale del spoofing, pero ésta consiste en tomar una conexión existente entre dos computadores.
El primer paso en este tipo de ataques es tomar el control de un dispositivo de red LAN como un firewall que pueda monitorear la conexión. Una vez monitoreando el

enlace, el atacante puede determinar la secuencia de números usadas por ambas partes.

Después de hecho esto, el atacante puede generar tráfico que parezca venir de una de las partes envueltas en la comunicación, robando la sesión de los individuos envueltos. Como en spoofing, el atacante podría sobrecargar uno de los dos computadores con exceso de paquetes que haga que la sesión se caiga.

El hecho que un host haya identificado la persona con la cual se está comunicando no podría asegurar que desde ese mismo IP esté el host auténtico durante el resto de la sesión. Para esto se necesita de un esquema que autentique los datos durante toda la transmisión. Pero de igual forma, usando el método de autenticación más poderoso no podríamos prevenir 100% ataques por hijacking; en realidad la única defensa contra tales ataques es la implementación de mecanismos de encriptación.

4.2.6.1.3 Sniffing

Sniffing es un ataque que es posible hacer en redes donde el medio es compartido, tales como redes ethernet, donde generalmente, los paquetes están disponibles para todos los nodos en la red. Lo normal es que cada NIC (Tarjeta de interfaz de Red) solamente escuche y responda los paquetes que van direccionados específicamente para este. Sin embargo, es relativamente fácil colocar una NIC en modo promiscuo, es decir, que ellas pueden recolectar cada paquete que pasa por el cable. Estas NIC en modo promiscuo, no pueden ser detectadas por algún otro computador en la red, porque cuando escuchan paquetes no cambian absolutamente nada en ellos, simplemente los guardan.

Un tipo de software llamado sniffer puede aprovecharse de esta característica de la tecnología ethernet. Tal herramienta puede grabar todo el tráfico que pasa por el nodo. Los sniffer son necesarios para diagnosticar problemas en redes ethernet. Sin embargo, en manos de alguien que quiera escuchar comunicaciones privadas, un sniffer es una poderosa herramienta de olfateo. Por ejemplo, un atacante podría usar un sniffer para grabar todos los paquetes que contienen nombres de usuarios y claves en una red y luego usar esa información para entrar a sistemas para los cuales él no está autorizado a acceder.
Otro de los malos usos que se le puede dar a un sniffer es el de coleccionar datos y mensajes de una compañía para poder así identificar quien se comunica con

quien, qué se está comunicado y poder usar esta información en labores de espionaje corporativos.

Encriptar datos es una forma de proteger contra sniffing, aunque el atacante podría tener los recursos para guardar los datos encriptados y luego tratar de descifrarlos cuando esté desconectado. La inspección física de las redes es una buena forma de reducir los riesgos de sniffing. En algunos computadores como aquellos que corren sistema operativo Linux se puede chequear fácilmente si una NIC está en modo promiscuo.

4.2.6.1.4. Ataque del Hombre-en-la-Mitad

Aunque se ha dicho que usar tecnologías de cifrado y autenticación previenen en cierta medida de las amenazas en una red IP, el cifrado no es una solución del todo confiable. Los ataques de el hombre-en-lamitad son tendientes a burlar los sistemas de cifrado.

Para cifrar se debe primero intercambiar las llaves de cifrado. Pero es conveniente intercambiar dichas llaves con ciertas precauciones. Un intruso podría emplear técnicas de spoofing, hijacking y sniffing para capturar las llaves de cifrado que se intercambian en un sistema. El podría introducir su propia llave anticipadamente en el proceso y la otra persona podría creer que se está comunicando con la llave de la otra parte cuando en realidad esa llave es la conocida por el invasor. Este ataque es conocido como el-hombre-en-la-mitad.

4.2.6.2. SISTEMAS DE AUTENTICACIÓN

La autenticación es parte vital dentro de la estructura de seguridad de una VPN. Sin ella no se podría controlar el acceso a los recursos de la red corporativa y mantener a los usuarios no autorizados fuera de la línea. Los sistemas de autenticación pueden estar basados en uno de los siguientes tres atributos: algo que el usuario tiene (por ejemplo la llave de una puerta); algo que el usuario sabe (por ejemplo una clave); ó algo que el usuario es (por ejemplo sistemas de reconocimiento de voz ó barrido de retinas). Es generalmente aceptado el uso de un método sencillo de autenticación tal como el password, pero no es adecuado para proteger sistemas. Los expertos recomiendan los llamados sistemas de

autenticación complejos, los cuales usan al menos dos de los atributos de autenticación anteriores.

A continuación trataremos los sistemas de autenticación más comúnmente usados en los ambientes de redes: passwords tradicionales, passwords únicos, PAP, CHAP y Radius.

4.2.6.2.1. Passwords Tradicionales

Son la forma más simple de autenticar pero es un método inadecuado para garantizar la seguridad en el acceso a una red, dado que los passwords pueden ser adivinados e interceptados durante transmisiones en la red. Por ejemplo, servicios tales como FTP y Telnet transmiten los nombres y las claves en texto plano, haciéndolos fácilmente interceptables.

4.2.6.2.2. Passwords Únicos

Una forma de prevenir el uso no autorizado de Passwords interceptados es evitar que sean reutilizados. Los sistemas de Passwords Únicos restringen el uso de un password a una sola sesión de comunicación, es decir que se requiere un password nuevo para cada nueva sesión. Estos sistemas, de los cuales S/KEY es el mejor ejemplo, facilitan al usuario la escogencia de un nuevo password para la siguiente sesión generando automáticamente una lista de posibles passwords para el usuario.

S/KEY usa un password secreto encriptado generado por el usuario, para crear la secuencia de passwords únicos. El password del usuario nunca atraviesa la red, por lo tanto dicho password no es sujeto de ataques. Con esto se logra que los passwords únicos que son generados por esta clave y que pudieron ser interceptados para luego ser utilizados no le sirvan al atacante.

El primer password único es producido aplicando al mensaje original una función HASH n veces, donde n es un número especificado por el usuario. El siguiente password único es generado aplicando al mensaje original la misma función HASH n-1 veces y así sucesivamente hasta generar n passwords únicos.

Cuando un usuario intenta entrar a la red el servidor de red en el cual está habilitado el S/KEY genera una respuesta que consiste de un número y una cadena de caracteres, la cual es llamada seed.

En respuesta al mensaje enviado por el servidor de red el usuario usa el número y el seed que le ha llegado más su propio password secreto en un software generador S/KEY que corre en su computador. Este software se encarga de combinar los tres elementos y de iterarlos tantas veces como el número que le ha llegado en el mensaje de respuesta del servidor.

El password único resultante es enviado al servidor de autenticación el cual también lo itera tantas veces como el se lo haya indicado al cliente en funciones HASH, luego lo compara con el password único que tenía almacenado. Si hay una concordancia entre los mismos al usuario se le permite el ingreso a la red, una vez esto pasa el número n es decrementado y el siguiente password único es guardado para el siguiente intento de ingreso.

Los sistemas de passwords únicos como el S/KEY requieren que el software del servidor sea modificado para realizar los cálculos requeridos y que cada computador remoto tenga una copia de un software cliente. Estos sistemas no son muy escalables dado que se dificulta administrar listas de passwords para un gran número de usuarios.

4.2.6.2.3. PAP (Password Authentication Protocol)

PAP o Protocolo de Autenticación de Passwords fue diseñado originalmente como una manera sencilla para que un computador se autenticara en otro cuando los mismos usan un protocolo de comunicación punto a punto como PPP. PAP es un protocolo de dos vías, el host que se está conectando envía un nombre de usuario y un password al sistema destino con el cual trata de establecer su comunicación, y el sistema destino (el autenticador) responde si es el caso, que el computador remoto está autenticado y aprueba su comunicación.

PAP es un protocolo de autenticación que puede ser usado al comienzo del establecimiento de un enlace PPP, o bien durante el transcurso de la sesión PPP para reautenticar el enlace.

PAP no es seguro porque la información de autenticación es transmitida en texto plano, esto hace vulnerable a que atacantes obtengan información de nombres de usuario y claves de manera fácil.

4.2.6.2.4. CHAP (Challenge Handshake Authentication Protocol)

CHAP es muy similar a PAP pero es más seguro para autenticar enlaces PPP. CHAP es un protocolo de tres vías y al igual que PAP, puede ser usado al comienzo de un enlace PPP y ser repetido cuando el enlace ya se haya establecido.

CHAP incorpora tres pasos para la autenticación de un enlace, que son:

1. El autenticador envía un mensaje al nodo remoto.
2. El nodo calcula un valor usando una función HASH y lo envía de regreso al autenticador.
3. El autenticador avala la conexión si la respuesta concuerda con el valor esperado.

El proceso puede repetirse en cualquier momento del enlace PPP para asegurarse que la conexión no ha sido tomada por otro nodo. A diferencia de PAP, en CHAP el servidor controla la reautenticación. PAP y CHAP tienen algunas desventajas, en ninguno de los dos se pueden asignar diferentes privilegios para acceder a la red a diferentes usuarios remotos que usan el mismo computador. El siguiente protocolo (Radius) entrega más flexibilidad para asignar privilegios de acceso.

4.2.6.2.5. RADIUS (Remote Authentication Dial-In User Service)

El protocolo del Servicio del usuario de marcación de autenticación remota (RADIUS) es un método popular para administrar la autenticación y autorización de usuarios remotos. El RADIUS es un protocolo muy ligero, basado en UDP, fue desarrollado por Livingston Enterprise, ahora una división de Lucent Technologies.

RADIUS usa una arquitectura cliente – servidor e incluye dos componentes: un servidor de autenticación y un protocolo cliente. El servidor es instalado en un computador central, el protocolo cliente es implementado en el servidor de acceso a la red (NAS).

El proceso de autenticación con RADIUS tiene los siguientes pasos:

1. Un usuario remoto marca a un RAS. Cuando la conexión al MODEM se completa, el RAS pregunta por un nombre de usuario y password.

2. Una vez recibido el nombre de usuario y el password, el RAS crea un paquete de datos llamado requerimiento de autenticación. Este paquete incluye información tales como el nombre del usuario, el password, el modem de conexión, entre otros. Para evitar que un hacker escuche la información, el RAS actúa como un cliente del RADIUS, cifrando el mensaje con una clave compartida predeterminada entre el RAS y el servidor RADIUS.

3. El requerimiento de autenticación es enviado por la red desde el cliente hasta el servidor RADIUS. Esta comunicación puede ser hecha sobre una red de área local o global. Si el servidor RADIUS no puede ser alcanzado, el cliente RADIUS puede rutear el requerimiento a un servidor alternativo.

4. Cuando un requerimiento de autenticación es recibido, el servidor RADIUS valida el requerimiento y verifica la información del nombre de usuario y password. Esta información también puede ser transmitida a un sistema de seguridad apropiado que soporte los archivos de autenticación, por lo general bases de datos.

5. Si el nombre de usuario y el password son correctos, el servidor envía un reconocimiento de autenticación que puede incluir información del usuario en la red y los servicios que el requiere. Por ejemplo, el RADIUS le puede decir al NAS que el usuario requiere una dirección IP estática o que obtiene su dirección IP de un rango dinámico de direcciones, también puede contener información sobre los filtros que pueden limitar al usuario a accesar ciertos recursos específicos de la red como por ejemplo el uso de un servidor proxy.

6. Si en este punto del proceso la autenticación no se tiene éxito, el RADIUS envía un mensaje de desconexión al RAS y al usuario se le niega el acceso a la red.

De la misma manera que un RAS y un servidor RADIUS usan claves compartidas, dos servidores RADIUS en modo proxy usan otra clave compartida para proteger la comunicación entre ellos. La figura 12 muestra un esquema de RADIUS en modo proxy, muy utilizado para hacer roaming entre distintas ISPs.

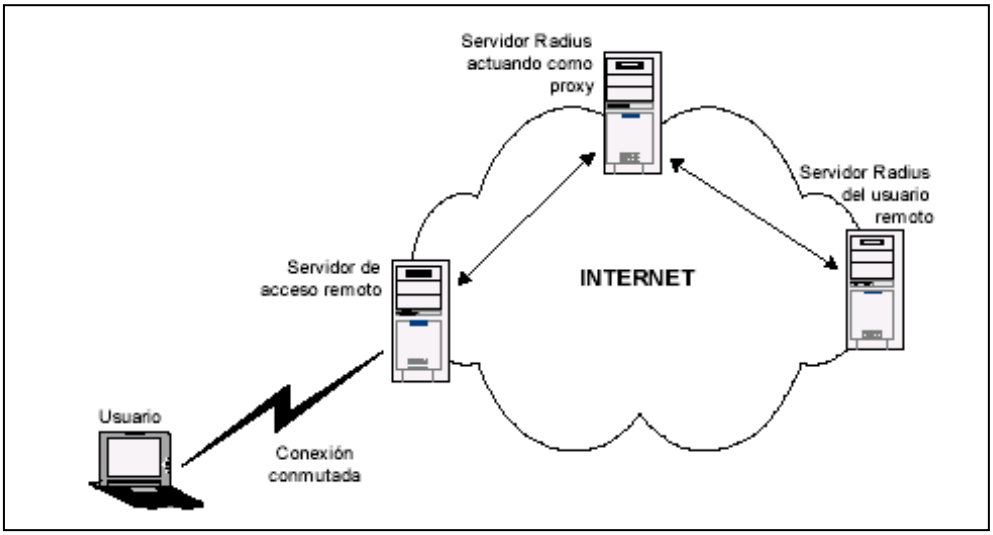


Figura 12. Autenticación RADIUS usando un servidor proxy

4.2.7. CIFRADO

En una tarea de cifrado, el emisor y el receptor, deben conocer el conjunto de reglas que rigen el mecanismo como tal. Las llaves son usadas para transformar la información original en una resultante llamada texto cifrado. Como ambas partes conocen el cifrado, cualquiera de ellas puede reversar el proceso para abstraer el texto original.

El cifrado se basa en dos componentes: un algoritmo y una llave. Un algoritmo criptográfico es una función matemática que combina texto plano o cualquier otra información inteligible con una cadena de dígitos llamada key (llave) para producir un texto cifrado o no inteligible. Tanto la llave como el algoritmo son cruciales en un proceso de cifrado.

El cifrado basado en un sistema de llaves ofrece una gran ventaja, los algoritmos criptográficos son difíciles de idear por lo cual sería traumático usar un nuevo algoritmo cada vez que una parte se quiera comunicar de manera privada con una nueva. Usando una llave, un usuario podría utilizar el mismo algoritmo para comunicarse con diferentes usuarios remotos; y todo lo que se debería hacer sería utilizar una diferente llave con cada uno de ellos.

El número de llaves posibles que tiene cada algoritmo depende del número de bits de la llave. El número de posibles llaves viene dado por la fórmula 2n, donde n es el número de bits de la llave. Por ejemplo, una llave de 64 bits permite 264 posibles combinaciones numéricas o llaves. Es decir, 18'446.744'073.709'551.616 claves. El gran número de posibles claves dificulta los ataques de fuerza bruta en donde se examinan todas las posibles combinaciones. Por lo tanto la fortaleza del cifrado depende de la longitud de la llave.

El sistema basado en llaves es llamado "de llaves secretas" o "cifrado simétrico". En este esquema tanto el emisor como el receptor poseen la misma llave para encriptar o desencriptar los datos. Pero con el tiempo el cifrado simétrico presentó algunos problemas, por ejemplo: ambas partes deberían de estar de acuerdo para usar la misma llave. Otro problema es que si una parte tenía n receptores, entonces debería guardar registro de n llaves secretas, una por cada uno de los receptores.

Otro gran problema del esquema de cifrado simétrico es con la autenticación, dado que la identidad del emisor que envía el mensaje al emisor no puede ser probada. Esto se debe a que tanto el emisor como el receptor poseen la misma llave, es decir, cualquiera de ellos puede crear y encriptar un mensaje y decir que la otra persona se lo envió. La manera de resolver este inconveniente es usando un esquema llamado "criptografía de llaves públicas", el cual hace uso de algoritmos de cifrado asimétricos.

4.2.7.1. CRIPTOGRAFÍA DE LLAVES PÚBLICAS

La criptografía de llaves públicas se basa en el manejo de una pareja de llaves. Cada llave puede encriptar información que sólo la otra puede desencriptar. La llave privada, únicamente es conocida por su propietario; la llave pública, se pública abiertamente, pero sigue asociada al propietario. Los pares de llaves tienen una característica única: los datos encriptados con una llave sólo pueden desencriptarse con la otra llave del par. En otras palabras, no tiene importancia que se use la llave privada o la pública para encriptar un mensaje, ya que el receptor puede usar la otra llave para desencriptarlo.

Las llaves se pueden usar de dos maneras diferentes: para garantizar confidencialidad al mensaje y para probar la autenticidad del emisor de un mensaje. En el primer caso, el emisor usa la llave pública del receptor para

encriptar un mensaje, de manera que el mensaje continúe siendo confidencial hasta que sea decodificado por el receptor con la llave privada. En el segundo caso, el emisor encripta un mensaje usando la llave privada, una llave a la cual sólo tiene acceso él. La llave pública del receptor asegura la confidencialidad; la llave privada del emisor verifica la identidad del mismo. Por ejemplo, para crear un mensaje confidencial, una persona necesita conocer primero la llave pública de su receptor, después deberá usar la misma para encriptar el mensaje y enviarlo. Como el mensaje se encriptó con la llave pública del receptor, sólo éste con su llave privada puede desencriptar el mensaje.

Aunque una persona puede encriptar un mensaje con una llave pública o con una llave secreta, usar la llave pública presenta ciertas ventajas. Por ejemplo, la llave pública de la pareja de llaves se puede distribuir en un servidor sin temor de que esto comprometa el uso de la llave privada. Por ello, no se necesita enviar una copia de la llave pública a todos los receptores; ya que ellos la pueden obtener desde un servidor de llaves mantenido por la compañía, o a través de un proveedor de servicio. La figura 13 muestra el esquema con el cual un emisor encripta su mensaje por medio de la llave pública del destinatario y como este último con su llave privada desencripta el mensaje cifrado que le ha llegado.

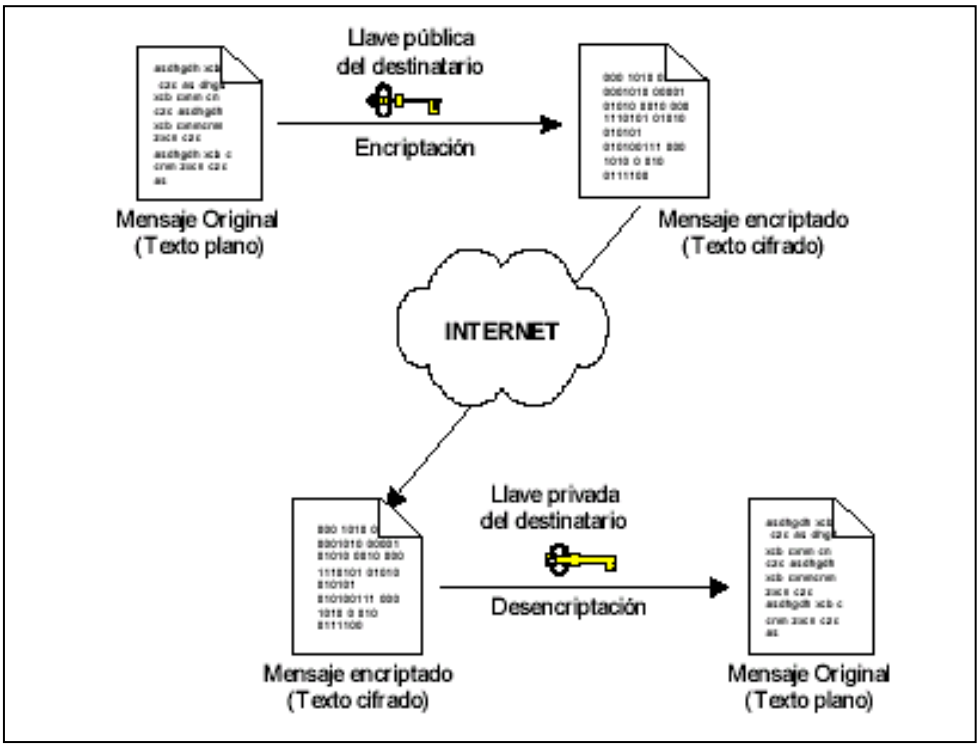


Figura 13. Esquema de cifrado con llaves públicas

Colocar una llave pública en una red la vuelve fácilmente accesible, y no se pone en peligro la llave privada correspondiente.

Otra ventaja de la criptografía con llave pública es que permite que el receptor autentifique al originador del mensaje. La idea básica es esta: ya que el emisor es la única persona que puede encriptar algo con su llave privada, todo aquel que use la llave pública del mismo para desencriptar el mensaje, puede estar seguro de que el mensaje proviene de él. Así, el uso de su llave privada en un documento electrónico es similar a la firma en un documento de papel. Pero hay que recordar que aunque el receptor puede estar seguro de que el mensaje proviene del emisor, no hay forma de garantizar que alguien más lo haya leído con anterioridad.

Usar algoritmos criptográficos de llaves públicas para encriptar mensajes es computacionalmente lento, así que se ha descubierto una manera para generar con rapidez una representación corta y única del mensaje, llamada "resumen" (message digest), que se puede encriptar y después usar como firma digital.

Algunos algoritmos criptográficos populares y veloces para generar resúmenes se conocen como funciones de dispersión (hash) de un solo sentido. Una función de dispersión (hash) de un solo sentido no usa una llave; simplemente es una fórmula para convertir un mensaje de cualquier longitud en una sola cadena de dígitos, llamada "resumen". Cuando se usa una función de dispersión (hash) de 16 bits, el texto procesado con dicha función produciría 16 bits de salida (un mensaje podría dar como resultado la cadena CBBV235ndsAG3D67, por ejemplo). Cada mensaje produce un resumen de mensaje al azar. Para obtener una firma digital solo basta con encriptar dicho resumen con su llave privada.

Por ejemplo, suponiendo que el emisor, A, calcula un resumen para un mensaje, y encripta dicho resumen con su llave privada, luego envía esa firma digital junto con un mensaje de texto simple a B.

Después de que B usa la llave pública de A para desencriptar la firma digital, B tiene una copia del resumen del mensaje que A calculó. Dado que B pudo desencriptar la firma digital con la llave pública de A, sabe que A lo creó, autentificando así al originador. B usa entonces la misma función de dispersión (que se acordó de antemano) para calcular su propio resumen del mensaje de texto simple de A. Si su valor calculado y el que A envió son iguales, entonces B puede estar seguro de que la firma digital es auténtica, lo que significa que A no sólo envió el mensaje, sino que el mensaje no fue alterado.

4.2.7.2. DOS ALGORITMOS IMPORTANTES DE LLAVES PÚBLICAS

Existe un amplia variedad de algoritmos criptográficos para llaves públicas, pero quizá dos de los más importantes han sido: Diffie-Hellman y RSA.

4.2.7.2.1 Diffie-Hellman

El protocolo Diffie-Hellman, también llamado (protocolo de acuerdo de llaves exponenciales) fue desarrollado por Whitfield Diffie y Martin Hellman en 1976 y ublicado en el magazín "Nuevas directrices en Criptografía" (aunque se tienen evidencias de haber sido previamente inventado por Malcom Williamson en 1974).

El protocolo Diffie-Hellman permite a dos usuarios intercambiar una llave secreta sobre un medio inseguro sin tener acuerdos preestablecidos.

Diffie-Hellman no se usa para encriptar datos, como se piensa generalmente. Se usa para intercambiar de forma segura las llaves que encriptan los datos. Esto lo logra generando un "secreto compartido", también llamado "llave de cifrado de la llave" (key encryption key – en inglés) entre las dos partes. Este secreto compartido luego encripta la llave simétrica (usando DES, 3DES, CAST, IDEA, Blowfish, etc.) que asegura la transmisión.

Los sistemas de llaves asimétricas (la base de la infraestructura de llaves públicas) usan dos llaves –la llave privada y la llave pública-, desafortunadamente estos sistemas tornan lenta la transmisión de datos. Lo práctico hoy en día, es usar un sistema simétrico para encriptar los datos y un sistema asimétrico para cifrar las llaves a usar en el proceso de cifrado de los datos.

Inicialmente, cada lado de la comunicación tiene su llave privada y la llave pública del otro lado. Diffie-Hellman tiene la capacidad de generar llaves compartidas idénticamente iguales en ambos lados de la comunicación con la llave privada local y la llave pública del lado remoto.

4.2.7.2.2. RSA

RSA es un sistema de cifrado de llaves públicas que se usa tanto para cifrado de datos como para autenticación de llaves públicas. Fue inventado por Ronald **R**ivest, Adi **S**hamir y Leonard **A**dleman en 1977. De las iniciales del apellido de sus creadores **RSA** tomó su nombre.

4.2.8. INFRAESTRUCTURA DE LLAVES PÚBLICAS

El comercio electrónico y la transmisión de datos privados sobre Internet ha crecido vertiginosamente, por tanto la autenticación ha cobrado un papel crucial en este proceso. La criptografía de llaves públicas ofrecen una gran herramienta matemática para facilitar la autenticidad, pero surge un gran problema y es el cómo manejar y publicar dichas llaves para cada persona o entidad que las necesiten.

Una infraestructura de llaves públicas (Public Key Infrastructure - PKI) es el conjunto de servicios y políticas que rigen el esquema de vinculación de una identidad con una llave pública y la posterior redistribución de ese vínculo.
Una PKI tiene tres procesos básicos: certificación, validación y la revocación de certificados. La certificación es la vinculación de una identidad a una llave pública. La llave pública y la identidad o atributos son puestos dentro de una documento digital llamado certificado. Un tercer participante confiable firma el certificado digitalmente, dando fe de la validez del contenido. El tercer participante en una PKI es llamado una Autoridad de Certificación (CA).

La validación es el proceso de comprobar la autenticidad del certificado, por tanto de asegurar que el contenido del mismo es confiable. Esto requiere la verificación de la firma del CA usando la llave pública del mismo y chequeando el certificado contra una lista de revocación de certificados (CRL).

Una CRL contiene una lista de certificados que han sido revocados anteriormente por la CA indicando que ese vínculo no es válido. La validación también involucra chequear el periodo de validez contenido en el certificado mismo.

La revocación de un certificado es el proceso de desconocer un certificado previamente emitido antes de su fecha de expiración. Estos suceden cuando algunos aspectos de la información contenidos en el certificado cambian; quizás porque la identidad del suario ha cambiado o porque la llave privada del usuario ha sido comprometida. El CA es responsable de emitir una CRL actualizada.

Un aspecto fundamental de las PKI es el grado de confianza que deposita en las CAs. Sin tal confianza los certificados digitales emitidos por cada CA perderían valor.

4.2.8.1 Arquitectura De Una Infraestructura De Llaves Públicas

Una PKI incluye la autoridad certificadora (CA) y todos los otros componentes que permiten la certificación, validación y revocación. La figura 14 muestra los principales componentes de una PKI: El usuario, el validador, la autoridad de registro RA, la autoridad de certificación CA, el certificado y un depósito de CRLs. Todos estos componentes interactúan para facilitar la adquisición y uso de certificados digitales.

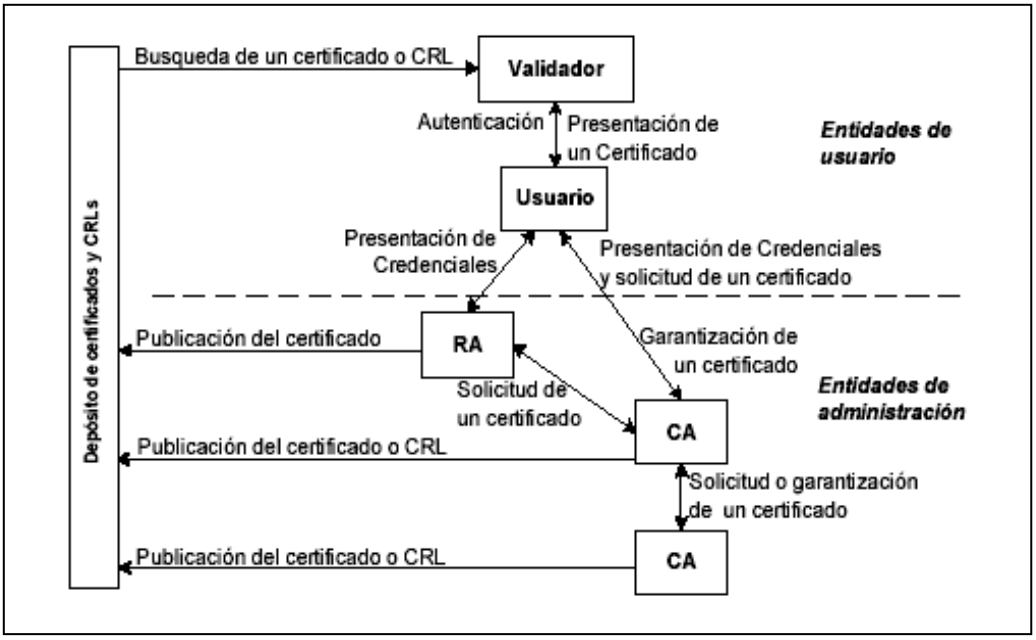


FIGURA 14. Arquitectura de una Infraestructura de llaves públicas.

Las CAs, las RAs y el depósito de CRLs son entidades de manejo o administración dado que ellos son responsables de la generación, distribución, almacenamiento y revocación de certificados digitales. Los usuarios y los validadores son entidades de usuario dado que ellos usan los certificados y las funciones de la PKI para lograr sus propósitos. Las entidades de usuarios realizan requerimientos a las entidades de manejo, bien sea para adquirir un certificado o validar alguno que haya presentado otra entidad de usuario.

Después que las credenciales son certificadas y verificadas, un certificado es emitido al usuario y publicado en el depósito. Cuando un validador necesita autenticar un usuario, usa la llave pública válida contenida en el certificado para verificar un mensaje firmado por la llave privada del usuario. Las CAs también

publican las CRLs en el depósito, por tanto el validador puede chequear si el certificado del usuario es todavía válido.

Las CRLs también pueden ser recibidas periódicamente sin necesidad de alguna petición. Un conjunto de protocolos ha sido desarrollados y estandarizados para administrar las diferentes transacciones entre todas las entidades.

4.2.8.2. Certificación

La certificación es el proceso de vincular un usuario con su información. Para asegurar la autenticidad e integridad de tal vínculo, la CA firma el documento usando su llave privada. El proceso de certificación toma varios pasos. Primero, el CA debe verificar que la información contenida en el certificado digital es auténtica y precisa. Esto implica un cierto nivel de seguridad en el canal que se usa para hacer este requerimiento y un especial cuidado del personal autorizado para insertar la información de la entidad dentro de un certificado. En algunas ocasiones la parte que entra la información no es el usuario a certificar.

El siguiente paso es la generación del par de llaves. La llave pública del usuario deberá ser incluida en el certificado. Algunas veces el usuario genera el par de llaves y pasa solamente la llave pública a la CA, por tanto solo él conoce su llave privada. Después, la CA firma el certificado con su llave privada. Esto tiene dos objetivos: Que el certificado sea garantizado por la CA y que la integridad del certificado sea protegida.

Después que el certificado digital es creado y firmado por la CA, el usuario puede recuperarlo desde ella. El proceso de recuperación del certificado comienza con la presentación de una credencial por una única y primera vez a la CA, usualmente es un número de referencia y un código de autorización dado al usuario por otro medio (preferiblemente seguro). En algunos casos es tan simple como un e-mail que envía la CA al usuario.

4.2.8.3. Validación

Un certificado debe ser validado antes de poder ser usado para brindar confiabilidad, la validación del certificado comprende los siguientes pasos:

1. La integridad del certificado es chequeada verificando la firma digital por medio de la llave pública de la CA.
2. El intervalo de validación del certificado digital es chequeado.
3. La CRL de la CA es chequeada para asegurarse que el certificado no ha sido rechazado.

4.2.8.4. Revocación Del Certificado

Un certificado puede ser revocado antes de su fecha de expiración si pierde su validez de alguna manera, por ejemplo cuando la longitud de la información contenida en el no es válida. Así como con el proceso de certificación, el requerimiento para revocar un certificado deberá ser recibido por medio de un canal seguro y examinado detenidamente.

La CA revoca un certificado incluyéndolo en la lista de certificados revocados o CRL (Certificate Revocation List). Una CRL usualmente contiene solo los números seriales de los certificados revocados. La inclusión de toda la información de los certificados revocados dentro de la CRL resultaría innecesaria y de un tamaño de archivo muy grande. La CA garantiza la integridad de la CRL firmando la misma con su propia llave privada. La CA da a conocer la CRL publicándola en su depósito. LA CRL es actualizada frecuentemente (por ejemplo cada ocho horas). La entidad de validación puede realizar un requerimiento de la CRL actualizada cuando la misma en su posesión ha expirado.
En algunas ocasiones la CA proactivamente entrega su CRL a las entidades de validación más grandes cuando una nueva revocación ha sucedido, de esta manera el efecto se torna inmediato.

4.2.8.5. Formatos De Certificados Digitales

Un certificado digital, como ya se había dicho anteriormente, vincula la identidad de una entidad a su llave pública. La autenticidad de la información es garantizada por la firma digital de la CA emisora. Varios estándares describen la información que debe estar contenida en el certificado, cómo debe ser organizada dentro del mismo y cómo se firma el certificado. Entre los formatos más usados se encuentran el X.509 y el PGP.

4.2.8.6. Certificado X.509

La X.509 define los lineamientos de los certificados de llaves públicas, incluyen una especificación de los certificados usados para vincular un nombre con una llave pública, y una especificación de revocación para los certificados emitidos que no sean confiables. El estándar X.509 no especifica una infraestructura de llaves públicas (PKI) en su totalidad, solo provee las bases sobre las cuales una PKI puede ser construida.
X.509 define el formato de certificados de llaves públicas más ampliamente usado. La primera versión, X.509v1 fue publicada en 1988 y provee la estructura básica del certificado. X.509v2 apareció en 1993 y le adicionó a la primera versión dos campos opcionales para proveer de unicidad al certificado en cuanto a su emisor y sujeto. La tercera y actual versión, X.509v3 fue publicada en 1997 con extensiones opcionales que ayudan a personalizar el formato del certificado para varias aplicaciones.

Un certificado digital X.509 es un documento firmado que garantiza el vínculo de un nombre y una llave pública, por lo tanto, debe contener al menos un nombre y una llave pública.

4.2.8.7. Certificados PGP

Otro formato de certificados ampliamente usados es el conocido como PGP (Pretty Good Privacy). Un certificado PGP incluye la siguiente información:

- Versión PGP: Este campo identifica que versión de PGP fue usada para crear la llave asociada con el certificado.
- La llave pública del portador del certificado y su algoritmo: Esta es la parte pública de la pareja de llaves con el algoritmo de la llave: RSA, DH (Diffie-Hellman) o DSA (Digital Signature Algorithm).
- Información del portador del certificado: Este consiste de la información sobre el usuario tal como su nombre, su identificación (user ID), etc.
- La firma digital del propietario del certificado: También llamada autofirma. Es la firma usando la correspondiente llave privada de la llave pública asociada con el certificado.
- El periodo de validez del certificado: Incluye la fecha y hora de inicio del certificado y la fecha y hora de expiración del mismo.
- El algoritmo de cifrado simétrico preferido para la llave: Este indica el algoritmo de cifrado que el propietario del certificado prefiere para que su

información sea encriptada. Los algoritmos soportados son CAST, IDEA y 3DES

Un certificado PGP es construido de un número de registros etiquetados llamados paquetes

Este certificado PGP consiste de cinco paquetes: un paquete de llave pública, un paquete de identificación de usuario, un paquete de firma, un paquete de subllave pública y otro paquete de firma. Cada uno de estos paquetes está constituido de varios campos, como por ejemplo el algoritmo que se usó para encriptar la llave (algo), la fecha de creación del certificado (created, en formato UTC, es decir el número de segundos transcurridos desde el 1 de Enero de 1970), la fecha en la que el certificado expira (expires), etc.

4.2.9. SISTEMAS DE ADMINISTRACIÓN DE CERTIFICADOS

La interacción de todos los componentes de una PKI que manejan la creación, renovación, mantenimiento y revocación de certificados digitales es conocida como el Sistema de Administración de Certificados (Certificate Management System). Esos componentes incluyen:

- Autoridad de certificación
- Autoridad de registro
- Depósito de certificados y CRL

Algunas veces todos los tres componentes residen en el mismo computador.

4.2.9.1. Autoridad De Certificación (CA)

La CA es la entidad que emite y revoca los certificados, entre sus funciones están:

- Creación y administración de las llaves públicas y privadas de la propia CA
- Creación de parejas de llaves públicas y privadas para los usuarios que así las necesitan.
- Creación de un certificado vinculando la llave pública del usuario a la identidad del mismo.
- Revocación de certificados.
- Creación de la lista de certificados revocados.
- Administración de una base de datos de información segura donde reside la historia de los certificados emitidos y revocados.

- Manejo de un completo registro (log) de mensajes para propósitos de auditoría.

4.2.9.2. Autoridad de Registro (RA)

Una CA es responsable de dos cosas: La verificación de la información del usuario y la emisión del certificado. La emisión de un certificado requiere acceso a la llave privada de la CA para que ella misma lo firme. Lo ideal es mantener la llave privada de la CA en un pequeño número de sitios. La verificación de la información de un usuario, el requerimiento de un certificado, la generación de la llave y el almacenamiento de la misma, son aspectos que hace la CA sin requerir accesar la llave privada del usuario. Uno o más autoridades de registro (RA) son empleadas para realizar estas funciones. Una CA puede tener muchas RAs estratégicamente localizadas para proveer una alta disponibilidad. Dado que la población de usuarios crece continuamente, más y más RAs deben ser adicionadas para mantener estable el nivel de servicio.

Una desventaja obvia de tener más y más RAs es que se incrementa la complejidad del mantenimiento de la seguridad; ya que cada RA debe ser certificada por la CA y debe comunicarse con la misma y con las otras RAs que tienen que ver con la verificación y revocación de los certificados que ella maneja.

4.2.10. CONTROL DE ACCESO

El control de acceso es un conjunto de políticas y mecanismos que permiten a las partes acceso autorizado a determinados recursos. De esta manera protege al recurso de accesos maliciosos o accidentales de usuarios que no están autorizados a accederlos.
La figura 15 muestra un control de acceso en un modelo cliente-servidor. Se considera usuario a cualquier entidad (usuario o aplicación trabajando en nombre de ese usuario) que desee acceder al recurso. Se determina por recurso a cualquier objeto que puede ser manipulado de alguna manera, tales como lectura, escritura o modificación, ausadas por la realización de alguna acción, tales como la ejecución de un programa o el envío de un mensaje.

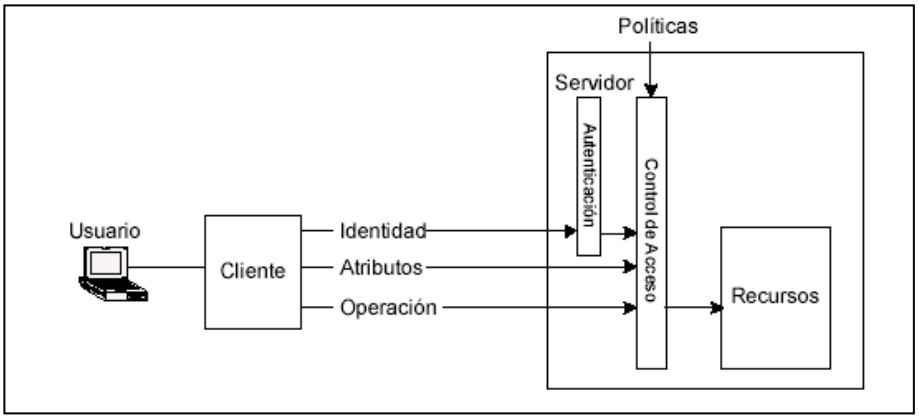


Figura 15. Control de acceso en un modelo Cliente-servidor.

Un usuario tiene una identidad y un conjunto de atributos asociados. El cliente envía la identificación del usuario, los atributos y el requerimiento de una operación al servidor. El servidor puede autenticar la identidad del usuario y remitirlo junto con los atributos y el requerimiento solicitado a los mecanismos de control de acceso. Las políticas son preestablecidas en el mecanismo de control de acceso; la información del usuario es comparada con las reglas de las políticas para determinar los derechos de acceso del usuario a ese recurso.

4.2.10.1. POLÍTICAS DE CONTROL DE ACCESO

Una política de control de acceso es el conjunto de reglas que definen la protección de uno o más recursos. Esas reglas son generalmente expresadas en términos de la información del usuario (atributos) y las condiciones para el uso de un recurso (atributos del recurso y otros factores del entorno).

En general hay dos tipos de políticas de control de acceso, las discrecionales y las mandatarias. El control de acceso discrecional permite al dueño del recurso determinar qué derechos de acceso son garantizados y a quienes. Un ejemplo son los permisos que se le pueden colocar a un archivo. Las empresas u organizaciones especifican control de acceso mandatario. Un ejemplo de este es el control de acceso que fijan las entidades militares.

4.2.10.2. REGLAS DE CONTROL DE ACCESO

Las políticas de control de acceso representan los deseos de las entidades que dicen ser dueñas o ejercen influencia sobre el recurso. En general, las políticas de

control de acceso son reglas que comparan la información del usuario y las condiciones del entorno con las condiciones del recurso para ser usado.

En general, las reglas de control de acceso son expresadas como un juego de condiciones de concordancia basadas en los atributos del usuario, los atributos del recurso y las condiciones del entorno. Una regla por defecto se usa para negar acceso diferente al que ha sido permitido por las reglas específicas.

Por lo general el orden de las reglas no interesa, pero es recomendable organizarlas de la más específica a la más general.

4.2.10.3. MECANISMOS DE CONTROL DE ACCESO

Los mecanismos de control de acceso son las formas concretas para expresar una regla. Las listas de control de acceso y las listas de capacidades son dos de los mecanismos más usados para especificar las reglas condicionales.

4.2.10.3.1. Listas De Control De Acceso

Una ACL (Access Control List) asocia cada recurso con una lista ordenada de qué usuarios pueden tener acceso al recurso y cómo esos usuarios pueden accederlo. Este método es de recurso céntrico; dando el nombre del recurso, del usuario, los atributos del mismo y el tipo de operación, el mecanismo de control de acceso puede buscar la ACL correspondiente a ese recurso y determinar si el usuario puede o no realizar la operación. Los usuarios en algunas ocasiones son puestos en grupos o en clases equivalentes, las cuales tienen los mismos derechos. Esta práctica tiene como objetivo volver más escalables las ACLs dependiendo del número de usuarios en el sistema.

El sistema de archivos UNIX usa una forma de ACL para permitir o denegar las operaciones que pueden ser hechas en los archivos. Hay tres tipos de operaciones básicas: lectura, escritura y ejecución. Cada archivo tiene asociados tres juegos de permisos: uno para el propietario del archivo, uno para el grupo y uno para cualquier otra persona. Cada permiso contiene los tres derechos: lectura (R), escritura (W) y ejecución (X); los derechos que no son garantizados se llenan con un guión (-). Los tres conjuntos con los tres privilegios forman una cadena de nueve dígitos (rwxrwxrwx).

El control de acceso en un firewall es otro ejemplo de como las ACLs son usadas. Generalmente un firewall es ubicado en los límites entre una Intranet e Internet. El firewall, por lo tanto, tiene dos interfaces: una con una dirección IP externa generalmente pública, y otra interfaz con una dirección interna (generalmente privada). El firewall implementa políticas de control de acceso para proteger los recursos de la Intranet de accesos maliciosos y mal intencionados.

La primera regla permite que desde Internet haya tráfico hacia cualquier host de la Intranet usando el puerto 80 (trafico http), la segunda regla permite el tráfico de protocolo ssh desde Internet usando el puerto 22, la tercera regla permite el tráfico por el puerto 23, usado para conexiones telnet desde Internet. La primera linea del ejemplo sirve para definir la variable $oif usada por las reglas del firewall y hace referencia a una tarjeta adaptadora de interfaz donde esta conectado un cablemodem que provee la conexión a Internet.

4.2.10.3.2. Listas de Capacidades

Las listas de capacidades (C-list) son equivalentes a las ACLs pero son centradas en el usuario a diferencia de las ACLs que son centradas en el recurso. En una C-list cada usuario tiene una lista de recursos que puede acceder.
Una C-list es usada si los recursos pueden ser agrupados en clases equivalentes, por ejemplo en la clasificación de seguridad militar, donde un documento puede ser marcado como: no clasificado, secreto o supersecreto.

La gran desventaja de usar una C-list es la dificultad de determinar todos los usuarios que tienen derechos de acceso a un recurso en particular. Como todos los usuarios tienen acceso al recurso, cada uno de ellos pueden hacer cambios sobre este, consecuentemente revocar o modificar los derechos de acceso en un recurso debiera requerir cambiar de rango a ese usuario o promover un rango superior a los demás.

4.2.10.4 ADMINISTRACIÓN DE LAS POLÍTICAS DE CONTROL DE ACCESO

Las políticas de control de acceso usualmente son dinámicas, es decir que nuevas políticas deben ser aplicadas cada vez que nuevos recursos o nuevos usuarios aparecen en la red. El proceso de crear, mantener y distribuir las políticas de control de acceso es llamado administración de las políticas de control de acceso.

Una administradora de políticas es la entidad que tiene el control sobre todas las políticas de acceso en un sistema. El manejador de las políticas es el servicio responsable de proveer a los administradores de una interfaz fácil de usar que defina, instale, modifique y despliegue políticas. El manejador de políticas también es el encargado de traducir las reglas del lenguaje abstracto que maneja el administrador a expresiones que son usadas en los mecanismos de control de acceso.
Cuando múltiples puntos de control de acceso existen en una red, la administración de las políticas puede ser hecha de una manera centralizada o de una manera distribuida.

4.2.10.4.1. Administración de políticas distribuidas

Una administración de políticas distribuidas es mostrada en la figura 16, el administrador de políticas usa los manejadores de políticas que se encuentran cerca o en los puntos a asegurar. Cuando una política es creada, actualizada o borrada, el administrador contacta al manejador asociado con ese recurso, y son éstos últimos los
encargados de almacenar las políticas internamente. Cuando una decisión de control de acceso debe ser tomada, el recurso asegurado le pregunta al respectivo manejador encargado de sus políticas. Este manejador está usualmente muy cercano, o inclusive localizado en el recurso mismo.

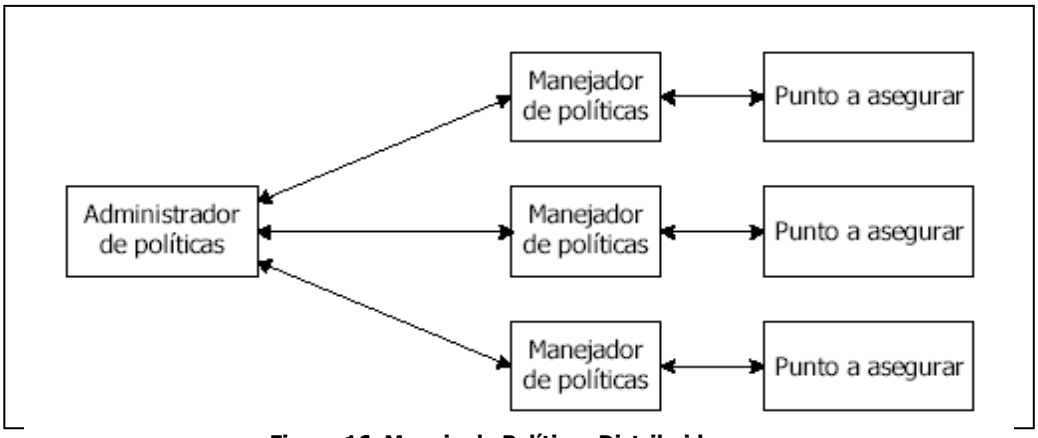


Figura 16. Manejo de Políticas Distribuidas

La administración de políticas distribuidas permite que las decisiones de control de acceso sean hechas de una manera más rápida, ya que el manejador está cercano al punto asegurado. Dado que las políticas no viajan a través de la red para cada

decisión, son menos susceptibles de ataques tales como la introducción de falsas políticas o la alteración de las mismas.

La desventaja de este sistema distribuido se centra en la consistencia. Dado que en un ambiente de redes los puntos a asegurar pueden interactuar con múltiples entidades, las políticas deberían ser creadas y mantenidas en varios manejadores. Si la seguridad de alguno de estos manejadores es violentada, el control de acceso del sistema global puede ser comprometido.

4.2.10.4.2. Administración centralizada de políticas

A diferencia de la administración de política distribuida, la administración centralizada tiene solo un depósito central de políticas.

Cuando el administrador de políticas debe crear, actualizar o borrar una política, solo tiene que contactar a un solo manejador, el cual a su vez almacena la política en el depósito central. Dicho depósito central de políticas puede estar cerca o inclusive ser parte del mismo manejador de políticas. Cada punto a asegurar obtiene sus políticas de control de acceso desde el depósito central a través de protocolos de intercambios de políticas estandarizados o propietarios.

Una ventaja de este sistema es la facilidad de uso para el administrador de políticas ya que contacta solo a un manejador. También es fácil mantener la consistencia de todos los recursos. La desventaja de este sistema es la latencia en la que se puede incurrir cuando los puntos a asegurar están alejados del depósito central.

Realizar un caché de éstas políticas en sitios cercanos a los puntos a asegurar resuelve el problema de la latencia, pero puede crear potenciales problemas de inconsistencias dado que debe transcurrir un tiempo de actualización cuando en el depósito central es cambiada una política. Otro problema que se puede presentar es que éstos caches multiplican la posibilidad de ser sujetos de ataques.

En la figura 17 se muestran todos los componentes que intervienen en el manejo centralizado de políticas y la relación entre cada uno de ellos.

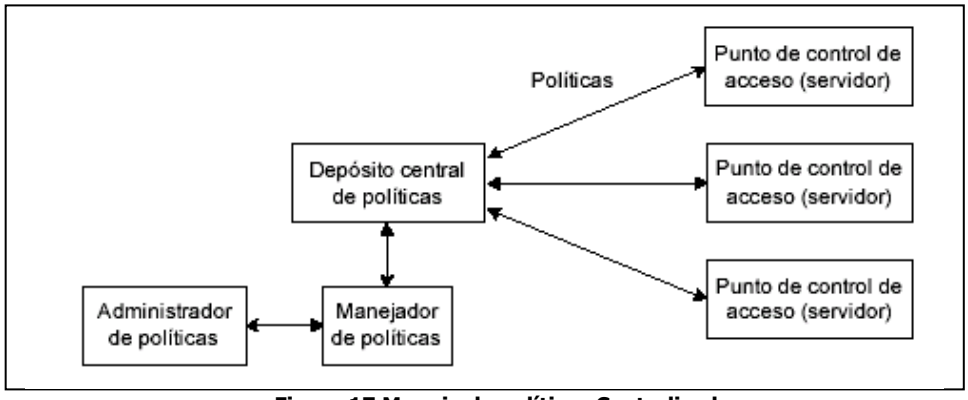


Figura 17.Manejo de políticas Centralizadas

4.2.11 TECNOLOGÍAS VPN

Básicamente, y desde el punto de vista de la torre OSI, se puede crear una VPN usando tecnologías de capa 2 (enlace de datos) y de capa 3 (red). Dentro de la primera categoría están PPTP y L2TP, y en la segunda se encuentra IPSec. MPLS tiene características de las dos al ser una red conmutada que usa etiquetas para enrutar paquetes. A continuación trataremos las tecnologías VPN más conocidas, y que técnicamente presentan las mejores características de seguridad, rendimiento, facilidad y economía.

4.2.11.1. PPTP (Point-to-Point Tunneling Protocol)

Es quizá el protocolo más sencillo de entunelamiento de paquetes. Es usado, en general, por pequeñas empresas para realizar sus VPNs LAN-to-LAN, y en topologías de acceso remoto, para trabajadores teleconmutados (teleworkers), tales como vendedores externos o trabajadores que se mantienen en constante movimiento por fuera de sus oficinas. El protocolo PPTP fue propuesto por el Foro PPTP (PPTP Forum), compuesto por 3Com, Ascend (ahora Lucent), Microsoft, ECI Telematics y USRobotics.

Debido a la integración que hizo Microsoft en sus sistemas operativos Windows NT, y luego en Windows98 y posteriores, PPTP tuvo gran acogida en el mercado mundial, a tal punto que un protocolo de capa 2 lanzado por Cisco Systems al mismo tiempo, prácticamente no se conoció, L2F (Layer-2- Forwarding)

El protocolo más comúnmente usado para acceso conmutado a Internet es el protocolo punto-a-punto (PPP). PPTP se soporta sobre toda la funcionalidad que PPP le brinda a un acceso conmutado para construir sus túneles a través de Internet. PPTP encapsula paquetes PPP usando una versión modificada del Protocolo de Encapsulamiento Ruteado Genérico (GRE – Generic Routing Encapsulation) Dado lo anterior, PPTP no solo es capaz de encapsular paquetes IP, sino IPX y NETBEUI, los protocolos de red local más usados. La figura 18 muestra una conexión PPP entre un host y un RAS. Como se puede ver, es una conexión sencilla punto a punto donde lo primero que se realiza es una autenticación sencilla previa al envío y recibo de tramas PPP de datos.

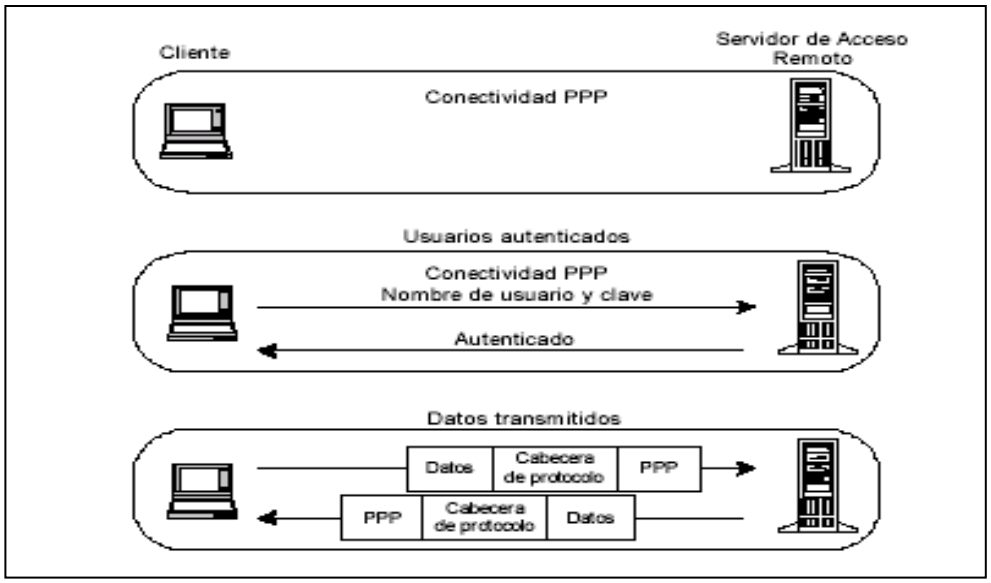


Figura 18. Conexión PPP típica entre un host y un RAS

Una de las ventajas que tiene PPTP por ser un protocolo de nivel 2, es que puede transmitir protocolos diferentes a IP en sus túneles, a diferencia de IPSec que se restringe a trabajar solamente con paquetes IP.

4.2.11.2. RELACION ENTRE PPP Y PPTP

PPP es el protocolo más comúnmente usado para acceso a Internet, prácticamente el único[4], además es usado en algunos enlaces seriales punto a punto WAN. PPP trabaja en la capa 2 de la torre OSI, la capa de enlace de datos, e incluye métodos

[4] Otro protocolo de comunicación serial es SLIP pero prácticamente ha desaparecido.

para encapsular varios tipos de datagramas para ser transferidos sobre enlaces seriales. PPP tiene dos juegos de protocolos: el Protocolo de Control de Enlace (LCP) que se encarga de las labores de establecimiento, configuración y prueba de la conexión y una serie de Protocolos de Control de Red (NCPs) para el establecimiento y configuración de los diferentes protocolos de capa 3.

PPP es capaz de encapsular paquetes IP, IPX y NETBEUI en tramas PPP y enviar estos paquetes encapsulados de extremo a extremo (entre dos computadores por ejemplo). Para el establecimiento de una comunicación, cada extremo de un enlace PPP primero envía paquetes LCP para configurar y probar el enlace de datos; cuando un enlace PPP ha sido establecido, el usuario es usualmente autenticado[5]. La autenticación es un paso previo para comenzar la fase de control de protocolos de red. En PPP, la autenticación puede ser implementada con PAP o CHAP. Cabe resaltar que PAP envía las claves a través del enlace en texto plano, mientras que CHAP es un protocolo de autenticación un poco más robusto ya que el usuario interactúa con el sistema autenticador respondiendo acertadamente a un requerimiento de desafío (challenge) al host remoto, estos sistemas de autenticación son llamados de tres vías.

Después de que el enlace ha sido establecido y varias opciones han sido negociadas por el protocolo LCP, PPP envía paquetes LCP para escoger y configurar uno o más protocolos de capa de red. Después de que cada uno de los protocolos de capa de red han sido configurados, los datagramas de cada uno de ellos pueden ser enviados sobre el enlace.

PPTP depende del protocolo PPP para crear la conexión conmutada entre el cliente y el servidor de acceso a la red. PPTP confía las siguientes funciones a PPP:

- Establecimiento y finalización de la conexión física
- Autenticación de los usuarios
- Creación de datagramas PPP

Luego que el enlace PPP es creado, el protocolo PPTP define dos diferentes tipos de paquetes: paquetes de control y paquetes de datos, cada uno de los cuales es asignado a diferentes canales lógicos. PPTP separa los canales de control y de datos usando un flujo de control que corre sobre TCP y un flujo de datos que está encapsulado con cabeceras IP usando GRE. La conexión TCP es creada entre el cliente y el servidor PPTP. Esta conexión es usada para intercambiar mensajes de

control. Los paquetes de datos contienen los datos del usuario, es decir, los datagramas del protocolo de capa de red usado. Los paquetes de control son enviados periódicamente para indagar sobre el estado del enlace y las señales de manejo entre el cliente y el servidor PPTP. Los paquetes de control también se usan para enviar información de manejo básica del dispositivo y de configuración. Los mensajes de control establecen, mantienen y finalizan un túnel PPTP.
Después de que el túnel PPTP se ha establecido, los datos del usuario son transmitidos entre el cliente y el servidor PPTP. Estos datos son transmitidos en datagramas IP contenidos dentro de los paquetes PPP.

Los datagramas IP son creados usando una versión modificada del protocolo GRE (Generic Routing Encapsulation); esta modificación consiste en incluir un identificador de los host que puede ser usado para controlar los privilegios de acceso y la capacidad de reconocimiento, la cual es usada para monitorear la rata de transferencia a la cual los paquetes están transmitiéndose en el túnel.

La cabecera GRE es usada para encapsular el paquete PPP dentro del datagrama IP. La información útil del paquete (Payload) es esencialmente el paquete PPP original enviado por el cliente. Dado que PPTP opera con un protocolo de capa 2, debe incluir una cabecera que depende del medio en el cual el túnel está transmitiendo, esta puede ser Ethernet, Frame Relay o PPP. La figura 19 muestra la estructura en los diferentes sitios de un túnel de un paquete IP usando encapsulacion PPTP desde el sistema cliente hasta la LAN corporativa.

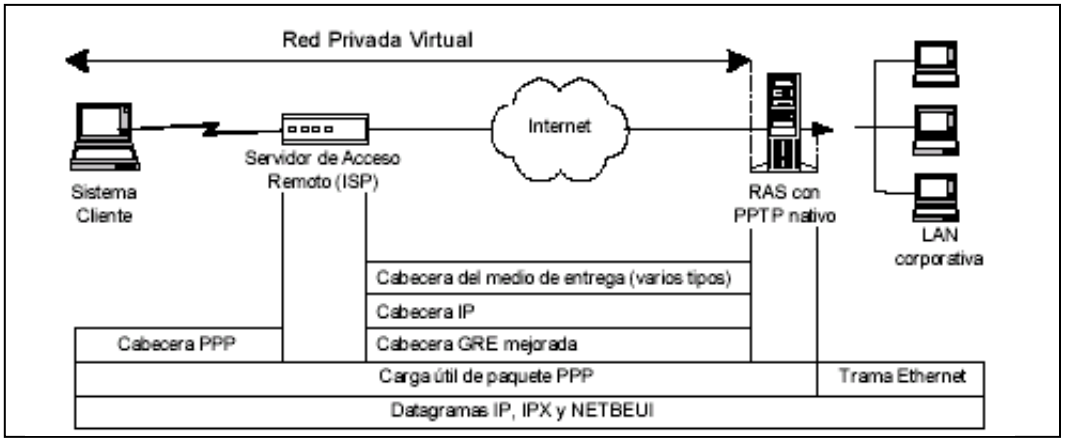


Figura 19. Estructura de un túnel PPTP

4.2.11.3. TUNELES

PPTP permite a los usuarios y a las ISPs crear varios tipos de túneles, basados en la capacidad del computador del usuario final y en el soporte de la ISP para implementar PPTP. De esta manera, el computador del usuario final determina el lugar de terminación del túnel, bien sea en su computador, si está corriendo un cliente PPTP, o en el servidor de acceso remoto de la ISP, si su computador solo soporta PPP y no PPTP. En este segundo caso el servidor de acceso de la ISP debe soportar PPTP, a diferencia del primer caso, donde la ISP no se involucra en ningún proceso de entunelamiento de datos.
Dado lo anterior, los túneles se pueden dividir en dos clases, voluntarios y permanentes.

Los túneles voluntarios son creados por requerimiento de un usuario y para un uso específico. Los túneles permanentes son creados automáticamente sin la acción de un usuario y no le permite escoger ningún tipo de privilegio.
En los túneles voluntarios, la configuración del mismo depende del usuario final, cuando se usan túneles de este tipo, el usuario puede simultáneamente acceder a Internet y abrir un túnel seguro hacia el servidor PPTP. En este caso el cliente PPTP reside en el computador del usuario. Los túneles voluntarios proveen más privacidad e integridad de los datos que un túnel permanente. La figura 20 muestra un escenario de túneles voluntarios creados desde dos clientes distintos a un mismo servidor PPTP a través de Internet.

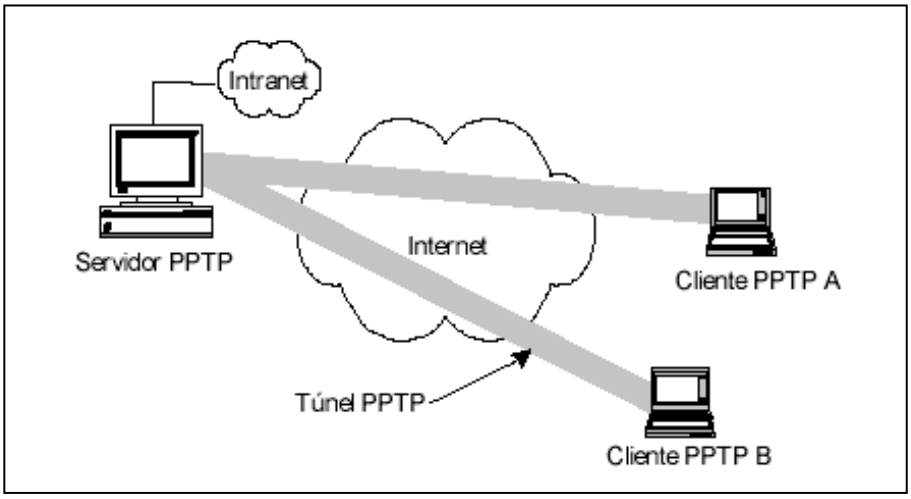


Figura 20. Tuneles Voluntarios

Los túneles permanentes son creados sin el consentimiento del usuario, por lo tanto, son transparentes para el mismo. El cliente PPTP reside en el servidor de acceso remoto de la ISP al que se conectan los usuarios finales. Todo el tráfico originado desde el computador del usuario final es reenviado por el RAS sobre el túnel PPTP. En este caso la conexión del usuario se limita solo a la utilización del túnel PPTP, no hay acceso a la red pública (Internet) sobre la cual se establece el túnel. Un túnel permanente PPTP permite que múltiples conexiones sean transportadas sobre el mismo túnel. La figura 21 muestra un túnel permanente entre un RAS con capacidad para encapsular sesiones PPP usando PPTP y por medio del cual van multiplexadas dos sesiones de clientes A y B.

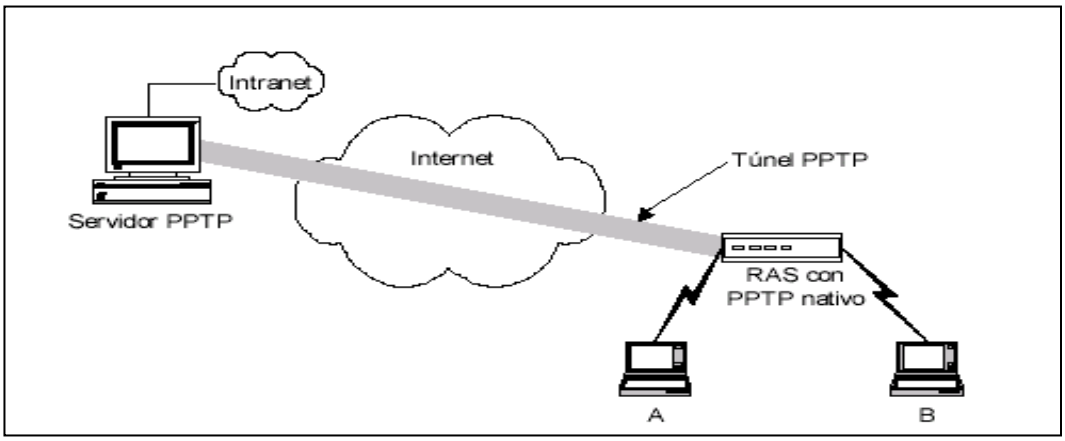


Figura 21 Tuneles permanentes

Dado que los túneles permanentes tienen predeterminados sus puntos finales y que el usuario no puede acceder a Internet, estos túneles ofrecen mejor control de acceso que los túneles voluntarios. Otra ventaja de los túneles permanentes, es que reducen el ancho de banda utilizado, ya que múltiples sesiones pueden ser transportadas sobre un único túnel, a diferencia de los túneles voluntarios donde cada sesión tiene que trabajar con cabeceras independientes que ocupan un ancho de banda.

Una desventaja de los túneles permanentes es que la conexión inicial, es decir, entre el usuario final y el servidor de acceso que esta actuando como cliente PPTP, no hace parte del túnel, por lo tanto, puede ser vulnerable a un ataque.

Los túneles permanentes se dividen en estáticos y dinámicos. Los túneles estáticos son aquellos que requieren equipos dedicados y su configuración es manual. En este tipo de túneles el usuario final tiene a su disposición varios RAS, los cuales tienen establecidos diferentes túneles a diferentes servidores PPTP.

Los túneles permanentes dinámicos usan el nombre del usuario para determinar el túnel asociado con él, es decir que se encargan de aprovechar mejor los recursos y el usuario puede marcar al mismo número para establecer túneles a diferentes sitios. La información asociada con cada usuario puede residir en el servidor Radius en el cual ese servidor de acceso esta autenticando todas las conexiones.

Claramente se observa que los túneles permanentes estáticos son más costosos que los dinámicos, ya que involucran un servidor de acceso por cada destino que un cliente VPN quiera alcanzar.

4.2.11.3.1 ENTUNELAMIENTO LAN-to-LAN

Originalmente PPTP fue desarrollado pensando en brindar soluciones de acceso remoto VPN, es decir, proveer acceso conmutado seguro a redes locales corporativas vía Internet. Los túneles LAN-to-LAN no fueron soportados en un comienzo. Solo hasta el año 1997 cuando Microsoft introdujo su servicio de enrutamiento de acceso remoto (RRAS) para servidores NT 4.0, se pudieron implementar topologías LAN-to-LAN usando PPTP como protocolo de entunelamiento.

La implementación de Microsoft para entunelamiento LAN-to-LAN exige la presencia de dos servidores PPTP que tienen la función de hacer de gateways seguros de las dos redes locales. Sin embargo, la gran desventaja de usar PPTP en topologías LAN-to-LAN es la inseguridad inherente a la arquitectura del protocolo. En efecto, la autenticación y el cifrado son controlados por protocolos que ofrecen un nivel muy bajo de confiabilidad, como CHAP o MS-CHAP. La figura 22 muestra una topología de red LAN-to-LAN entre una pareja de servidores PPTP usando un túnel PPTP sobre Internet, para los usuarios tanto de la LAN corporativa A como de la B el túnel es transparente, y a nivel lógico se trabaja como en una única red local.

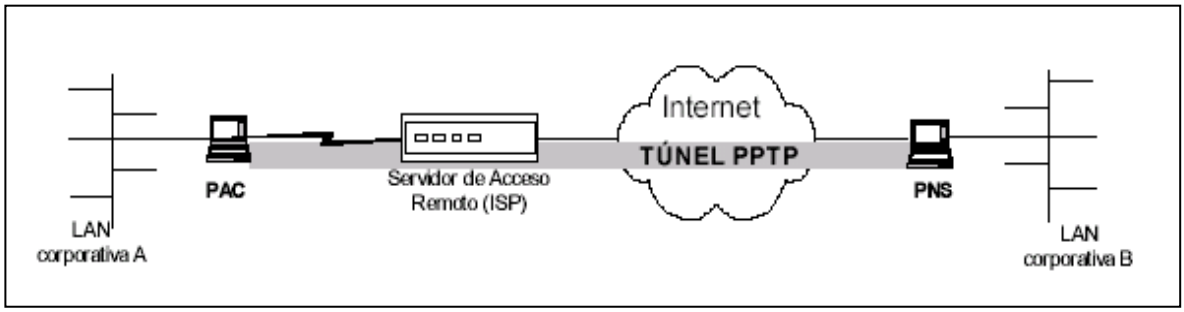


Figura 22. Topología LAN-TO LAN usando un túnel PPTP

Para crear un túnel entre dos sitios, un servidor PPTP es autenticado por el otro usando passwords simples, algo similar a un usuario conmutado. En este caso, uno de los sitios actúa como el servidor PPTP y el otro como un cliente PPTP, de esta manera, un túnel voluntario es creado entre los dos extremos y por el mismo pueden existir varias sesiones.

Dado que un túnel PPTP puede encapsular varios protocolos de capa de red, los usuarios no tendrán acceso a los recursos, que cada protocolo le provee hasta que sus privilegios sean validados por el correspondiente protocolo.

4.2.12. SERVIDORES DE ACCESO DE RED

Los servidores de acceso a la red también llamados servidores de acceso remoto o concentradores de acceso, son los encargados de soportar las conexiones PPP de una gran cantidad de clientes que se conectan a este por medio de enlaces telefónicos conmutados. Sus funciones van desde el establecimiento de la conexión física (modulación, demodulación, compresión de datos, corrección de errores, etc.) hasta labores de enrutamiento presentes en la capa 3 de la torre OSI.

4.2.13. L2TP (Layer 2 Tunneling Protocol)

L2TP fue creado como el sucesor de PPTP y L2F. Las dos compañías abanderadas de cada uno de estos protocolos, Microsoft por PPTP y Cisco por L2F, acordaron trabajar en conjunto para la creación de un único protocolo de capa 2 y así lograr su estandarización por parte de la IETF.

Como PPTP, L2F fue diseñado como un protocolo de entunelamiento usando para ello encapsulamiento de cabeceras. Una de las grandes diferencias entre PPTP y L2F, es que el entunelamiento de éste último no depende de IP y GRE, permitiéndole trabajar con otros medios físicos por ejemplo Frame Relay. Paralelamente al diseño de PPTP, L2F utilizó PPP para autenticación de usuarios accesando vía telefónica conmutada, pero también incluyó soporte para TACACS+ y Radius. Otra gran diferencia de L2F con respecto a PPTP es que permite que un único túnel soporte más de una conexión. Hay dos niveles de autenticación del usuario: primero, por la ISP antes de crear el túnel; segundo, cuando la conexión está configurada y la autenticación la realiza el gateway corporativo.

Todas las anteriores características de L2F han sido transportadas a L2TP. Como PPTP, L2TP utiliza la funcionalidad de PPP para proveer acceso conmutado que puede ser tunelizado a través de Internet a un sitio destino.Sin embargo, como se ha mencionado anteriormente, L2TP define su propio protocolo de entunelamiento basado en L2F permitiendo transporte sobre una amplia variedad de medios de empaquetamiento tales como X.25, Frame Relay y ATM.

Dado que L2TP es un protocolo de capa 2, ofrece a los usuarios la misma flexibilidad de PPTP de soportar otros protocolos aparte de IP, tales como IPX y NETBEUI. Puesto que L2TP usa PPTP en enlaces conmutados, incluye mecanismos de autenticación nativos de PPP como PAP y CHAP.
Microsoft incluye L2TP a partir del sistema operativo Windows 2000, ya que las mejoras de L2TP con respecto a PPTP saltan a la vista.

4.2.14. COMPONENTES BÁSICOS DE UN TÚNEL L2TP

4.2.14.1 Concentrador de acceso L2TP (LAC)

Un LAC es un nodo que se encuentra en un punto extremo de un túnel L2TP. El LAC se encuentra entre un LNS y un sistema remoto y reenvía los paquetes a y desde cada uno. Los paquetes enviados desde el LAC hasta el LNS van tunelizados. En algunas ocasiones el sistema remoto actúa como un LAC, esto se presenta cuando se cuenta con un software cliente LAC.

4.2.15. IPSEC

En IPv4 no se desarrollaron mecanismos de seguridad inherentes al protocolo, por tanto, protocolos y procedimientos adicionales a IPv4 fueron necesarios para brindar servicios de seguridad a los datos. IPSec es un conjunto de protocolos diseñados para proveer una seguridad basada en criptografía robusta para IPv4 e IPv6, de hecho IPSec está incluido en IPv6.

Entre los servicios de seguridad definidos en IPSec se encuentran, control de acceso, integridad de datos, autenticación del origen de los datos, protección antirepetición y confidencialidad en los datos. Entre las ventajas de IPSec están la

modularidad del protocolo, ya que no depende de un algoritmo Criptográfico específico.

4.2.15.1. COMPONENTES DE IPSEC

IPSec está compuesto por tres componentes básicos: los protocolos de seguridad (AH y ESP), las asociaciones de seguridad (SAs) y las bases de datos de seguridad; cada uno de los cuales, trabaja de la mano con los demás y ninguno le resta importancia al otro.

4.2.15.2. Protocolos de Seguridad

IPSec es un conjunto de protocolos que provee varios servicios de seguridad. Esos servicios de seguridad trabajan gracias a dos protocolos, el Authentication Header (AH) y el Encapsulating Security Payload (ESP), y también al uso de protocolos y procedimientos para el manejo de llaves criptográficas tales como IKE (Internet Key Exchange Protocol) El éxito de una implementación IPSec depende en gran medida de una adecuada escogencia del protocolo de seguridad y de la forma como se intercambian las llaves criptográficas.

AH es un protocolo que añade una nueva cabecera justo después de la cabecera IP original. AH provee autenticación del origen de los datos e integridad de los mismos, también provee integridad parcial para prevenir ataques de repetición. Este protocolo es apropiado cuando se requiere autenticación en vez de confidencialidad.

ESP provee confidencialidad para el tráfico IP, al igual que autenticación tal cual como lo hace AH, pero solo uno de estos servicios puede ser proporcionado por ESP al mismo tiempo.

IKE es un protocolo que permite a dos entidades IPSec negociar dinámicamente sus servicios de seguridad y sus llaves de cifrado al igual que la autenticación de la sesión misma

4.2.15.3 Asociaciones de Seguridad (SAs)

El concepto de asociación de seguridad (SA) es clave en IPSec. Una SA define las medidas de seguridad que deberían ser aplicadas a los paquetes IP basados en quién los envía, hacia donde van y qué tipo de carga útil ellos transportan. El conjunto de servicios de seguridad ofrecidos por una SA dependen de los

protocolos de seguridad y del modo en el cual ellos operan definidos por la SA misma.
La figura 23 muestra los dos modos en los cuales un protocolo de seguridad puede operar: transporte y túnel; la diferencia radica en la manera como cada uno de ellos altera el paquete IP original. El modo de transporte es diseñado para proteger los protocolos de capas superiores tales como TCP y UDP. En modo túnel, el paquete IP original se convierte en la carga útil de un nuevo paquete IP. Esto le permite al paquete IP inicial, "ocultar" su cabecera IP para que sea encriptada, considerando que el paquete IP externo sirve de guía a los datos a través de la red.

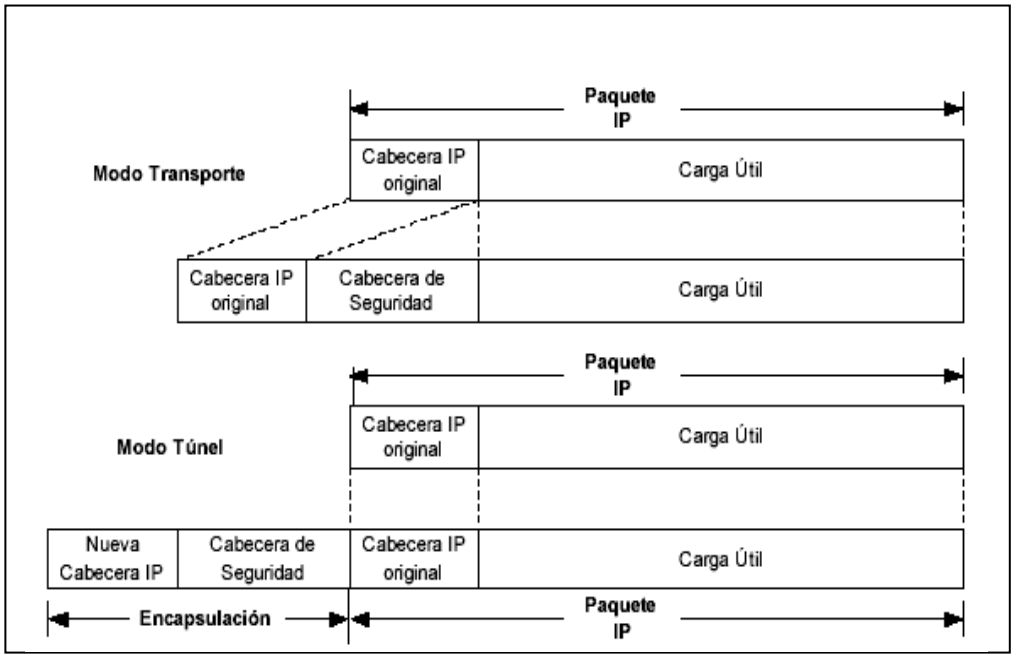


Figura 23 Estructura del paquete IP en mode de transporte y Túnel.

Las SAs pueden ser negociadas entre dos entidades IPSec dinámicamente, para lo cual se basan en políticas de seguridad dadas por el administrador del sistema o estáticamente especificadas por el administrador directamente.

Una SA es únicamente identificada por tres parámetros: una dirección IP de destino, un identificador del protocolo de seguridad y un índice del parámetro de seguridad (SPI). La dirección IP de destino es aquella por la cual se identifica el punto final de la SA, el SPI es un número de 32 bits usualmente escogido por el punto final de destino de la SA y que solo tiene significado local dentro de ese punto destino. El identificador del protocolo de seguridad es un número con el cual se define cada uno de ellos, 51 para AH o 50 para ESP. Como se nota, la dirección

IP del origen no se usa para definir una SA, esto dado que una SA se define entre dos host o gateways para datos enviados en una sola dirección, de aquí que, si dos dispositivos necesitan intercambiar información en ambas direcciones usando IPSec, requerirán de dos SAs, una para cada sentido.

En modo de transporte, la cabecera IP original se mantiene intacta y una cabecera de seguridad es colocada entre la cabecera IP misma y su carga útil. La cabecera IP original es modificada para que el receptor del paquete entienda que antes de la carga útil se encuentra una cabecera de seguridad. En modo túnel, el paquete IP original se convierte en la carga útil de un paquete IP encapsulado. La cabecera IP nueva le indica al receptor del paquete que una cabecera de seguridad se encuentra a continuación de ella.

Varias SAs pueden ser aplicadas en serie para incrementar los servicios de seguridad del tráfico IP. En estas situaciones una SA es encerrada por otra. El protocolo IPSec define dos formas: transporte adyacente y túneles iterados.

En transporte adyacente se usan tanto AH como ESP y ellos son aplicados por el mismo host. Es de anotar que trabajar con adyacencias de transporte AH sobre AH o ESP sobre ESP no trae beneficios adicionales. Lo deseable en este caso es aplicar AH después de ESP.

En túneles iterados, se puede combina cualquier cantidad de túneles con lo cual se logra proveer de capas anidadas de seguridad. Los puntos finales del túnel pueden ser en la misma o en diferentes locaciones. Por ejemplo, un túnel host-to-host puede ser entonelado por un túnel gateway-to-gateway; y un túnel gateway-to-gateway puede de nuevo ser entunelado por otro túnel gateway-to-gateway.

4.2.15.4 AUTHENTICATION HEADER (AH)

El protocolo de cabecera de autenticación AH es usado para propósitos de utenticación de la carga útil IP a nivel de paquete por paquete, esto es autenticación de la integridad de los datos y de la fuente de los mismos. Como el término autenticación indica, el protocolo AH se asegura que los datos entregados dentro del paquete IP son auténticos, es decir, que han arribado a su destino sin ninguna modificación. AH también provee de un mecanismo de protección opcional antirepetición de paquetes IP. Sin embargo, AH no protege la confidencialidad de los datos, es decir, no recurre a ningún tipo de cifrado de los mismos.
El protocolo AH define como un paquete IP sin protección es convertido en uno nuevo que contiene información adicional y que brinda autenticación. El elemento

fundamental usado por AH es una cabecera de autenticación como se muestra en la figura 24.
El nuevo paquete IP es formado insertando la cabecera de autenticación, bien sea, después de la nueva cabecera IP o después de la cabecera IP original modificada según sea el modo en el cual trabaje la SA, más adelante se tratara con mayor detalle cada uno de estos dos modos: transporte y tunel.

Cuando la cabecera de autenticación es insertada, la cabecera IP que la precede deberá indicar que la próxima cabecera que se encuentra es la cabecera de autenticación y no la carga útil del paquete original. La cabecera IP realiza esta acción colocando el campo Protocolo en el valor 51 (valor de protocolo para AH).

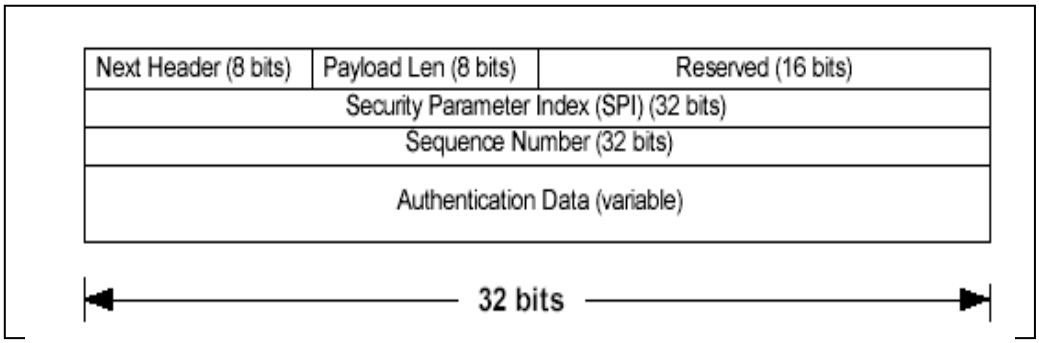


Figura 24. Formato de cabecera de autenticación

La cabecera de autenticación contiene seis campos:

- ✓ Next Header: El campo Next Header es un campo de ocho bits que identifica el tipo de protocolo de la carga util del paquete IP original.
- ✓ Payload Len: El campo Payload Len es un campo de ocho bits que especifica la longitud de la cabecera de autenticación (no confundir con la cabecera original del paquete IP).
- ✓ Reserved: El campo Reserved se encuentra reservado para uso futuro, actualmente debe ser puesto en 0.
- ✓ Security Parameter Index: El campo Security Parameter Index es un número arbitrario de 32 bits. Este valor es usado junto con la dirección IP de destino y el tipo de protocolo IPSec (en este caso, AH) únicamente para identificar la SA para este paquete IP. El valor SPI es escogido por el sistema destino cuando la SA es establecida.
- ✓ Sequence Number: El campo Sequence Number es un campo de 32 bits que mantiene un incremento monotónico de la secuencia de paquetes IPSec. Comienza en 0 cuando la SA es establecida y se incrementa por cada paquete

IP saliente que usa esta SA. Este campo se usa como un mecanismo de protección antirepetición.

- ✓ Authentication Data: El campo Authentication Data es un campo de longitud variable que contiene el valor de chequeo de integridad ICV (Integrity Check Value) para este paquete IP. El ICV es calculado con el algoritmo seleccionado por la SA y es usado por el recepto para verificar la integridad del paquete IP entrante.

Hay que tener en cuenta, que la autenticación no puede ser aplicada sobre la cabecera entera del paquete IP, ya que algunos campos de la cabecera IP original cambian durante el transito por Internet. Esos campos son llamados Campos Mutables, y son:

- Type of service (TOS)
- Fragment offset
- Fragmentation flags
- Time to live (TTL)
- Header checksum

4.2.15.4.1 Modo Transporte

En modo transporte, la cabecera del paquete IP original es conservada como la cabecera del nuevo paquete IP, y la cabecera de autenticación es insertada entre la cabecera IP y la carga útil original, como se muestra en la figura 25. El único cambio que se realiza en la cabecera IP es el del campo Protocolo que cambia a 51, valor para el protocolo AH. El valor reemplazado en el campo Protocolo pasa a ser el valor del campo Next Header en la cabecera de autenticación. Finalmente el ICV es calculado sobre la totalidad del nuevo paquete IP excluyendo los campos mutables mencionados previamente.

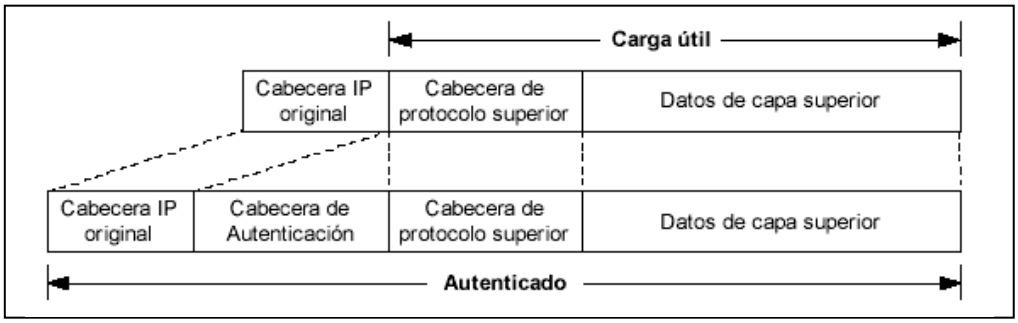


Figura 25 Modo Transporte AH

La ventaja del modo Transporte es que solo adiciona unos pocos bytes extra a el paquete IP original. Sin embargo, por conservarse la cabecera IP original como la misma cabecera del nuevo paquete IP, solamente puede ser usado por hosts finales, esta es una limitación grande cuando los dispositivos que están gobernados por esta SA IPSec actúan como gateways de otros hosts que se encuentran detrás de ellos.

4.2.15.4.2 Modo Túnel

En modo Túnel, una nueva cabecera es creada para el nuevo paquete IP y la cabecera de autenticación es insertada entre las cabeceras nueva y original, tal como se uestra en la figura 26. El paquete IP original permanece intacto y es encapsulado dentro del nuevo paquete IP. De esta manera, la autenticación se aplica sobre el paquete IP original entero (incluyendo los campos mutables de la cabecera IP original).

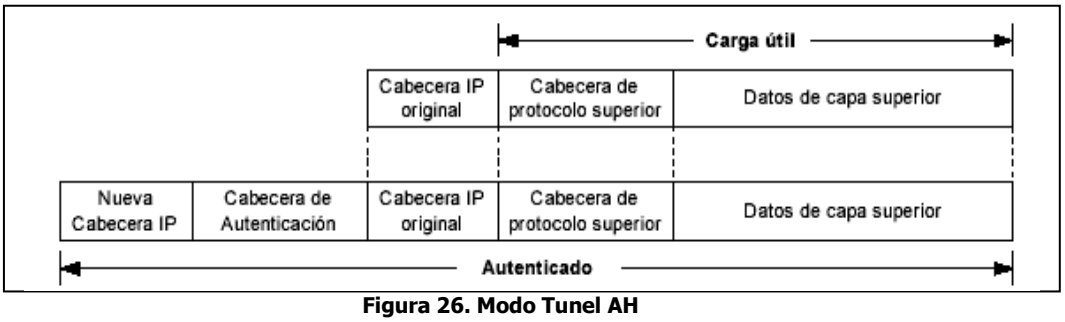


Figura 26. Modo Tunel AH

La cabecera IP original permanece completamente inalterada y contiene las direcciones IP tanto de destino como fuente de los dispositivos que emiten y reciben el tráfico IP original. La nueva cabecera IP contiene la dirección IP fuente y de destino de los dispositivos IPSec entre los cuales viaja el nuevo paquete. De esta manera el modo Túnel puede ser usado si los puntos finales de la SA son un host o gateway de seguridad.

A diferencia del modo Transporte, el modo Túnel tiene como desventaja adicionar mas bytes extra por lo cual el throughput efectivo del enlace disminuye al igual que el desempeño de los dispositivos se torna mas lento por el doble procesamiento de cabecera que se necesita.

El valor del campo Protocolo en la nueva cabecera IP es 51 (como en el modo Transporte) y el campo Next Header en la cabecera de autenticación contiene el valor 4, que especifica que la siguiente cabecera es de 1 paquete de tipo IPv4.

4.2.15.5 ENCAPSULATING SECURITY PAYLOAD – ESP

El protocolo ESP IPSec provee autenticación, confidencialidad de los datos por medio de cifrado y una protección opcional antirepetición para los paquetes IP. La utenticación y el cifrado son también opcionales, pero al menos una de ellas debe ser empleada; de lo contrario, este protocolo carecería de fundamento.

La confidencialidad es lograda por medio de técnicas de cifrado. Los algoritmos de cifrado empleados a los paquetes IP son definidos por la SA sobre la cual los paquetes son enviados. El algoritmo de cifrado Null en el cual el cifrado no es aplicado, es también un algoritmo válido en este protocolo. En este caso, ESP solamente presta el servicio de autenticación para el tráfico.

4.2.16. INDEPENDENCIA Y CONTROL DEL REENVIO

En el reenvío de paquetes IP convencional, cualquier cambio en la información que controla el reenvío de paquetes es comunicado a todos los dispositivos que controlan el dominio de enrutamiento. Este cambio, siempre lleva consigo un periodo de convergencia mientras que la información es actualizada en toda la red.

De lo anterior es claramente deseable, un mecanismo que pudiera cambiar el trayecto por el cual se reenvía un paquete sin afectar los demás dispositivos que conforman la red. Para implementar este mecanismo, los dispositivos de enrutamiento no deberían depender de la información que se contiene en la cabecera IP, para lo cual se necesitaría adjuntar una etiqueta adicional al paquete reenviado que indique el comportamiento que tome el mismo a lo largo de la red. Si las decisiones de reenvío se basan entonces en etiquetas adjuntadas a los paquetes IP originales, cualquier cambio en el proceso de decisión puede ser llevado a cabo únicamente adjuntado nuevas etiquetas y así no se impactarían ninguno de los otros dispositivos de enrutamiento que conforman la red.

4.2.17 PROPAGACIÓN DE INFORMACIÓN EXTRA DE ENRUTAMIENTO

En una red que trabaja con el mecanismo de reenvío convencional de paquetes, todos los dispositivos de enrutamiento, conocen la paquete es enrutado basado en la dirección destino que esta contenida en su cabecera de capa de red.

Este método tiene implicación de escalabilidad en términos de propagación de rutas y de memoria y CPU utilizadas en los enrutadores del backbone, teniendo en cuenta que la única acción que se necesitaría sería reenviar desde el router de Cartagena hasta los routers del otro extremo sin involucrar de manera alguna la toma de decisiones a nivel 3 en los routers del backbone. Un mecanismo que permita a los dispositivos de enrutamiento conmutar los paquetes a través de la red, desde un router destino hasta un router final, sin analizar la dirección destino sería un objetivo a perseguir.

4.2.18 MPLS

MPLS quiere decir Conmutación de Etiquetas Multiprotocolo (Multiprocol Label Switching). Es una tecnología relativamente nueva que se desarrolló para solucionar la mayoría de los problemas que existen en la técnica actual de reenvío de paquetes. La IETF cuenta con un grupo de trabajo MPLS que se ha unido esfuerzos en estandarizar esta tecnología. Según aparece en el documento draft-ietf-mpls-framework, "el objetivo primario de MPLS, es estandarizar una tecnología base que integre el intercambio de etiquetas durante el reenvío con el sistema de enrutamiento actual de redes. Se espera que esta nueva tecnología mejore la relación precio/desempeño del enrutamiento que se realiza en la capa de red, que mejore la escalabilidad de la misma capa, y que provea una gran flexibilidad en la entrega de (nuevos) servicios de enrutamiento". La arquitectura MPLS describe cómo se realiza la conmutación de etiquetas, la cual combina los beneficios del reenvío de paquetes a nivel de Capa 2 con los beneficios del enrutamiento a nivel 3. Similar a como se hace en las redes Capa 2, MPLS asigna etiquetas a los paquetes para que sean transportados a través de redes basadas en paquetes o en celdas. Este mecanismo de reenvío a través de dichas redes es conocido como intercambio de etiquetas (label swapping), lo cual permite que con una etiqueta pequeña y de longitud fija que se añade al paquete original se pueda enrutar dicho paquete a lo largo de un camino determinado que se crea con la información que cada switch en la red tiene y sobre la que existe en cada etiqueta. Esta es la forma como se puede crear una VPN usando MPLS.

En el reenvío de paquetes usando MPLS se puede apreciar una diferencia drástica con el reenvío original de paquetes, dado que en este último entorno, cada paquete es analizado en cada uno de los saltos de la red, donde se chequea la cabecera Capa 3, y con base en la información de la misma se toma una decisión conforme a la tabla de enrutamiento de cada dispositivo de Capa 3.
La arquitectura MPLS se divide en dos componentes: el componente de reenvío (también llamado data plane) y el componente de control (también llamado control plane).

El componente de reenvío, como su nombre lo indica, se encarga de reenviar los paquetes basado en las etiquetas que cada uno de ellos transporta, para esto usa una base de datos de reenvío de etiquetas que es mantenida por un switch de etiquetas (label switch). Haciendo la analogía con el esquema tradicional de reenvío de paquetes, esta base de datos es la tabla de enrutamiento.

El componente de control es el responsable de crear y mantener toda la información de reenvío de etiquetas (también llamada Vínculos) entre un grupo de switches de etiquetas interconectados. De nuevo, haciendo la analogía con el esquema tradicional de enrutamiento, el componente de control es el protocolo de enrutamiento.

Tal como en los routers tradicionales, los protocolos de enrutamiento IP son los encargados de mantener la tabla de enrutamiento, en la cual se basan los dispositivos de Capa 3 para tomar la decisión de reenvío del Paquete.

En un nodo MPLS, la tabla de enrutamiento es usada para determinar el intercambio de Vínculos de etiquetas, dicho intercambio es realizado por el Protocolo de Distribución de Etiquetas o LDP (Label Distribution Protocol). El componente de control usa las etiquetas intercambiadas con los nodos MPLS adyacentes para construir la Tabla de Reenvío de Etiquetas o LFT (Label Forwarding Table), la cual usa el componente de datos para reenviar los paquetes etiquetados a través de la red MPLS.

4.2.19 Introducción a NAT

La Traducción de Direcciones de Red, o NAT (*Network Address Translation*), es un sistema que se utiliza para asignar una red completa (o varias redes) a una sola dirección IP. NAT es necesario cuando la cantidad de direcciones IP que nos haya

asignado nuestro proveedor de Internet sea inferior a la cantidad de ordenadores que queramos que accedan a Internet.

NAT nos permite aprovechar los bloques de direcciones reservadas. Generalmente, una red interna se suele configurar para que use uno o más de estos bloques de red. Estos bloques son:

10.0.0.0/8	(10.0.0.0 - 10.255.255.255)
172.16.0.0/12	(172.16.0.0 - 172.31.255.255)
192.168.0.0/16	(192.168.0.0 - 192.168.255.255)

Un sistema OpenBSD configurado para NAT tendrá como mínimo dos adaptadoras de red, una para Internet y la otra para la red interna. NAT se encargará de traducir los requerimientos desde la red interna, de modo que parezca que todos provienen del sistema OpenBSD en el que se encuentra configurado NAT.

4.2.19.1 Cómo Funciona NAT

Cuando un cliente en la red interna contacta con un máquina en Internet, envía paquetes IP destinados a esa máquina. Estos paquetes contienen toda la información de direccionamiento necesaria para que puedan ser llevados a su destino. NAT se encarga de estas piezas de información:

- Dirección IP de origen (por ejemplo, 192.168.1.35)
- Puerto TCP o UDP de origen (por ejemplo, 2132)

Cuando los paquetes pasan a través de la pasarela de NAT, son modificados para que parezca que se han originado y provienen de la misma pasarela de NAT. La pasarela de NAT registra los cambios que realiza en su tabla de estado, para así poder: a) invertir los cambios en los paquetes devueltos, y b) asegurarse de que los paquetes devueltos pasen a través del cortafuegos y no sean bloqueados. Por ejemplo, podrían ocurrir los siguientes cambios:

- IP de origen: sustituida con la dirección externa de la pasarela (por ejemplo, 24.5.0.5)
- Puerto de origen: sustituido con un puerto no en uso de la pasarela, escogido aleatoriamente (por ejemplo, 53136)

Ni la máquina interna ni el anfitrión de Internet se dan cuenta de estos pasos de traducción. Para la máquina interna, el sistema NAT es simplemente una pasarela

a Internet. Para el anfitrión de Internet, los paquetes parecen venir directamente del sistema NAT; ni siquiera se da cuenta de que existe la estación interna.

Cuando el anfitrión de Internet responde a los paquetes internos de la máquina, los direcciona a la IP externa de la pasarela de NAT (24.5.0.5) y a su puerto de traducción (53136). La pasarela de NAT busca entonces en la tabla de estado para determinar si los paquetes de respuesta concuerdan con alguna conexión establecida. Entonces encontrará una única concordancia basada en la combinación de la dirección IP y el puerto, y esto indica a PF que los paquetes pertenecen a una conexión iniciada por la máquina interna 192.168.1.35. Acto seguido PF realiza los cambios opuestos a los que realizó para los paquetes salientes, y reenvía los paquetes de respuesta a la máquina interna.

La traducción de paquetes ICMP ocurre de forma parecida, pero sin la modificación del puerto de origen.

4.2.20 WEBMIN

Webmin es una interfaz que permite administrar su Unix/Linux a partir de un navegador web. Webmin le permite por ejemplo administrar sus cuentas de usuario, Apache, DNS, samba a partir de una interfaz única.

Casi todo el desarrollo de Webmin fue hecho por Jamie Cameron, aunque muchas personas han contribuido parches y traducciones en los idiomas adicionales. Hay también muchos módulos terceristas que fueron desarrollados separadamente por otras personas.

Usermin es una interface de tejido que puede ser usada por cualquier usuario en un sistema de Unix o Linux, para realizar tareas fácilmente como lee correo, prepara SSH o configura correo remitiendo. Puede pensarse de como una versión simplificada de Webmin diseñada para el uso por usuarios normales en lugar de administradores del sistema.

Guste Webmin, Usermin consiste en un servidor de tejido simple, y varios CGI programa que directamente pone al día archivos de config de usuario gusta ~ / .cshrc y ~ / .forward.

Usermin está disponible libre para el anuncio y el uso personal bajo la licencia de BSD. Porque Usermin apoya el concepto de módulos (como el plugins de

PhotoShop), cualquiera puede desarrollar y puede distribuir sus propios módulos para cualquier propósito, y los distribuye bajo cualquier licencia (como GPL, comercial o shareware).

4.2.21 TECNOLOGIA GPS.

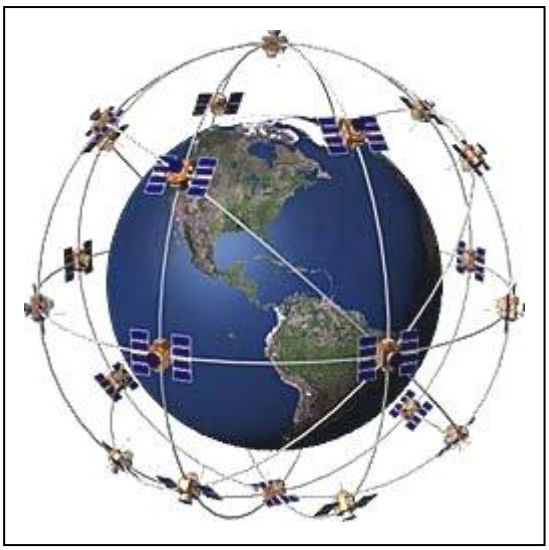


FIGURA 27. Sistema de Posicionamiento Global (Global Positioning System, GPS)

El Sistema de Posicionamiento Global (Global Positioning System, GPS) desarrollado por Estados Unidos, se ha incorporado masivamente a todo tipo de trabajos que necesitan de una precisión exhaustiva a la hora de determinar la posición en que se encuentra un barco, un avión, un coche, un explorador o un iceberg sobre nuestro planeta.

La base de este sistema consiste en un conjunto de 21 satélites que en todo momento están describiendo una órbita en torno a la Tierra. Estos satélites emiten su señal durante las 24 horas del día. La recepción de varias de estas señales es lo que permite al GPS portátil (del tamaño de un transistor de bolsillo), calcular su posición en la Tierra. A mayor número de satélites "visibles" por el aparato, más precisos son los cálculos. Con sucesivas posiciones el receptor puede suministrarnos otros datos derivados, como nuestra posición exacta y relativa, la velocidad de navegación o desplazamiento, cómo debemos cambiar el rumbo para llegar a nuestro destino y otras opciones.

4.2.21.1 Como funciona un receptor GPS

Los receptores GPS reciben la información precisa de la hora y la posición del satélite. Exactamente, recibe dos tipos de datos, los datos del Almanaque, que consiste en una serie de parámetros generales sobre la ubicación y la operatividad de cada satélite con relación al resto de satélites de la red, esta información puede ser recibida desde cualquier satélite, y una vez el receptor GPS tiene la información del último Almanaque recibido y la hora precisa, sabe donde buscar los satélites en el espacio; La otra serie de datos, también conocida como Efemérides, hace referencia a los datos precisos, únicamente, del satélite que está siendo captado por el receptor GPS, son parámetros orbitales exclusivos de ese satélite y se utilizan para calcular la distancia exacta del receptor al satélite. Cuando el receptor ha captado la señal de, al menos, tres satélites calcula su propia posición en la Tierra mediante la triangulación de la posición de los satélites captados,

5. METODOLOGÍA

5.1 TIPO DE INVESTIGACIÓN

El presente trabajo se encuentra en el tipo Cuasiexperimental, durante el desarrollo se trabajo bajo Prueba-Error, se realizo investigación de las opciones ofrecida para el desarrollo e implementación del trabajo.

5.2 LINEAS DE INVESTIGACION

- Redes y sistemas distribuidos: Con tendencia hacia la definición de estándares y la interoperabilidad, las comunicaciones sin cable, las redes empresariales, los sistemas transaccionales.

5.3. ETAPAS O FASES

5.3.1 Fase de Exploración

Dentro de la investigación realizada para la toma de una buena solución en el problema que nos atañe, se realizaron estudios de los recursos con los que cuentan los colegios Gabriel Echavarría y Tecnológico a nivel informático, además se analizaron las diferentes soluciones ofrecidas por la tecnología hoy en día.

5.3.1.1. Tipos de Soluciones

1. Solución **FIBRA OPTICA**: los dos colegios se encuentran a una distancia de 1200 metros, se busco un proveedor que nos cotizara interconectar estos dos colegios a través de fibra óptica. El costo de esta implementación bordeaba los 40'.000.000 de pesos faltando el medio para salir a Internet. Analizamos que con esta opción el costo era demasiado alto y poco práctico.

2. Solución **ADSL:** es una técnica de transmisión que, aplicada sobre los abonados de la red telefónica, permite la transmisión de voz y datos a altas velocidades. Para ello utiliza frecuencias más altas que las empleadas en el servicio telefónico y sin

intervenir en ellas, permitiendo así el uso simultaneo del servicio telefónico y para acceder al servicio de datos a través de ADSL.

3. Solución **RED TELEFONICA (MODEM)**: Esta solución no se tomo en cuenta debido a que los Colegios Gabriel Echavarria y Tecnológico no tiene sino dos líneas telefónicas cada uno. Además este tipo de solución es de bajo desempeño y no supliría las necesidades de los colegios.

4. Solución **RDSI**: Aunque es una solución que nos ofrece un mejor desempeño y bajo costo, no hay un proveedor que llegue a la localidad de Madrid.

5. Solución **ISP**: Es un Proveedor de Servicio de Internet, el cual nos ofrece el servicio que requerimos en esta zona a través de un radio enlace. Se citaron varios proveedores pero ninguno ofreció el servicio para el municipio de Madrid. Realizamos un estudio en los Café Internet del Municipio de Madrid y encontramos que el proveedor que les da este servicio es IFX. (ver Anexo A),nos ofrecieron varias alternativas de las cuales en conjunto con las directivas de los colegios se toma la de un canal dedicado de 128k, para 20 computadores, el cual nos incluye el uso de un hosting con capacidad de 50 megas, en donde se puede alojar la página diseñada, adicionalmente incluye cupo para diez correos electrónicos y dos direcciones IP, a un costo que e encuentra estipulado en el contrato.

5.3.1.2 REDES PRIVADAS VIRTUALES – VPNs

Una VPN es una conexión que tiene la apariencia y muchas de las ventajas de un enlace dedicado pero trabaja sobre una red pública. Para este propósito usa una técnica llamada entunelamiento (tunneling), los paquetes de datos son enrutados por la red pública, tal como Internet o alguna otra red comercial, en un túnel privado que simula una conexión punto a punto. Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura. También hace universales para su transporte los diferentes protocolos LAN entre los que se encuentran IP, IPX, Appletalk y Netbeui, de allí la característica de multiprotocolo que hace sumamente universal la tecnología de las redes virtuales privadas. La figura 28 muestra los distintos escenarios que se pueden manejar con la tecnología de Redes Privadas Virtuales (Dial-Up, Intranet VPN y Extranet VPN).

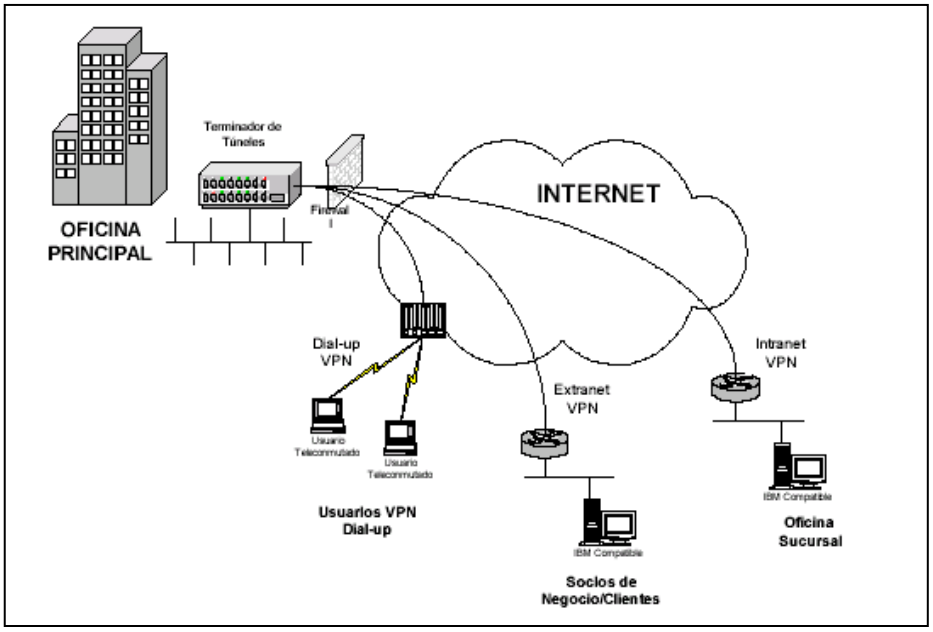


Figura 28. Distintas manera de crear una VPN.

Las técnicas de entunelamiento básicamente se puede decir que consiste en encapsular los paquetes de datos que salen de una LAN o del equipo del usuario remoto dentro de protocolos que trabajan a nivel 2 de la torre OSI.

Los componentes básicos de un túnel, y que se muestran en la figura 29. son:

- Un iniciador del túnel
- Uno o varios dispositivos de enrutamiento
- Un conmutador de túneles (opcional)
- Uno o varios terminadores de túneles

El inicio y la terminación del túnel pueden ser hechos por una amplia variedad de equipos o software. Un túnel puede ser empezado, por ejemplo, por un usuario remoto con un computador portátil equipado con un modem análogo y un software de conexión telefónica para hacer una VPN, también puede haber un enrutador de una extranet en una oficina remota o en una LAN pequeña. Un túnel puede ser terminado por otro enrutador habilitado para tal fin, por un switch con esta característica o por un software que haga tal fin.

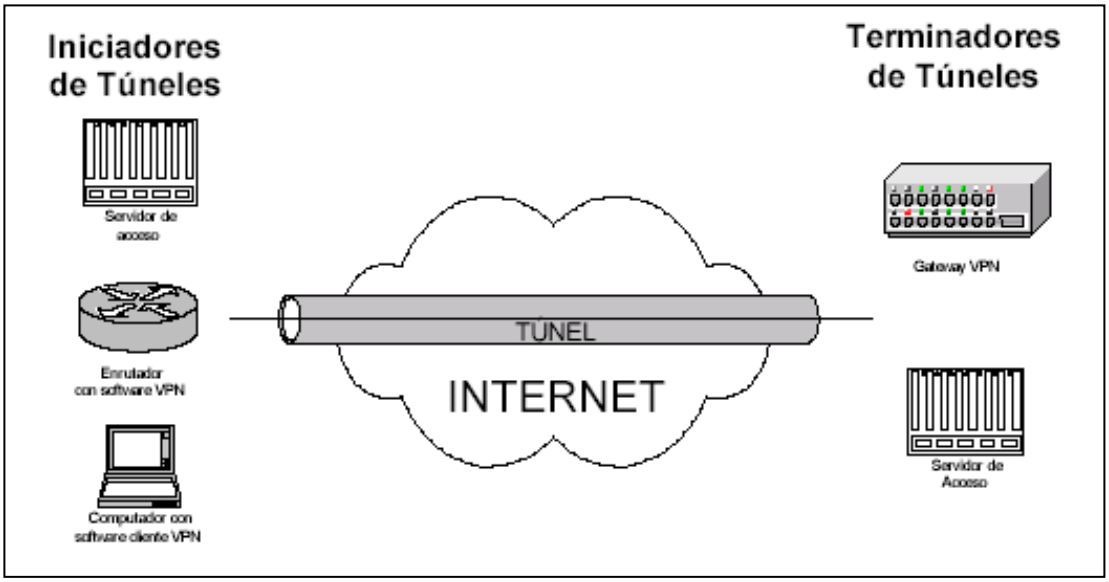


Figura 29. Elementos Básicos de un túnel VPN.

Adicionalmente y para completar una solución VPN deben existir uno o más dispositivos o paquetes de software que brinden cifrado, autenticación y autorización a los usuarios del túnel. Además muchos de estos equipos brindan información sobre el ancho de banda, el estado del canal y muchos más datos de gestión y de servicio.

La figura 30 muestra un diagrama más detallado de una VPN dial-up usando como protocolo de entunelamiento a PPTP. Se notan los trayectos en los cuales el protocolo que encapsula los datos es PPP y la parte del recorrido que es tunelizada usando PPTP.

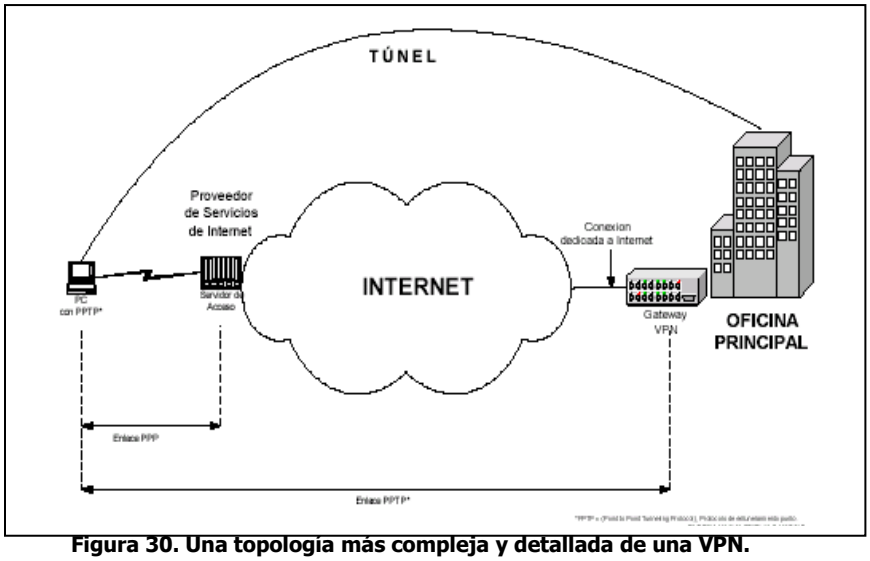


Figura 30. Una topología más compleja y detallada de una VPN.

En muchos casos las características que le permiten a los dispositivos ser iniciadores o terminadores del túnel se pueden adicionar con una simple actualización del sistema operativo o de sus tarjetas.

Una buena solución VPN requiere la combinación de tres componentes tecnológicos críticos: seguridad, control de tráfico y manejo empresarial:

Seguridad: Dentro de este punto se destacan: el control de acceso para garantizar la seguridad de las conexiones de la red, el cifrado para proteger la privacidad de los datos y la autenticación para poder verificar acertadamente tanto la identidad de los usuarios como la integridad misma de la información.

Control de tráfico: el segundo componente crítico en la implementación de una efectiva VPN es el control de tráfico que garantice solidez, calidad del servicio y un desempeño veloz. Las comunicaciones en Internet pueden llegar a ser excesivamente lentas, lo que las convertirían en soluciones inadecuadas en aplicaciones de negocios donde la rapidez es casi un imperativo. Aquí es donde entra a jugar parámetros como la prioridad de los datos y la garantización de ancho de banda.

Manejo empresarial: El componente final crítico en una VPN es el manejo empresarial que esta tenga. Esto se mide en una adecuada integración con la política de seguridad de la empresa, un manejo centralizado desde el punto inicial hasta el final, y la escalabilidad de la tecnología.

Las VPNs se caracterizan también por su flexibilidad. Pueden ser conexiones punto-punto o punto-multipunto. Reemplazando una red privada con muchos y costosos enlaces dedicados, por un solo enlace a una ISP que brinde un punto de presencia en la red (POP por sus siglas en inglés), una compañía puede tener fácilmente toda una infraestructura de acceso remoto, sin la necesidad de tener una gran cantidad de líneas telefónicas análogas o digitales, y de tener costosos pools de módems o servidores de acceso, o de pagar costosas facturas por llamadas de larga distancia. En algunos casos las ISP se hacen cargo del costo que les genera a los usuarios remotos su conexión a Internet local, pues ven en este tipo de negocio un mayor interés por los dividendos del acceso.

El objetivo final de una VPN es brindarle una conexión al usuario remoto como si este estuviera disfrutando directamente de su red privada y de los beneficios y servicios que dentro de ella dispone, aunque esta conexión se realice sobre una infraestructura pública.

5.3.1.3 ARQUITECTURAS VPN

El éxito de una VPN depende de una adecuada elección de la tecnología y del escenario, siempre acordes a las necesidades que se tengan.

La tecnología implica: técnicas de entunelamiento, autenticación, control de acceso, y seguridad de los datos; y los escenarios que se pueden construir son: Intranet VPN (LAN-to-LAN VPN), Acceso Remoto VPN y Extranet VPN.

Intranet VPN (LAN-to-LAN VPN): En este escenario, múltiples redes remotas de la misma compañía son conectadas entre si usando una red pública, convirtiéndolas en una sola LAN corporativa lógica, y con todas las ventajas de la misma.

Acceso Remoto VPN: En este caso, un host remoto crea un túnel para conectarse a la Intranet corporativa. El dispositivo remoto puede ser un computador personal con un software cliente para crear una VPN, y usar una conexión conmutada, o una conexión de banda ancha permanente.

Extranet VPN: Esta arquitectura permite que ciertos recursos de la red corporativa sean accesados por redes de otras compañías, tales como clientes o proveedores. En este escenario es fundamental el control de acceso.

5.3.1.3.1 Objetivos de implantación de una VPN

Los objetivos básicos que se persiguen con la instalación VPNs son los siguientes:

1. Interconexión total a la red de forma segura a través Internet
2. Intercambio de información en tiempo real.
3. Acceso remoto a la información
4. Flexibilidad y facilidad de uso.
5. Obtención de la máxima velocidad de transferencia de datos usando con eficiencia los recursos de los colegios.
6. Fácil adaptación a las nuevas tecnologías a un costo mínimo.

5.3.2 FASE DE IMPLEMENTACION.

5.3.2.1. Implementación e Infraestructura:

De acuerdo a la propuesta ofrecida la empresa IFX implemento el canal dedicado de 128k en demostración por una semana. Los miembros del proyecto se distribuyeron en parejas para coordinar en cada uno de los Colegios esta implementación**.**

Cuando se usan medios no guiados (microondas, radio) la velocidad de propagación de la señal es, aproximadamente, la velocidad de la luz en el vacío (300000 Km/s). En el caso de que se usen medios guiados (cables, fibras ópticas) esta velocidad es, aproximadamente, 2/3 de la velocidad de la luz en el vacío (es decir, unos 200000 Km/s).

La Figura 31 muestra lo que se dio como solución para los dos colegios Tecnológico de Madrid y Gabriel Echevarria.

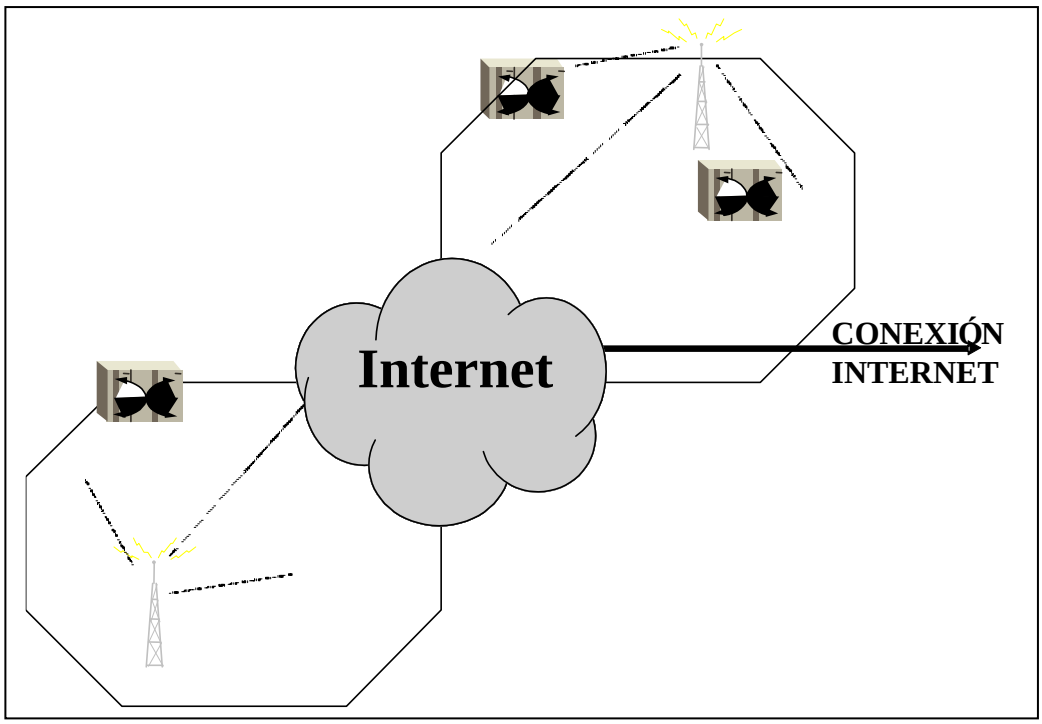


Figura 31 Solución para los Colegios Gabriel Echavaria y Tecnológico

La implementación de las VPN a través de Internet se muestra en la figura 32

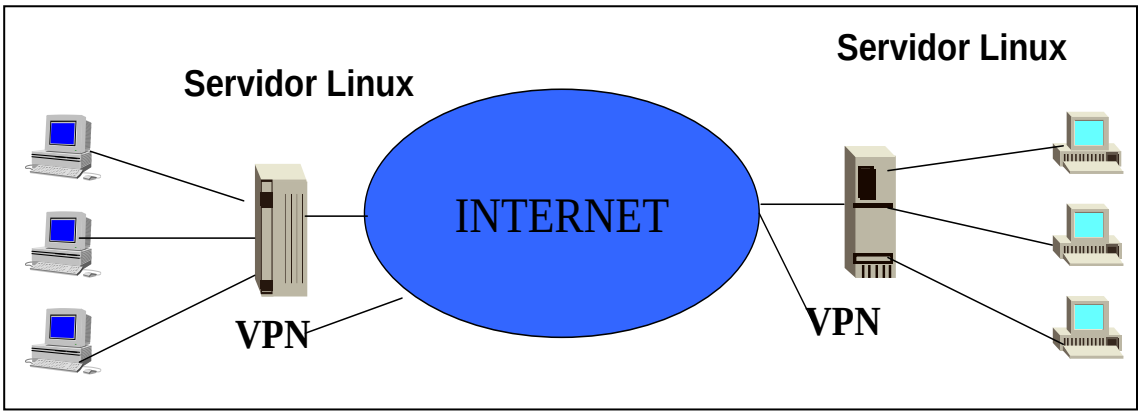


Figura 32 Implementación de VPN a través de Internet

El tipo de Antena que se esta utilizando es grilla figura 33. Este tipo de antena soporta distancias hasta de 20 Km, cuenta con un Edipolo Feeder por la que llega la señal, tiene un amplificador de señal que se usa para dar más potencia y más seguridad a la transmisión de los datos.
Dentro de la caja de la antena se encuentra el Autor, es decir, que esta a la intemperie y por dentro lleva una tarjeta que recibe el enlace por el cable UTP, lleva la señal y una caja negra que lleva la energía al radio enlace.

Figura. 33 antenas Grilla

Se utilizó un radio enlace que realiza la tarea del enrutador, un Gateway que es el encargado de dar la salida.

5.3.2.1.1 Factores que se tuvieron en cuenta en el desarrollo de la red.

Se realizo un estudio de factibilidad teniendo en cuenta la distancia de los colegios al Serró Mesetas, la cual es de 12 kilómetros; se realizó la verificación de línea de vista, el polo a tierra de los Colegios Gabriel Echevarria y Tecnológico de Madrid y que la señal de la antena no estuviera saturada de clientes.

Se hizo la prueba de Ver o Pingfill esto realiza la saturación del radio y muestra las estadísticas mostrando la información del estado del radio, tiene un límite de hasta 1 mg de ancho de banda. La entidad que garantiza la salida de ancho de banda es el Ministerio de Comunicaciones.

Las antenas utilizan tecnología GPS Global Positioning System. (Ver marco conceptual). GPS funciona de 3 a 5V, se encuentra ubicada en la antena del serró de Majuy denominada antena base que tiene una altura de 60 metros es la que recibe la señal de todas las antenas. En este momento se cuneta con 12 clientes.

5.3.2.1.2 Instalación de las Antenas en los colegios Tecnológico de Madrid y Gabriel Echavarria.

Las antenas ubicadas en los colegios cuentan con una altura de 15 metros.

5.3.2.1.2.1 Característica de Enlace:

Colegio Gabriel Echavarria:

Canal: Internet
Medio o frecuencia de radio : Wireless 2.4GHz
Radio Remoto: SM
Ancho de Banda (BW): 128KB.
Red IP Asignada:
Configuración: Routing
Base: Pozos Madrid
Red IP Asignada: 200.91.204.56 / 30
IP Pub. Proxy Server: 200.91.204.57

Colegio Tecnológico de Madrid:

Característica de Enlace:
Canal: Internet
Medio: Wireless 2.4GHz
Radio Remoto: SM
Ancho de Banda (BW): 128KB.
Red IP Asignada:
Configuración: Routing

Base: Pozos Pistones
Red IP Asignada: 200.91.204.148 / 30
IP Pub. Proxy Server: 200.91.204.150

Elementos

Cable LMR 600 coaxial: para el colegio Gabriel Echevarria se utilizo este tipo de cable por la distancia entre la antena y el centro de cableado que es de 20 metros. Para el Colegio Tecnológico de Madrid se utilizó cable UTP por la distancia entre la antena y el centro de cableado que es de 60 mts.

Configuración de Clientes:

IP: 192.168.0.x
Mask: 255.255.255.0
DNS:192.168.0.2, 200.91.200.100, 200.62.3.3

Red IP Privada: 192.168.0.0 / 24
DNS: 200.91.200.100, 200.62.3.3
SMTP: smtp.ifx.com.co, 200.91.200.87

Sistema Wireless – Instalación: (Sistema De Radio – Instalación)

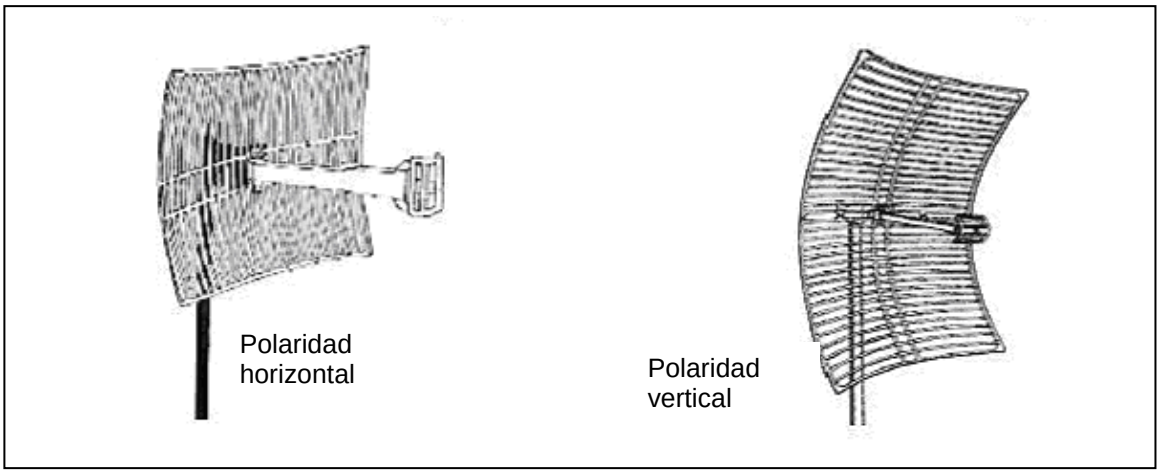


Figura 34. Posición de las antenas Grilla

POLARIZACIONES EN UNA ANTENA GRILLA

La antena debe estar dirigida de tal forma cuando usted mira hacia fuera desde el centro de la antena esta este apuntando hacia la antena receptora en el otro edificio. La señal de radio irradia desde el extremo de la antena como una linterna de foco amplio.

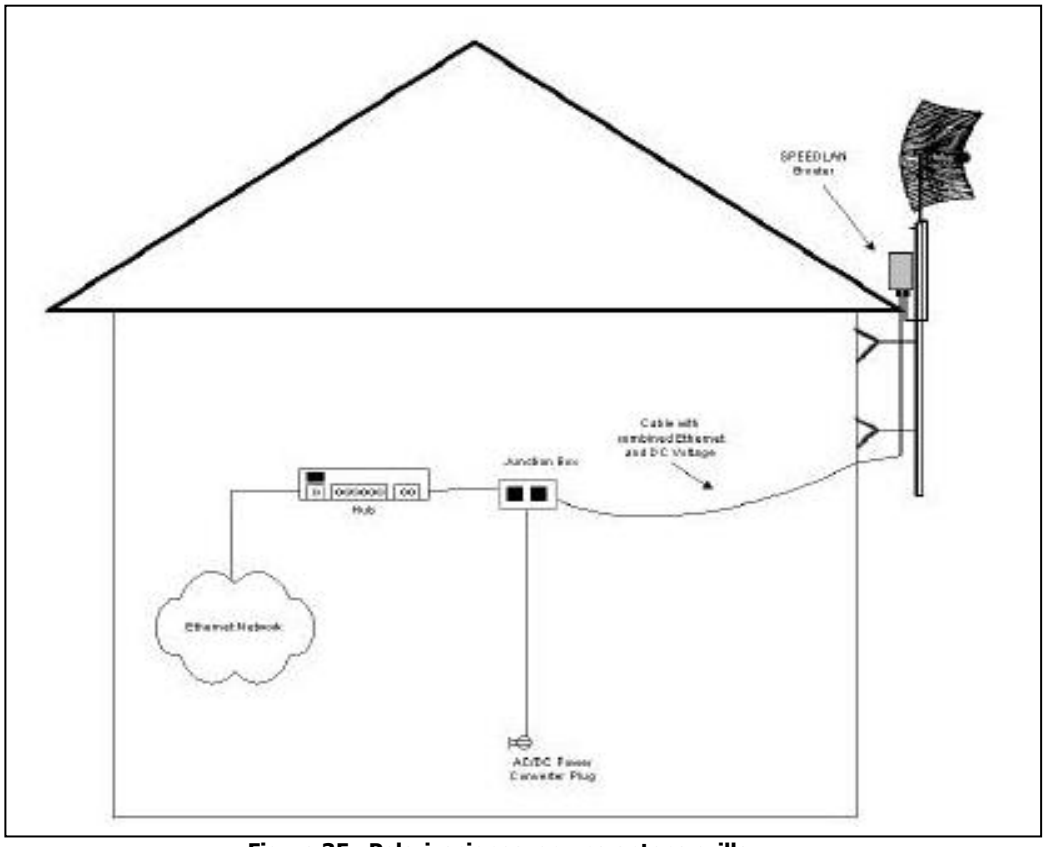


Figura 35. Polarizaciones en una antena grilla

Una vez que se tuvo la salida a Internet se configuró cada una de las máquinas de las salas de informática de cada Colegio (Gabriel Echevarria - Tecnológico de Madrid) así:

Con esta configuración las máquinas navegaban por Internet a través de NAT, puesto que no se contaba con la ambientación adecuada de los servidores para realizar la salida por proxy. (Ver marco conceptual)

En la semana de demostración se vio la necesidad de implementar los servidores para que salieran a través de un Proxy, ya que la velocidad de navegación era muy

lenta. Para la instalación del Proxy se realizo una revisión técnica a los servidores, encontrando que las unidades de CD se encontraban defectuosas, al ser Scsi no se podía remplazar fácilmente. Para solucionar este inconveniente gestionamos con la coordinadora de sistemas de la planta de Colceramica, el préstamo de una unidad con la que realizamos posteriormente las instalaciones.

DESCRIPCION DE LOS SERVIDORES DONADOS POR LA FUNDACION PILARES DE DESARROLLO

Servidor	Producto	Compañia Propietaria	Serie	Disco duro	Memoria	Procesador	Velocidad
Ubicado en el colegio Gabriel Echevarria	Compaq PROSIGNIA	Colceramica	3085	cuatro se desconoce el tamaño	Ram: 98 Mb	Pentium	120 Mhz.

Posteriormente se comenzó a instalar Linux en los servidores pero estos al ser COMPAQ, pedían el Smart Star, por la antigüedad de los equipos no se contaba con esta herramienta la cual permite la instalación de los sistemas operativos en servidores. Se Investigo sobre Linux y encontramos que desde el cd de instalación se puede generar un disket de arranque que funciona en los servidores, de esta forma se realizó la instalación de Linux Mandrake 8.0 en un equipo; este proceso duro varios días, el segundo servidor que se encuentra en el colegio Gabriel Echevarria se realizó la instalación porque este equipo no arrancaba, después de varias pruebas sin éxito (prueba-error), se decidió conseguir un asesor para guiar la implementación. En la primera sesión con el asesor se definieron los parámetros a seguir dentro de la implementación de la solución dada, así:

- Sistema Operativo.
- Un servidor Proxy
- Seguridad
- Implementación de VPN

5.3.2.1.3 SISTEMA OPERATIVO

Linux es un sistema operativo de inmensas capacidades que puede ser utilizado por diferentes tipos de usuarios debido a su versatilidad que permite configurarlo según las necesidades de cada uno de usuarios.

Durante el proceso de instalación experimentamos diversos errores que nos llevaron incluso, cuando estábamos a un paso de terminar la instalación, a volver

al principio. Una vez instalado Linux Mandrake 8.0 se observa que el sistema no reconocía toda la memoria RAM del servidor debido a que los requerimientos de maquina no eran suficientes para esta plataforma; por esta razón se cambiaron los servidores. Se procedió a instalar Red had 9.0 en los nuevos servidor, dentro de esta instalación no se incluyo la parte gráfica porque representar un peligro en la seguridad ; al no subir la parte grafica se empieza a trabajar en el nivel 3 en el se maneja el modo multiusuario, se habitaron las estaciones de trabajo como bastille (que permite agregar y quitar programas) drak conf (permite la configuración de red had como tal, Makdev (que permite la configuración de dispositivos), ip table (permite el manejo de tablas para la configuración de reglas de seguridad.), se subieron los servicios de webmin, squid, se habilitaron los puertos 10000 (de escucha) - 25 (para correo electrónico) – 80 (http) – 53 (DNS) – 443 (https) – 21 (ftp) y se configuraron las tarjetas de red con las direcciones preestablecidas, así:

Colegio Tecnológico de Madrid

Eth 0:

- IP pública 200.91.204.62
- Mascara de red 255.255.255.252
- Puerta de enlace 200.91.204.61
- DNS 200.91.200.100
  200.62.3.3

Eth 1:

- IP de la Lan 192.168.0.50
- Mascara de Red 255.255.255.0
- Puerta de Enlace 200.91.204.61
- DNS 200.91.200.100
  200.62.3.3

Colegio Gabriel Echevarria

Eth 0:

- IP pública 200.91.204.58
- Mascara de red 255.255.255.252
- Puerta de enlace 200.91.204.57
- DNS 200.91.200.100
  200.62.3.3

Eth 1:

- IP de la Lan 192.168.0.80
- Mascara de Red 255.255.255.0
- Puerta de Enlace 200.91.204.57
- DNS 200.91.200.100
  200.62.3.3

Una vez terminada la instalación del sistema operativo se coloca un path cord entre el router y la tarjeta de red Eth0 para la salida a Internet a través del servidor. Un path cord del switch a la tarjeta de red Eth1 esto habilita la salida a Internet de los equipos de la LAN, posteriormente se realizan pruebas desde el servidor con el siguiente comando:

$nslookup www.conavi.com

Se procede a realizar la instalación del sistema operativo del segundo servidor (donado por Corona), el equipo no subía, se realizaron pruebas detectando que el primer disco de la maquina estaba dañado, se retiro y luego se instaló Linux, al finalizar esta instalación se reventó el sistema. Al consultar con el asesor nos explico que los discos Scsi están jompiados de una manera especial en donde el 0 es de arranque y continúan sucesivamente, se coloco el disco 3 en la posición del disco 0 y ninguno estaba jompeado como 0. Esto se corrigió y al arrancar el equipo ya mostraba discos Scsi 0,1,2; Se volvió a realizar la instalación y esta vez si funciono.

Durante el proceso de instalación realizamos la configuración de red necesaria:

Colegio Tecnológico de Madrid :

IP LAN: 192.168.0.50
Mask: 255.255.255.0
IP pública: 200.91.204.62
Getway: 200.91.204.61
MASK: 255.255.255.252
DNS: 200.91.200.100
200.62.3.3

Colegio Gabriel Echavarría:

IP LAN: 10.26.16.80

Mask: 255.255.255.0
IP pública: 200.91.204.58
Getway: 200.91.204.57
MASK: 255.255.255.252
DNS: 200.91.200.100
200.62.3.3

Una vez terminada la instalación satisfactoriamente, se verifica que los puertos 25 (correo) y 80 (http) estuvieran abiertos, esto se realiza con el comando:

netstat -an

Mediante este comando se pude ver todos los puertos queden habilitados de no ser así genera inconvenientes en los siguientes pasos de implementación.

En el siguiente diagrama se muestra la configuración de seguridad realizada en cada uno de los colegios (Tecnológico de Madrid y Gabriel Echevarria):

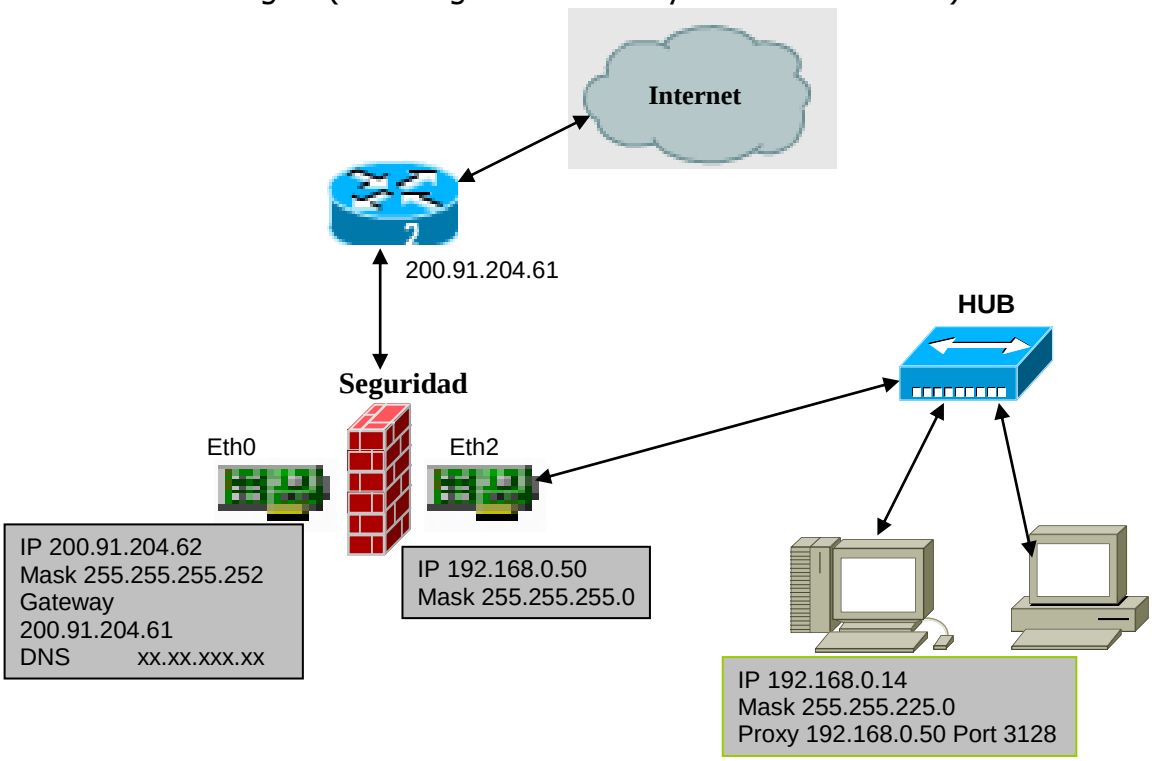


Figura 36. Seguridad establecida en los colegios

5.3.2.1.3.1 Servicios de Linux utilizados para la implementación de las VPNs:

5.3.2.1.3.1.1 FreeS/WAN:

Es una implementación de los protocolos IPSec (IP Security) en Linux.

5.3.2.1.3.1.1.1 Instalación de FreeS/WAN

Tras instalar el sistema en los dos servidores Linux, instalamos los fuentes del kernel y los paquetes con el soporte para FreeS/WAN versión 1.95

Configuración FreeS/WAN

FreeS/WAN posee un archivo principal de configuración y es el **ipsec.conf**, puede estar en /etc o en /etc/freeswan (depende la distribución de Linux). En este archivo se configura todo, hay otros archivos de configuración como el **ipsec.secrets** donde se coloca la información de claves, firmas de RSA, y/o ubicación de las claves de los certificados. Por último hay un directorio /etc/ipsec.d que se utiliza generalmente al trabajar con el parche de autenticación X509.
FreeS/WAN se compone de varias partes, que entre todas colaboran para implementar todos los protocolos de IPsec:

SSH (Secure Shell)

Este protocolo fue diseñado para dar seguridad al acceso a computadores en forma remota.

Cumple la misma función que telnet pero además, usando criptografía, logra seguridad con los datos.

A diferencia de telnet u otro servicio similar, SSH utiliza el puerto 22 para la comunicación y la forma de efectuar su trabajo es muy similar al efectuado por SSL.

Para su uso se requiere que por parte del servidor exista un demonio que mantenga continuamente en el puerto 22 el servicio de comunicación segura, el sshd.

El cliente debe ser un software tipo TeraTerm o Putty que permita la hacer pedidos a este puerto 22 de forma cifrada.

La forma en que se entabla una comunicación es en base la misma para todos los protocolos seguros:

- El cliente envía una señal al servidor pidiéndole comunicación por el puerto 22.
- El servidor acepta la comunicación en el caso de poder mantenerla bajo encriptación mediante un algoritmo definido y le envía la llave publica al cliente para que pueda descifrar los mensajes.
- El cliente recibe la llave teniendo la posibilidad de guardar la llave para futuras comunicaciones o destruirla después de la sesión actual.

5.3.2.1.4 ARCHIVOS DE CONFIGURACION IPSEC.CONF E IPSEC.SECRETS

Una vez se finalizó la conexión a Internet en ambos colegios, se realizaron pruebas de navegación desde las estaciones de trabajo.
Luego se realizaron pruebas de conectividad desde cada estación de trabajo que consistían en alcanzar a la otra por medio del comando (está navegando), luego aparece un ping al IP del gateway remoto IPSec (xx.xxx.xx.xxx) y por último aparece un ping al IP de la estación de trabajo que esta detrás del gateway remoto (192.168.200.x).

Para evitar exponer la comunicación a ataques del tipo hombre-en-el medio, FreeS/WAN maneja dos tipos de autenticación para sus túneles:

- ✓ Manual Keying: donde las dos partes comparten un llave secreta para encriptar sus mensajes. FreeS/WAN almacena estas llaves en el archivo /etc/ipsec.conf. Es claro que si alguien obtiene acceso a este archivo la comunicación será vulnerable.
- ✓ Automatic keying: Aquí los dos sistemas se autentican el uno con el otro por medio de sus propias llaves secretas. Estas llaves son cambiadas automáticamente de una manera periódica. Obviamente, este método de autenticación es mucho mas seguro, ya que si un intruso obtiene la llave, solo los mensajes entre la renegociación anterior y la siguiente serán expuestos.

Una vez comprobada la adecuada instalación del paquete, se procede a la configuración de los archivos /etc/ipsec.conf y /etc/ipsec.secrets.

Hay que aclarar que cada gateway debe tener un IP estático dado por el ISP, en una interfaz ethernet (por ejemplo eth0). A cada gateway se le debe asignar por nomenclatura como right o left.

El archivo /etc/ipsec.conf se puede dividir en dos secciones: la primera donde se configuran las opciones generales de IPSec, llamada config setup; y la segunda donde se define cada pareja IPSec llamada conn <*nombre que identifica el tunel*> . En esta última sección puede aparecer una llamada conn %default que es donde se definen las características que se aplican por defecto a cada pareja de gateways IPSec.

La parte más importante del archivo /etc/ipsec.conf es la que define cada conexión

Los campos básicos que define cada pareja IPSec
son:
left=
leftsubnet=
leftnexthop=
leftrsasigkey=
right=
rightsubnet=
rightnexthop=
rightrsasigkey=
auto=

Los campos left y right son las direcciones IP públicas de cada gateway.

Los campos leftsubnet y rightsubnet son las subredes que se encuentran detrás de cada gateway (la red privada).
Los campos leftnexthop y rightnexthop son las direcciones IP del equipo que recibe la conexión en el ISP. Es la puerta de enlace de cada máquina Linux.

Los campos leftrsasigkey y rigthrsasigkey son las llaves públicas de cada gateway IPSec, y se obtienen con los comandos:
ipsec showhostkey --left (para la máquina llamada left), y ipsec showhostkey --right (para la máquina llamada right).
En caso de no contar con estas llaves, se puede generar cada una de ellas con el comando:

ipsec newhostkey --output /etc/ipsec.secrets –hostname <*hostname*>

Para la configuración de las VPNs en los colegios Gabriel Echavarria y Tecnológico de Madrid se usaron los siguientes parámetros:

Comandos para la generación de llaves:

Leftrsasigkey
Rightrsasigkey

COLEGIO TECNOLOGICO DE MADRID

ipsec.conf

```
conn net-to-net
    left=200.91.204.58            # Local vitals
    leftsubnet=10.26.20.0/24      #
    leftnexthop=%defaultroute     # correct in many situations
    right=200.91.204.62           # Remote vitals
    rightsubnet=192.168.0.0/24    #
    rightnexthop=%defaultroute    # correct in many situations
    auto=start                    # authorizes but doesn't start this

leftrsasigkey=0sAQONfeLImCbIo+ITCrjZZX5K0PELEKXs7mmJeZ64z8lrxwapSzYO5WEnuqyDvZQa2U
68dfjFr7J8d0wAaHgtZnl3
rightrsasigkey=0sAQOYid+XaVAIYFhvW9RlpJlUq/A9LfoYdJy9Q3Hjo3DnahnjaLShno6Tp1j1AVS31Yf2
KBDVTyUel8F+AEk1dfYP
[root@tecno etc]#
```

ipsec.secrets

```
: RSA  {
       # RSA 512 bits   tecno   Sat Sep  4 14:57:06 2004
       # for signatures only, UNSAFE FOR ENCRYPTION

#pubkey=0sAQOYid+XaVAIYFhvW9RlpJlUq/A9LfoYdJy9Q3Hjo3DnahnjaLShno6Tp1j1AVS31Yf2KBD
VTyUel8F+AEk1dfYP
       Modulus:
0x9889df9769500860586f5bd465a49954abf03d2dfa18749cbd4371e3a370e76a19e368b4a19e8e93a
758f50154b7d587f62810d54f251e97c17e00493575f60f
       PublicExponent: 0x03
       # everything after this point is secret
       PrivateExponent:
0x196c4fee918d56bab967e4a36646198e1ca80a32545968c4ca35e8509b3d7be6c1c2e69868c1debd
35838a594bd08427752b5ecd0f680ba693ea59033e3dd79f
       Prime1: 0xe4323d504e5c9381978531c5d1c1432c2b7f312936b409d4535cc3f380ca24ed
       Prime2: 0xab1fc3d1deb6c2a2cebe8523bc13796f0ba4a6ddbc00cedbf6a326423f38c36b
       Exponent1: 0x98217e3589930d010fae212e8bd62cc81cff761b79cd5be2e23dd7f7ab316df3
       Exponent2: 0x72152d369479d717347f036d280cfb9f5d186f3e7d55df3d4f176ed6d4d08247
       Coefficient: 0xd418cfb857ea38accb5c251b9bab09dfaae5c3a0ad7b82b1708a18ead44de6b7
       }
# do not change the indenting of that "}"
[root@tecno etc]#
```

COLEGIO GABRIEL ECHAVARRIA

ipsec.conf

```
conn net-to-net
    left=200.91.204.58            # Local vitals
    leftsubnet=10.26.20.0/24      #
leftnexthop=%defaultroute         # correct in many situations
    right=200.91.204.62           # Remote vitals
    rightsubnet=192.168.0.0/24    #
    rightnexthop=%defaultroute    # correct in many situations
    auto=start                    # authorizes but doesn't start this

leftrsasigkey=0sAQONfeLImCbIo+ITCrjZZX5K0PELEKXs7mmJeZ64z8lrxwapSzYO5WEnuqyDvZQa2U
68dfjFr7J8d0wAaHgtZnl3

rightrsasigkey=0sAQOYid+XaVAIYFhvW9RlpJlUq/A9LfoYdJy9Q3Hjo3DnahnjaLShno6Tp1j1AVS31Yf2
KBDVTyUel8F+AEk1dfYP
[root@colge etc]#
```

ipsec.secrets

```
: RSA  {
        # RSA 512 bits   colge   Thu Dec 20 05:37:37 2001
        # for signatures only, UNSAFE FOR ENCRYPTION
#pubkey=0sAQONfeLImCbIo+ITCrjZZX5K0PELEKXs7mmJeZ64z8lrxwapSzYO5WEnuqyDvZQa2U68d
fjFr7J8d0wAaHgtZnl3
        Modulus:
0x8d7de2c89826c8a3e2130ab8d9657e4ad0f10b10a5ecee6989799eb8cfc96bc706a94b360ee56127b
aac83bd941ad94ebc75f8c5afb27c774c0068782d667977
        PublicExponent: 0x03
        # everything after this point is secret
        PrivateExponent:
0x1794fb216eb12170a5add71ecee63fb722d2d72d70fcd266ec3eefc977f6e74b965b4444adaab961a9
c8f21c3366626dcf0ff32b8ef96d6d6e94d5573ee68ccb
        Prime1: 0xdb8254acbfa62562f03164574f0b516b28b9463e85323cdd4212e4c55add4721
        Prime2: 0xa5035ced3d3ee37acfc572bd10a93950b95cff81d0a7af09727083a75921e597
        Exponent1: 0x9256e31dd5196e41f57642e4df5ce0f21b262ed458cc28938161edd8e73e2f6b
           Exponent2: 0x6e023df37e29ecfc8a83a1d36070d0e07b93550135c51f5ba1a057c4e616990f
        Coefficient: 0x1dfec851e70449dbe7f9d0c3ceb827ebad66c4fb7cc94f79eadf3d815c5eb37b
        }
# do not change the indenting of that "}"
[root@colge etc]#
```

El ipsec.conf tiene dos tipos de secciones, la sección de "config" (configuración) y la sección de "conn" (conexiones). En este momento la única sección de configuración que se acepta en FreeS/WAN es la sección de config "setup".

5.3.2.1.4. Encripción

Las redes privadas virtuales garantizan la privacidad y la confidencialidad de la información haciendo uso de la encripción. En un muy breve resumen, encripción es una técnica que codifica la información de un modo que hace difícil o imposible su lectura, y la decodifica de modo que pueda ser leída nuevamente. A la información codificada se la llama cipher-text y a la información sin codificar, clear-text.

Cuando en una VPN se transmite información de un punto a otro, el Gateway de la VPN del punto de origen encripta la información en cipher-text antes de enviarla. En el otro punto, el Gateway receptor desencripta la información, es decir se vuelve clear-text, y luego la envía a la LAN.

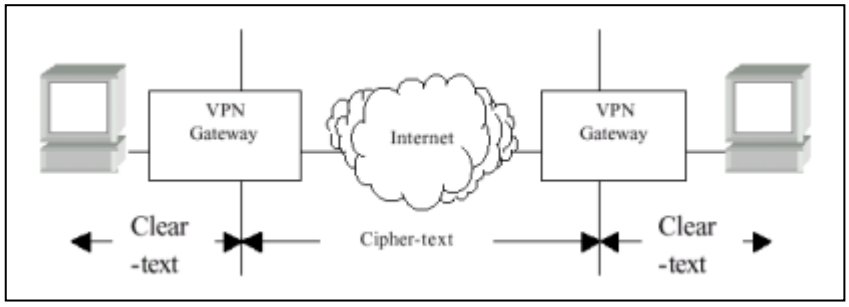


FIGURA 37. Técnica de Encriptación y Desencriptación

Un algoritmo de encripción es una técnica reproducible de cifrado y descifrado de información que puede ser realizada por personas o computadoras. Un ejemplo sencillo de un algoritmo de encripción sería reemplazar cada letra en una oración por la letra que le sigue inmediatamente a ésta en el alfabeto, obteniendo el cipher-text. Para leer la oración original, simplementa reemplazaríamos cada letra del cipher-text por la letra que la precede en el alfabeto.

En el pasado (y en algunas implementaciones actuales de baja calidad), la encripción permanecía segura manteniendo el algoritmo como un secreto. De este modo, no se podía leer un mensaje encriptado ya que se desconocía cómo había sido creado. El principal problema es que una vez que el algoritmo ha sido descubierto, se tiene acceso a toda la información que haya sido encriptada con el mismo. Peor aún, dado que la técnica de encripción es un secreto, resulta imposible determinar cuán buena es su calidad ya que muy poca gente puede probarla.

5.3.2.1.4.1. LLAVES

Ahora, dado que el método no es secreto, se evita que alguien acceda a la información mediante el uso de keys (claves). Una clave es un código secreto utilizado por el algoritmo de encripción para crear una versión única de cipher-text. Esta clave podría compararse con la combinación utilizada en una caja fuerte.

De este modo, la seguridad no depende de que el algoritmo de encripción sea un secreto. Actualmente, la mayoría de los estándares de seguridad de Internet (como DES y 3DES) toman esta postura de exponer su algoritmo ante cualquiera para que sea examinado y usado, brindando seguridad a través de la generación de claves únicas y con alta dificultad de ser conocidas. El nivel de seguridad generalmente depende en buena parte del largo de la clave (key lenght).

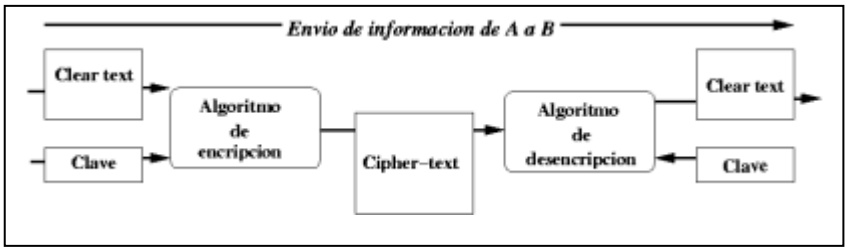


Figura 38. Envió de Información

Key Lenght

Utilizando algoritmos de encripción conocidos, la seguridad depende del largo de la clave. Una clave de 8 bits implica 2^8 combinaciones, mientras que una clave de 16 bits implica 2^{16} (65536) combinaciones posibles.

Con una clave de 16 bits, alguien podría realizar 65536 intentos antes de adivinar la clave que brinda acceso al *cipher-text*. Para una persona esto sería bastante difícil, pero para una computadora no sería un gran desafío y no tomaría demasiado tiempo recorrer todas las posibilidades.

Key lenght(bits)

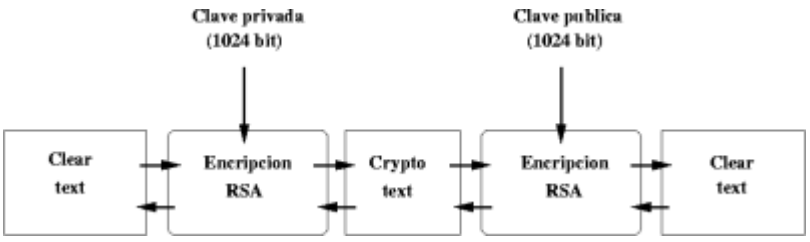
Combinaciones posibles
8 256
16 65.536
56 72.057.594.037.927.900

112 5.192.296.858.534.830.000.000.000.000.000.000
168 374.144.419.156.711.000.000.000.000.000.000.000.000.000.000.000

5.3.2.1.4.2. Claves Simétricas y Asimétricas

Cuando la misma clave es utilizada para encriptar y desencriptar la información, esta es denominada simétrica. Esto requiere que los puntos comunicados a través de la VPN posean la misma clave.

Otra técnica utilizada permite que la información sea encriptada con una clave, pero desencriptada con otra. La información encriptada con una clave no puede ser desencriptada con la misma y viceversa. Dos claves son requeridas, una para encriptar y otra para desencriptar, y estas no pueden ser intercambiadas. Estos pares de claves son denominadas claves asimétricas.



Con las claves asimétricas, a una clave se la denomina clave pública y a la otra clave privada. La clave pública en general no se mantiene en secreto. Si A desea enviarle un mensaje a B de modo tal que nadie más pueda verlo, entonces A encripta el mensaje usando la clave pública de B. B es el único capaz de desencriptar el mensaje, utilizando su clave privada. En otro ejemplo, si A envía un mensaje a B y desea que B pueda corroborar que efectivamente el mensaje proviene de A y no está falsificado, entonces A puede encriptar el mensaje utilizando su clave privada, y B puede desencriptar el mensaje con la clave pública de A. Si de este modo B logra desencriptar el mensaje correctamente, entonces el mensaje tiene que haber provenido de A.

Las claves asimétricas suelen ser muy largas - por ej. 1024 o 2048 bits -. El procesamiento de encripción requiere bastante potencia computacional y toma mucho tiempo. Por esto, las claves asimétricas son utilizadas para eventos que no ocurren frecuentemente, como establecer un túnel VPN. Las claves simétricas suelen ser mucho mas cortas - por ej. 56, 112 o 168 bits-, por lo que el

procesamiento de encripción utilizando claves simétricas es considerablemente mas rápido que con las asimétricas. Las claves simétricas se utilizan para transacciones de alta frecuencia, especialmente para la encripción de datos transmitidos sobre una VPN.

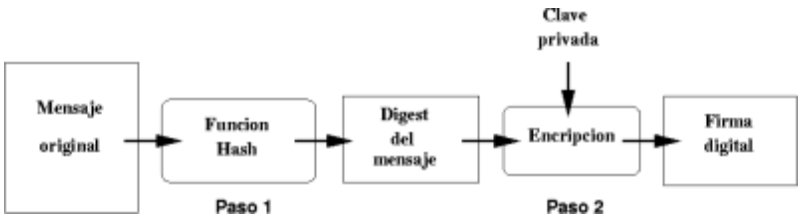
5.3.2.1.4.3. Autenticación

La tecnología de encripción garantiza la privacidad de la información al atravesar Internet. La tecnología de autenticación garantiza:

1. La identidad de los participantes de la VPN (los *gateways* y clientes son quienes dicen ser)
2. La integridad de la información recibida (no ha sido alterada en el camino)

Existen diversos modos de autenticación, siendo el mas común el uso de usuario y contraseña. El problema con este método en particular es que es un tanto inseguro: una de sus debilidades es que los usuarios deben elegir contraseñas que puedan recordar fácilmente. Esto significa que pueden ser adivinadas.

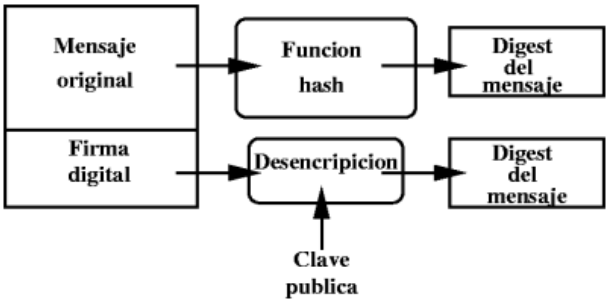
Una de las tecnologías mas utilizadas es la de certificados digitales, lo que permite autenticar e identificar tanto a personas como a sistemas sin el uso de usuarios y contraseñas. Un certificado digital es un registro que incluye varios datos, como el nombre de una persona, su dirección, su clave pública, y fechas de expiración del certificado que indican cuando éste deja de ser válido. En una VPN, los certificados digitales se utilizan para identificar a quien (persona o sistema) intenta conectarse a la VPN, y como medio de distribución de claves públicas.



Para evitar la falsificación, los certificados digitales se basan en la firma digital. La firma digital garantiza que la información recibida es auténtica y no ha sido alterada en modo alguno.

La creación de una firma digital es un procedimiento de dos pasos. Primero, el mensaje transmitido es procesado por un algoritmo de encripción particular: la

función de hash, que transforma un mensaje de largo arbitrario en un número único de longitud fija. Este número creado por la función hash es llamado el digest del mensaje. Si se cambia en cualquier forma el mensaje original, el digest de este cambia también. Las funciones de hash son muy conocidas, como SHA (Secure Hash Algorithm) y MD5(Message Digest 5). El segundo paso para crear la firma digital, es encriptar el digest del mensaje utilizando la clave privada. Esto da como resultado la firma digital.



Para garantizar la autenticidad de un mensaje, se crea una firma digital para el mismo y se incluye en el. El recipiente comprueba la autenticidad mediante:

1. La desencripción de la firma digital utilizando la clave pública del remitente (esto genera el digest del mensaje original).
2. Cálculo del digest del mensaje utilizando la función de hash (esto genera un nuevo digest del mensaje basado en los datos recibidos)
3. Comparación de resultados

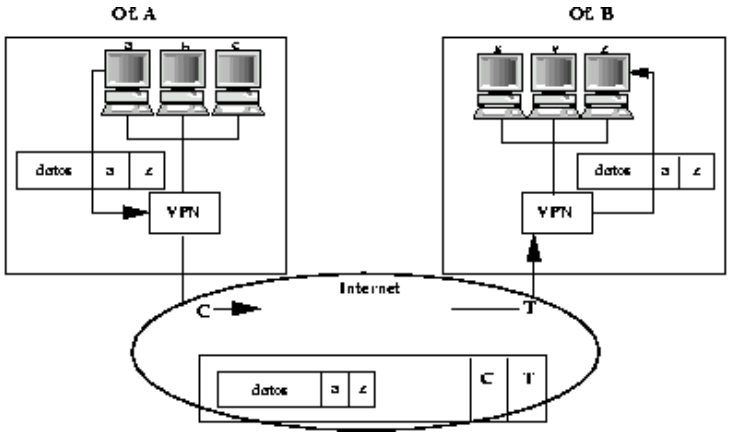
Si los resultados son idénticos, entonces el mensaje es auténtico y no ha sido alterado. Un mensaje que incluye una firma digital es un mensaje firmado.

Entonces, un certificado digital es un tipo especial de mensaje firmado que asocia a una persona, organización o computadora con una clave pública. Una entidad certificadora, llamada CA (*Certificate Authority*), acepta claves públicas con una prueba de identidad y crea certificados digitales dejándolos disponibles para otras personas. La entidad certificadora es un organismo confiable por ambas partes, el cual declara que efectivamente una clave pública pertenece a una persona, organización o sistema. Esta entidad puede utilizar protocolos de directorio como X.500 o LDAP para brindar sus servicios, o puede estar implementada haciendo uso de protocolos propietarios.

PKI (*Public Key Infrastructure*: Infraestructura de claves públicas) es una serie de servicios de seguridad para administrar claves, certificados digitales y políticas de seguridad. Las PKIs están diseñadas para dar soporte a grupos abiertos, a fin de manejar interacciones entre personas y sistemas que no se conocen previamente. Por ejemplo, en un sistema de compras a través de Internet. En particular, las PKIs posibilitan la coordinación entre múltiples CAs, dado que distintas personas o sistemas puede poseer certificados emitidos por distintas CAs.

Encapsulamiento

Encripción, claves, certificados y firmas digitales son las tecnologías de seguridad que garantizan la privacidad en una VPN. Ahora, generalmente, el envío de información en una VPN se realiza entre direcciones privadas. Es decir, entre direcciones no routeables vía Internet.



5.3.2.1.5. IPSec: Protocolo Seleccionado Para La Implementación

IPSec es el estándar *de facto* para garantizar la seguridad y autenticidad de las comunicaciones privadas a través de redes públicas basadas en IP, y se basa en estándares desarrolados por la IETF. Si bien la incorporación de IPSec es opcional en implementaciones de IPv4, debe estar presente en las implementaciones de IPv6, por lo que puede asumirse que IPSec será utilizado en forma creciente.

IPSec es realmente flexible y muy escalable, y si bien las implementaciones suelen ser bastantes complejas, una vez superada ésta se obtiene una notable estabilidad.

IPSec provee encripción y autenticación al nivel de IP en la pila de protocolos de red, por lo que protege todo tipo de tráfico transportado sobre IP y puede ser utilizado en routers, firewalls, servidores de aplicaciones e incluso desktops y laptops.

Se utilizan tres protocolos:

- AH(*Authentication Header*)
- ESP(*Encapsulating Security Payload*)
- IKE(*Internet Key Exchange*)

El protocolo IKE prepara las conexiones IPSec (ESP o AH) tras negociar ciertos parámetros (algoritmos a utilizar, claves, etc). Esto se realiza intercambiando paquetes en el puerto 500/UDP entre ambos *gateways*. IKE se encuentra definido en RFC2409.

AH brinda un servicio de autenticación a nivel de paquetes. Esta autenticación se brinda en forma separada a la encripción agregando un *header* de autenticación (AH) entre el *header* IP y el resto. Los detalles pueden encontrarse en RFC2402. Los datos de autenticación del *header* dependen tanto de una clave simétrica como de cada *byte* de los datos que son autenticados. La técnica utilizada es HMAC (RFC2104). Los algoritmos involucrados son SHA y MD5. AH utiliza el protocolo 51.

El protocolo ESP brinda encripción y autenticación de paquetes. Puede usarse con o sin AH.

La autenticación se realiza en forma similar a AH. Los algoritmos de encripción pueden variar de acuerdo a la implementación (los RFCs requieren únicamente DES y encripción nula). FreeS/WAN, la implementación de IPSec para Linux utiliza 3DES actualmente, aunque existen *patches* para agregar soporte de otros, como AES (Rijndael), Blowfish y CAST. Pese al requerimiento de DES, FreeS/WAN no lo implementa, ya que como anteriormente se dijo es inseguro. ESP utiliza el protocolo 50.

Modos

Pueden realizarse conexiones IPSec de dos modos diferentes: modo de transporte y modo de túnel.

El modo de transporte es una conexión de host a host y sólo involucra dos máquinas. Cada equipo realiza su propio procesamiento de IPSec y routea paquetes en forma acorde (algunos via IPSec).

El modo de túnel es una conexión entre *gateways*, los cuales proveen túneles para ser utilizados por máquinas clientes detrás de cada *gateway*. Las máquinas clientes no realizan ningún procesamiento de IPSec, tan sólo routean a los *gateways*.

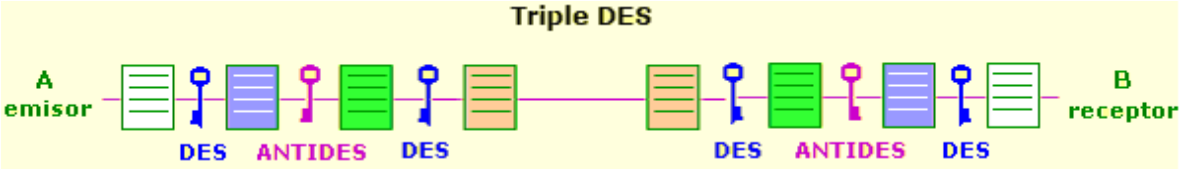
5.3.2.1.5. ALGORITMO PARA LA IMPLEMENTACION: DES, *Triple-Pass* DES y 3DES

Triple DES:

El sistema DES se considera en la actualidad poco práctico, debido a la corta longitud de su clave. Para solventar este problema y continuar utilizando DES se creó el sistema Triple DES (**TDES**), basado en tres iteraciones sucesivas del algoritmo DES, con lo que se consigue una longitud de clave de 128 bits, y que es compatible con DES simple.

Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se encripta el mismo bloque dos veces con dos llaves diferentes se aumenta el tamaño efectivo de la llave.

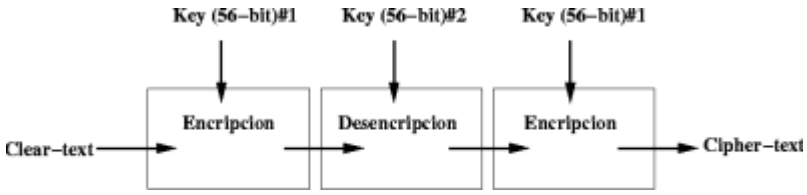
Para implementarlo, se toma una clave de 128 bits y se divide en 2 diferentes de 64 bits, aplicándose el siguiente proceso al documento en claro:



- Se le aplica al documento a cifrar un primer cifrado mediante la primera clave, C1.
- Al resultado (denominado ANTIDES) se le aplica un segundo cifrado con la segunda clave, C2. Y al resultado se le vuelve a aplicar un tercer cifrado con la primera clave, C1.

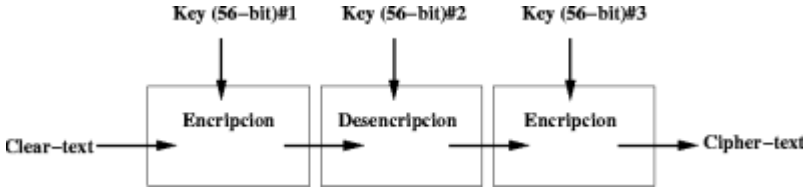
Triple-Pass DES es un sistema DES que incrementa la seguridad encriptando la información varias veces. Los datos son encriptados utilizando una clave de 56 bits. El *cipher-text* resultante es desencriptado utilizando una segunda clave de 56

bits. Esto da como resultado un *clear-text* que nada tiene que ver con lo que originalmente fue encriptado. Finalmente, los datos son nuevamente encriptados utilizando la primera clave:



A esta técnica de encriptar, desencriptar y volver a encriptar se la conoce como EDE. Incrementa efectivamente la clave de 56 bits a 112 bits.

3DES es un algoritmo de encripción que provee una seguridad aún mayor que *triple-pass* DES. Con 3DES, los datos son encriptados, desencriptados y vueltos a encriptar (EDE), pero con tres claves distintas. Esto resulta en una clave de 168 bits.

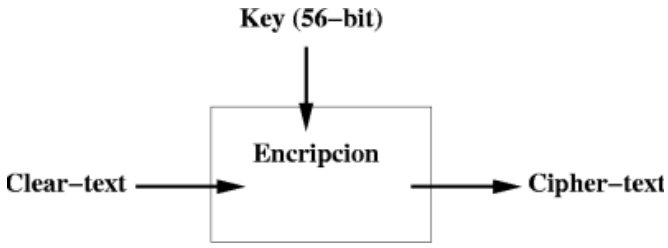


Generar claves seguras es sólo una parte de la ecuación. Para garantizar una seguridad continua, lo deseable es que las claves cambien constantemente cada breves periodos de tiempo. Del mismo modo en que los algoritmos que basan su seguridad en mantenerse secretos, sucede con las claves. Si se logra adivinar una clave, se tiene acceso a toda la información encriptada con ella. Por este motivo, en una buena implementación nuevas claves son generadas cada vez que un túnel VPN es establecido, y las claves son regeneradas cada cierto tiempo, generalmente cada dos horas.

DES (Data Encryption Standard):

El sistema DES usa claves de 56 bits para encriptar datos en bloques de 64 bits. La clave de 56 bits brinda 2^{56} combinaciones posibles. Esto implica que una persona valiéndose de una PC para adivinar la clave, tendría que recorrer durante alrededor de 20 años las distintas combinaciones. Por otro lado, si imaginamos una

gigantesca organización con millones de computadoras recorriendo en paralelo las distintas posibilidades, encontrar la clave podría reducirse a minutos. Por esto, DES puede ser seguro frente a atacantes casuales, pero no frente a una organización de amplios recursos realizando un ataque dirigido.

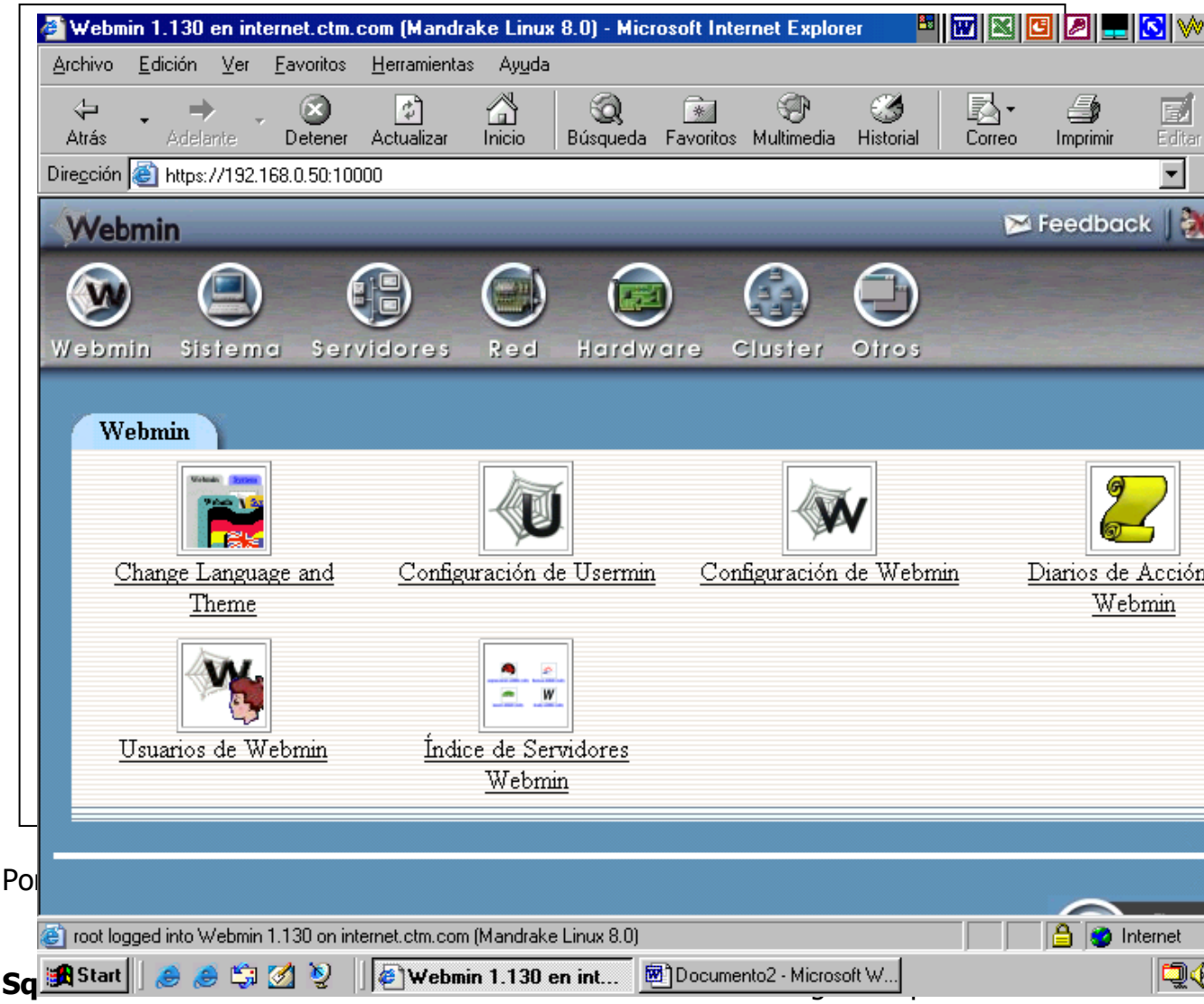


5.3.2.3 WEBMIN

Como la instalación del linux a realizamos sólo en modo texto, instalamos la herramienta WEBMIN, ya que por ser una herramienta gráfica nos permite administrar de un modo más amigable el servidor. Desde allí creamos un usuario para administrar el servidor, admón. Y la clave es: admon2004. Esto nos permite entregar esta clave a los profesores que van a administrar posteriormente el servidor, a esta cuenta le podemos colocar restricciones lo que nos beneficia por la seguridad del sistema. (ver marco conceptual)

Para acceder a webmin, dirija su navegador a http://nsXXXX.ovh.net:10000/ [con XXXX como número de servidor]
Nombre de Usuario: **root**
Password: contraseña que haya proveído en momento de la configuración del servidor.

5.3.2.4 INSTALACIÓN DEL PROXY

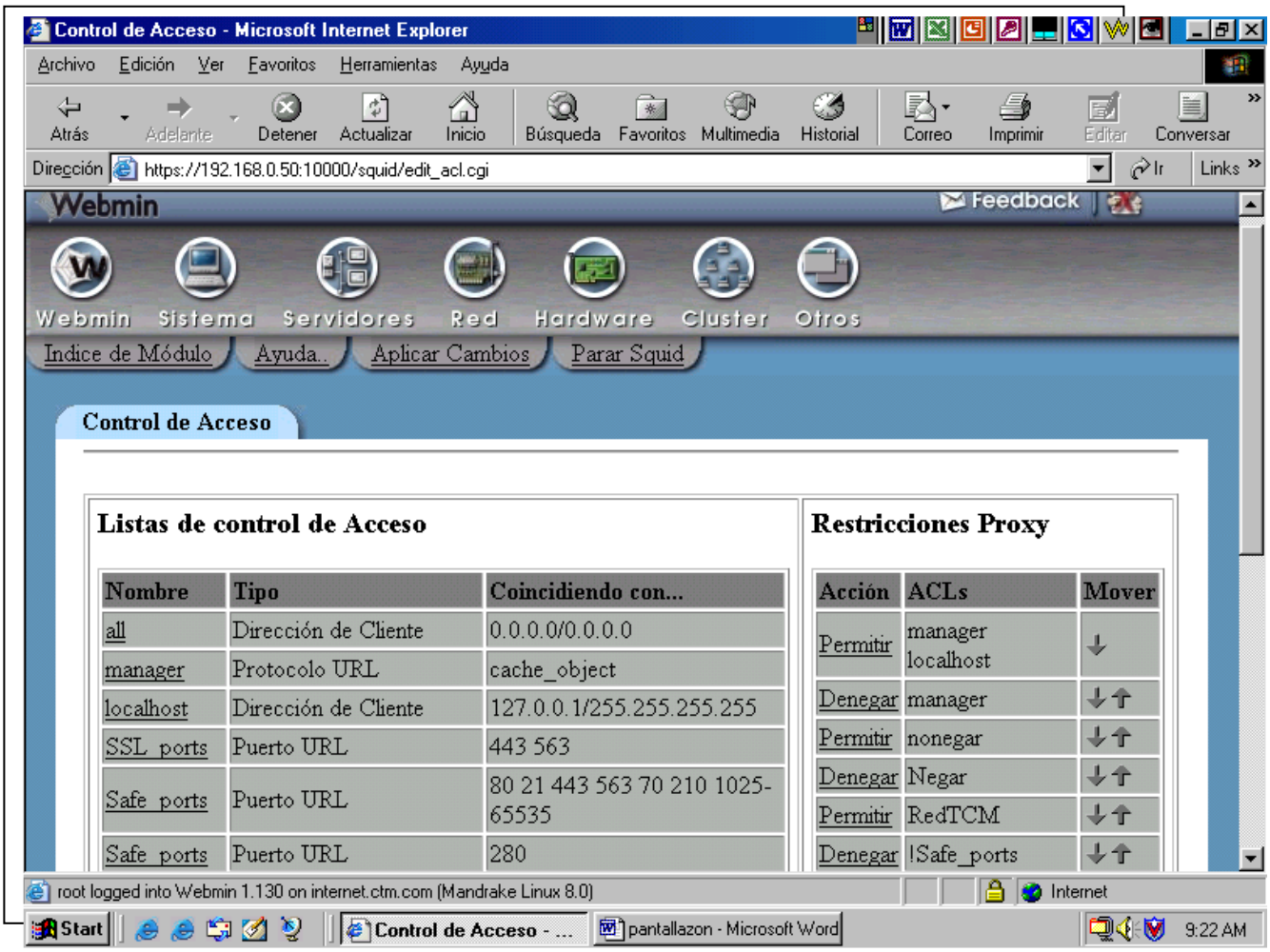


Po

Sq

para la salida a internet y la lista de contro de acceso.

Bloquear páginas a través del squid:



Como vemos en el pantallazo anterior, a través del squid podemos crear una regla en donde denegamos el acceso a determinadas páginas y ubicar la regla que actué de acuerdo al lugar de restricción en que la hemos dejado.

Se debe crear una regla para permitirnos el acceso y otra para no permitirnos. Estas listas quedan ubicadas en:

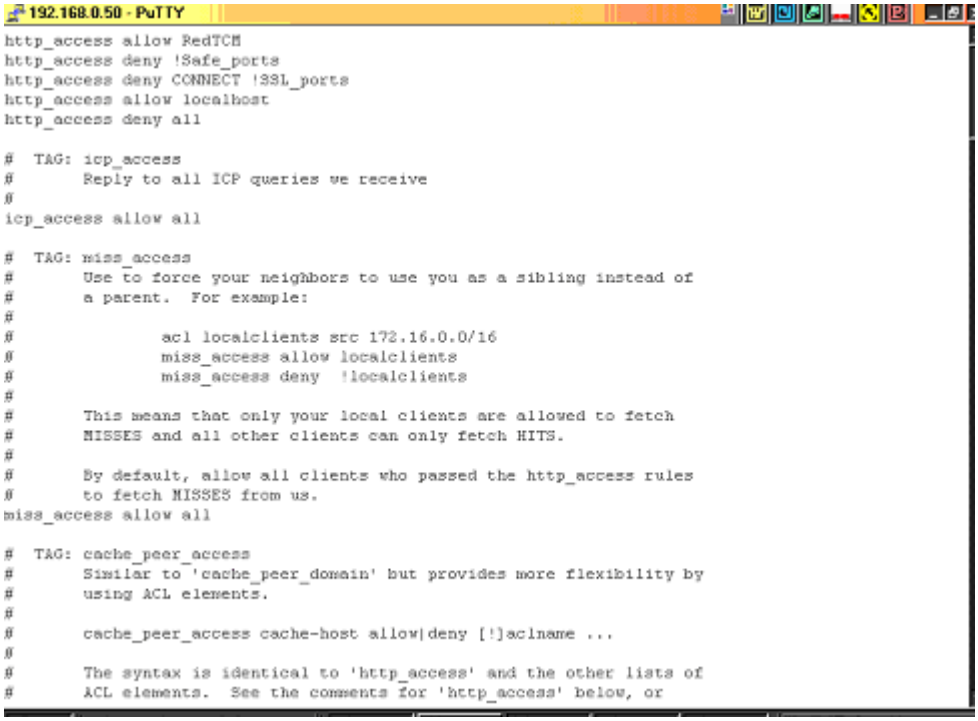
/etc/squid/permitidos

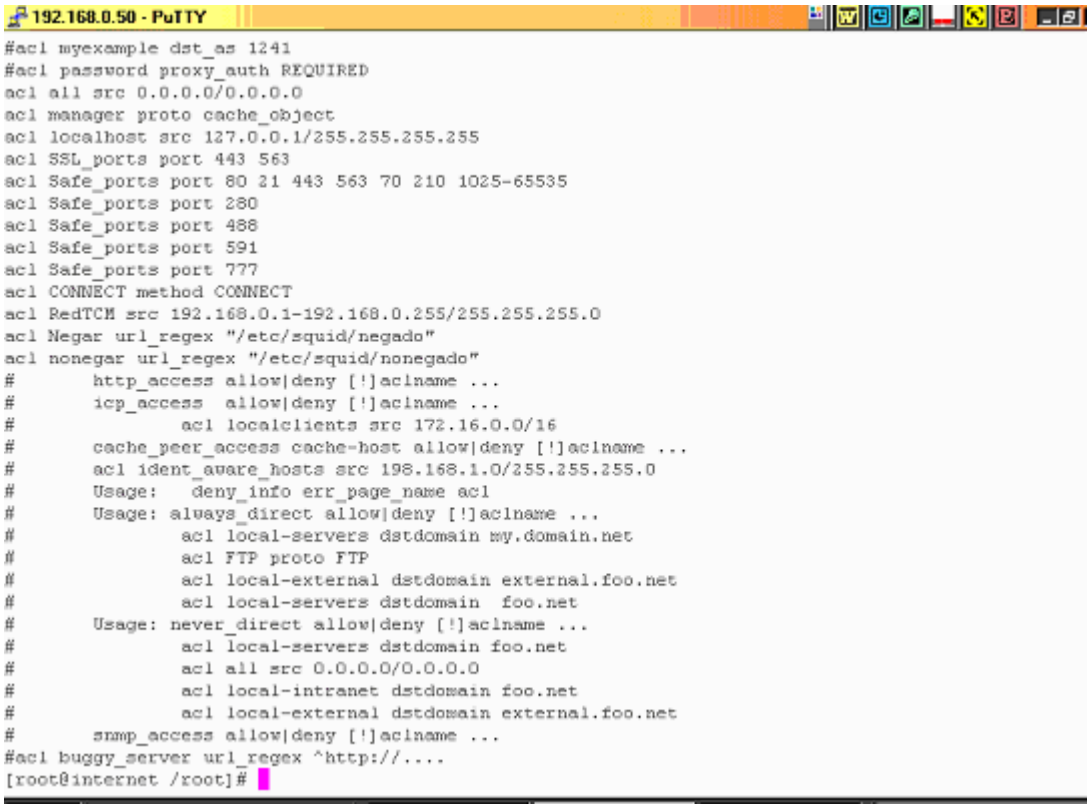
Se debe crear una regla que nos permita acceder y otra que nos niegue la autorización, ya que de lo contrario quedarían abiertos los permisos.

Cada vez que se realizan cambios en alguna regla del squid, se debe reiniciar el servicio, esto se hace con el comando:

Service squid restard

CONFIGURACION DE SQUID DESDE CONSOLA





5.3.2.5 Instalación de VPN

Para la configuración de las vpn, escogimos realizarla con fresswan el cual maneja el protocolo IPSEC, con este protocolo tenemos solución de entunelamiento y encriptación de la información. (ver marco Teórico)

Fresswan se instala del CD de instalación de red Had 9.0 y el SSH, es importante instales las librarías requeridas por fresswan :

\rpms\libgmp31

De igual manera se realiza la conexión al colegio Gabriel Echavarría a través del WEBMIN y realizamos la misma instalación en el servidor.

Los dos Archivos que deben ser tenidos en cuanta para configuración de las VPN :

/etc/fresswan/ipsec.conf

/etc/fresswan/ipsec.secret

Escogemos que colegio va a la derecha del diseño de las vpn y cual a la izquierda, para este caso escogió el colegio Tecnológico de Madrid como el de la izquierda y el Gabriel Echavarría como el de la derecha.

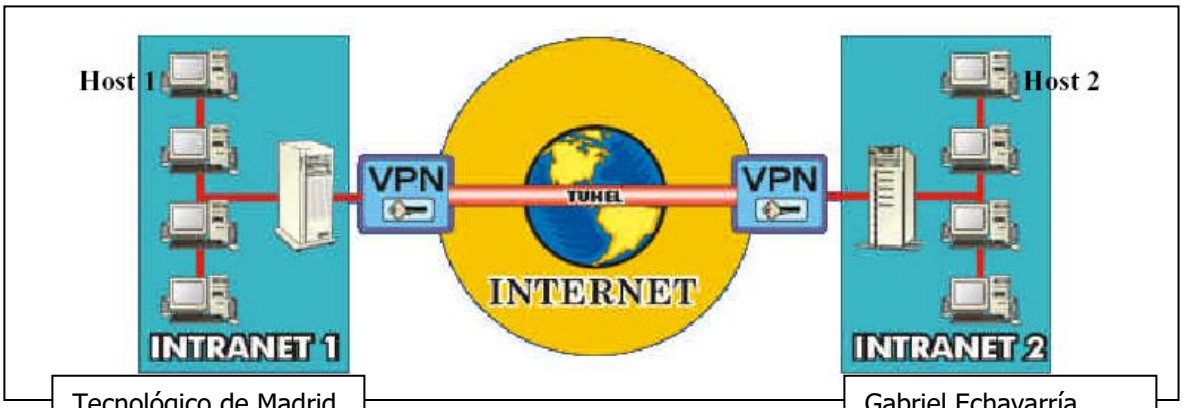


Figura 39. Modelo VPN. Colegios de Madrid

Generamos las llaves para intercambiar la información con el comando:

Ipsec rsasigkey 512

Esto quiere decir que se generan llaves a 512 bytes, la llave generada se copia en el archivo ipsec.conf, esto se hace en el campo:

leftrssagkey

La configuración del archivo.conf es igual para los dos colegios, lo que es diferente es la configuración del archivo ipesec.secret

En el campo Lettid= tecno
Right= colge
Left= Dir. Pública del tecnológico
Right= Dir. Pública del Echavarría

5.3.2.5.1 Tecnología utilizada para la implementación

Obviamente existen diferentes tecnologías sobre las que una VPN puede estar implementada (ver marco conceptual). A continuación destacamos la tecnología más importante en estos momentos:

5.3.2.5.1.1 IPSEC.

Ipsec es una tecnología que protege los paquetes IP de la capa de red, así se forma una capa segura de un nodo de la red a otro, definido con el advenimiento del IPv6. Aunque IPv6 está muy poco difundido en este momento, la tecnología marco IPSec se está utilizando ya, lo que asegura, entre otras cosas, la interoperatividad entre sistemas de diversos fabricantes y sistemas operativos, como Linux, windows macintosh, firewalls y routers comerciales. IPSec integra confidencialidad, integridad y autentificación en un mismo marco interoperante por lo que esta será la opción escogida para la implementación de las VPN. Además, como trabaja a nivel IP, es transparente a la aplicación, ya que esta no necesita modificación alguna, y ni siquiera se entera de la existencia de criptografía intermedia, a diferencia de protocolos de nivel de transporte, como son los túneles sobre TCP (SSL, SSH).

IPsec utiliza dos protocolos para la protección de los paquetes IP: "Cabecera de Autenticación" (AH: Authentication Header) y "Cargo de Seguridad Encapsulado" (ESP: Encapsulated Security Payload).

AH provee autenticación, integridad y protección a la réplica, mientras que **ESP** provee además confidencialidad (mediante cifrado). Una Asociación de Seguridad (**SA**: Security Association) es un enlace seguro de IPsec definido por un único flujo unidireccional de datos desde un único punto hasta otro. Consiste en el acuerdo de las dos partes comunicantes en el método utilizado para la comunicación segura. Todo el flujo de tráfico sobre un SA se trata del mismo modo. El tráfico puede ser entre dos hosts, entre un host y una pasarela de seguridad (Security Gateway) o entre dos pasarelas de seguridad.

Si el enlace es entre dos hosts, la SA es de **modo transporte**. En este modo de funcionamiento de SA, las cabeceras de seguridad se añaden entre la cabecera de la capa de red IP y la cabecera de transporte (TCP o UDP), garantizando la seguridad al paquete IP sin cabecera.

AH en modo transporte: **IP Header AH Header TCP Header Carga**

ESP en modo transporte: **IP Header ESP Header TCP Header Carga ESP Trailer ESP Authen** Si alguno de los extremos del enlace es una pasarela de seguridad, se utiliza el **modo túnel** de SA. En este caso, las cabeceras de seguridad engloban también a la cabecera IP original del paquete IP, teniendo que añadir una nueva cabecera IP que cubre solamente el salto al otro extremo de la conexión segura.

AH en modo túnel:**New IP Header AH Header IP Header Carga**
ESP en modo túnel: **New IP Header ESP Header IP Header Carga ESP Trailer ESP Authen** Cada paquete IP se asigna a una SA mediante tres campos: Dirección IP del Destino, Índice del Parámetro de Seguridad (SPI: Security Parameter Index) y Protocolo de Seguridad (AH o ESP).

Sin embargo, el protocolo no estipula cómo se han de autentificar los pares ni cómo se intercambian las claves de sesión. Estas tareas son gestionadas por el protocolo de intercambio de claves de Internet IKE (Internet Key Exchange). IKE permite que dos puntos extremos puedan establecer conexiones seguras, utilizando la infraestructura de llaves precompartidas o llaves públicas (PKI), certificados digitales administrados por una autoridad certificadora---un servicio externo o interno que registra las llaves públicas. IKE permite también que una red privada virtual (VPN) pueda ampliarse a cientos de puntos extremos, mediante el uso del equivalente a una tarjeta de identificación digital que identifica cada punto extremo.

IPsec se compone de tres protocolos:
· **AH** (Authentication Header, *Encabezado de Autentificación*), que proporciona autentificación a nivel de paquetes.
· **ESP** (Encapsulating Security Payload, *Encapsulación Segura de Datos*), que proporciona tanto autentificación como cifrado a una conexión.
· **IKE** (Internet Key Exchange, *Intercambio de Llaves por Internet*), que gestiona la configuración de los parámetros de la conexión, incluyendo el intercambio de llaves criptográficas para el cifrado y autentificación.

5.3.2.6. DISEÑO DE PÁGINAS WEB.

En la parte de diseño de páginas WEB del presente trabajo pretende elaborar una manera que permita la distribución y el almacenamiento centralizado de diferentes tipos de documentos, material de apoyo e información de los colegios Gabriel Echevarria y Tecnológico de Madrid

Actualmente los documentos y material de apoyo (textos, manuales, prácticas, etc.) en los colegio se realiza por carteleras murales son distribuidos entre los alumnos como material impreso, empleando documentos originales o fotocopias proporcionadas por el docente. Los beneficios con el desarrollo de las paginas Web:

- Ahorro en el tiempo de distribución y acceso a documentos e información referentes a los colegios.
- Existencia de correros electrónicos y VPN como forma de distribución de documentos y material de apoyo e información. Se contara con Módulo de Control de Usuarios, para la validación de usuarios y mantenimiento de cuentas de acceso al sistema. Módulo de Publicación, mediante el cual se agregará y mantendrá el material correspondiente a los colegios Gabriel Echevarria y Tecnológico de Madrid.

5.3.2.6.1 MÈTODO Y PROCEDIMIENTO

Interfaz de usuario

Macromedia Dreamweaver; diseño de las páginas de presentación de la información.

Servidor: PHP, para procesamiento de los datos y la generación de páginas HTML MySQL, servidor de base de datos SQL

Aplicación web

El sistema desarrollado utilizó el enfoque de aplicación web, donde la generación de la interfaz del usuario es dinámica y el acceso a los datos se realiza de manera local, entre el interprete de PHP y MySQL (el usuario en ningún momento se conecta con la base de datos).

La presentación de la interfaz de usuario e interacción con los elementos que la componen sucede en un navegador web, en el lado del usuario, ésta relación se refleja en el figura 38.

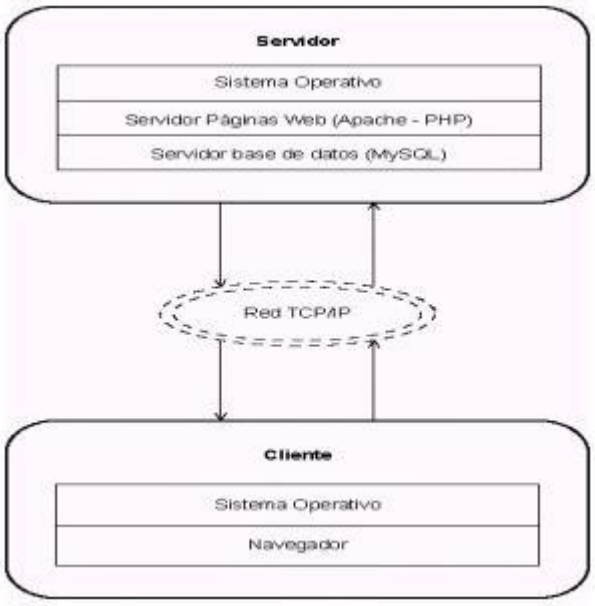


Figura 40 : Arquitectura global del sistema

La comunicación entre el usuario y el servidor se realiza utilizando el protocolo TCP/IP, ya sea dentro de una red local o por Internet para acceso remoto. Una diagramación del acceso al sistema está presente en el figura 39.

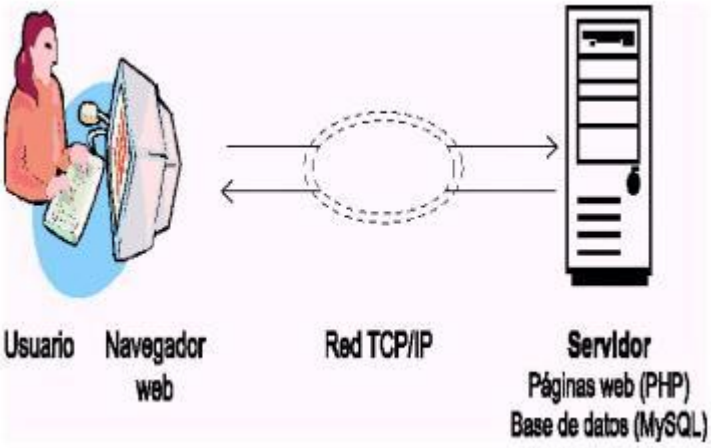


Figura 39: Acceso al sistema

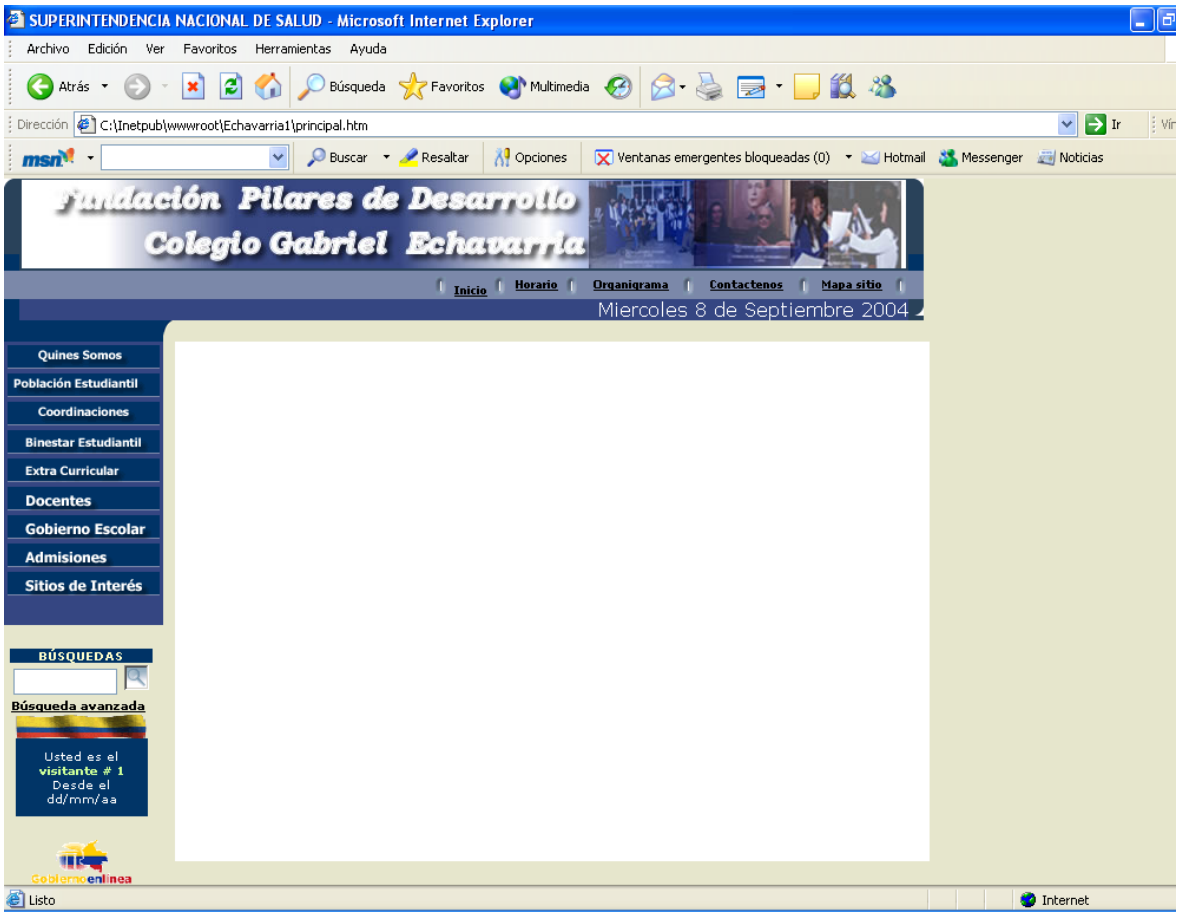
El desarrollo de aplicaciones web con acceso a base de datos es posible, y en especial, muy conveniente para la distribución de grandes volúmenes de información con acceso remoto.

Por la naturaleza de scripts PHP, interpretados en tiempo de ejecución, las modificaciones o actualizaciones del sistema están inmediatamente disponibles para los usuarios.

El diseño cumple con los requerimientos de los colegios:

PAGINA INCIAL COLEGIO GABRIEL ECHAVARRIA

PAGINA INTERNA COLEGIO GABRIEL ECHAVARRIA


SUPERINTENDENCIA NACIONAL DE SALUD - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección C:\Inetpub\wwwroot\Echavarria1\principal.htm
Buscar Resaltar Opciones Ventanas emergentes bloqueadas (0) Hotmail Messenger Noticias
Fundación Pilares de Desarrollo
Colegio Gabriel Echavarria
Inicio Horario Organigrama Contactenos Mapa sitio
Miercoles 8 de Septiembre 2004
Quines Somos
Población Estudiantil
Coordinaciones
Binestar Estudiantil
Extra Curricular
Docentes
Gobierno Escolar
Admisiones
Sitios de Interés
BÚSQUEDAS
Búsqueda avanzada
Usted es el visitante # 1 Desde el dd/mm/aa
Gobiernoenlinea
Listo
Internet

PAGINA DE INCIO COLEGIO TECNOLOGICO DE MADRID


I.E.D TECNOLOGICO DE MADRID
Filosofía del Colegio
QUIENES SOMOS
NORMATIVIDAD
GOBIERNO ESCOLAR
CONTRATACION
CURRICULO
DIRECTORIO
SIGUS
Ubicado en el barrio el Sociego; con una planta física nueva de propiedad del municipio, con cuerpo docente naminado por el mismo, con el cual se pretende dar al sector y a la comunidad de Madrid, personas integras en VALORES, CONDUCTAS, HABILIDADES, DESTREZAS y sobre todo, capaces de tomar decisiones y enfrentar desafios para la solución de sus problemas personales, familiares y

BIBLIOGRAFIA

Páginas de Internet:

htpp://www.vpnlabs.org/
htpp://www.compnetwording.about.com
htpp://www.pcworld.com
htpp://www.homenethelp.com
htpp://www.geocities.com

http://freswan.org/.com
http://www.linuxparatodos.com/linux/19-0-como-squid-general.php

Interconexión de dispositivos de red CISCO, Steve Mcquerry, Pearson Education.S.A. Madrid 2001.

Interconexión a Internet, Steve Mcquerry Perarson Education. S.A. Madrid 2011.

Colegio Gabriel Echavaria - Janeth Parra
Colegio Tecnológico - Cecilia Matiz

CONCLUSIONES

Con la realización de este trabajo se concluye

1. Se logro sensibilizar a las directivas de 2 instituciones para poder ejecutar e implementar este proyecto.

2. En La fase de exploración se reconoció las salas de informática con las que cuenta cada Colegio, y se determinó las falencias en común de los dos Colegios, Gabriel Echavarria y tecnológico.

3. Se compartió y enriqueció con aportes individuales una idea que fue creciendo y convirtiéndose en beneficio social y de gran impacto educativo.

4. Se beneficio a una comunidad educativa de estrato socioeconómicos bajos con la implementación de nuevas tecnologías, después de haber realizado un estudio de costos, se trabajo con plataforma y software libre, para reducir costos.

5. La implementación de la VPN y la elaboración de las páginas Web para las instituciones, son un hecho real que beneficia ampliamente la calidad de la educación en las dos instituciones.

6. A nivel individual y colectivo la ganancia en el aprendizaje de la implementación de nuevas tecnologías en instituciones educativas fue significativo y de gran trascendencia por que tuvimos la oportunidad de crecer nuestro espíritu investigativo y por ello ampliar profundamente nuestros conocimientos.

7. Este trabajo contribuye al mejoramiento de la calidad de la educación, por el aporte a las instituciones educativas de herramientas básicas para el acceso de los estudiantes, docentes y padres de familia a las nuevas tecnologías.

Anexo A

Propuesta de servicio de la Empresa de Teléfonos de Bogota

CONDICIONES ESPECIALES PARA LA PRESTACION DEL SERVICIO INTERNET EXTREMO DE ETB

La ETB S.A. ESP [ETB] en su calidad de Internet Service Provider [ISP] prestará el Servicio Internet Extremo de ETB por medio de su tecnología ADSL a **EL CLIENTE**, cuya información se ha relacionado anteriormente, de acuerdo con las presentes condiciones especiales.

Para el cabal entendimiento de las condiciones ofrecidas, a continuación se establecen las siguientes definiciones:

A. ADSL: Son las siglas de "Asimetric Digital Suscriber Line" [Línea de Usuario Digital Asimétrica]. Es una tecnología que consigue transformar las líneas telefónicas convencionales de **ETB** en líneas de acceso de banda ancha para navegar en Internet a alta velocidad.
B. CARGO MENSUAL: es el valor mensual que refleja los costos económicos para garantizar la disponibilidad permanente y continua del Servicio Internet Extremo de ETB, y la utilización de este.
C. CARGO DE INSTALACION: es el valor que **EL CLIENTE** cancela a **ETB** por la activación y conexión del Servicio Internet Extremo de ETB.
D. CARGO EQUIPO ADSL: es el precio que **EL CLIENTE** cancela a **ETB** por concepto de los Equipos ADSL suministrados por ésta.
E. CITA CONCERTADA [AGENDAMIENTO]: Es la cita que se acuerda entre **ETB** y **EL CLIENTE** para realizar las labores de revisión del estado de la red de cobre de la línea telefónica del cliente e instalaciones necesarias para prestar y acceder al Servicio Internet Extremo de ETB.
F. **EL CLIENTE**: Es la persona que solicita y obtiene el Servicio Internet Extremo de ETB con el fin de obtener los beneficios propios de este servicio.
G. CORREO POP3: Es un servicio, que permite por medio del protocolo POP3 la posibilidad de configurar en el equipo informático de **EL CLIENTE**, un programa administrador de correo, para poder recibir los mensajes directamente en el PC sin tener que ingresar al Correo Web.
H. CORREO WEB: Es el servicio de correo electrónico que puede ser utilizado al accesar www.etb.com.co con el objeto de intercambiar mensajes vía Internet con otras personas.
I. EQUIPOS ADSL: Término utilizado para designar el conjunto de bienes constituido por el Modem ADSL, el Splitter y/o los Micro filtros, elementos y demás accesorios suministrados e instalados por **ETB** en el lugar designado por **EL CLIENTE**.
J. EQUIPOS INFORMATICOS: Son los computadores y los equipos Hub, Router o Concentradores de propiedad de **EL CLIENTE**, a los cuales se les configura una conexión con el Módem ADSL para acceder al Servicio Internet Extremo de ETB.
K. FACILIDADES: son los "productos de software" conexos al Servicio Internet Extremo de ETB, tales como: correo web, correo POP3, PWP.
L. FACTURA DE SERVICIOS PUBLICOS: Es la cuenta que **ETB** envía a **EL CLIENTE** por causa del consumo y demás servicios inherentes en desarrollo del contrato de servicios públicos de **ETB**, y en la cual se incluyen, adicionalmente, los valores correspondientes a: (i) el cargo por instalación (ii) el cargo mensual; (iii) el cargo por los equipos ADSL, y (iv) el valor de los servicios inherentes al Servicio Internet Extremo de ETB.
M. LINEA TELEFONICA ETB: Es la línea telefónica **ETB** de **EL CLIENTE** a través de la cual se va a prestar el Servicio Internet Extremo de ETB.
N. MICROFILTROS: Dispositivos que pueden ser conectados a cada extensión telefónica de **EL CLIENTE**, para garantizar el buen funcionamiento de la línea de voz sobre la tecnología ADSL, evitando la interferencia en el funcionamiento simultáneo de los dos servicios.
O. MODEM ADSL: Equipo terminal instalado en el equipo informático de **EL CLIENTE**, que permite establecer una conexión de Internet entre un computador y el ISP, por medio de la línea

telefónica.
P. PWP: Es el servicio de alojamiento de páginas personales en un servidor de ETB haciéndolas disponibles al público en el Internet.
Q. REACTIVACION: Es el conjunto de actividades necesarias realizadas por **ETB** o por el personal técnico que éste designe, con el fin de activar nuevamente y volver a prestar el Servicio Internet Extremo de ETB, cuando el mismo fue suspendido por mora en el pago o por solicitud de **EL CLIENTE**.
R. RED DE TPBC: La Red de Telefonía Pública Básica Conmutada [TPBC] es el conjunto de elementos que hacen posible la transmisión conmutada de voz, con acceso generalizado al público.
S. SERVICIO DE INTERNET: Es el servicio de valor agregado prestado por **ETB**, por medio del cual **EL CLIENTE** accede a la red de Internet.
T. SERVICIO DE INSTALACION: Es el conjunto de actividades realizadas por **ETB** o por el personal técnico que ella designe, para la instalación de los Equipos ADSL en las instalaciones y equipos informáticos de **EL CLIENTE** para la prestación del Servicio Internet Extremo de ETB.
U. SERVICIO MULTIUSUARIO: Es la posibilidad de utilizar simultáneamente el Servicio Internet Extremo de ETB desde más de un computador.
V. SOPORTE TELEFONICO: Es el servicio de información y orientación telefónica que presta **ETB** a **EL CLIENTE** con ocasión del Servicio Internet Extremo de ETB.
W. SUSPENSION TEMPORAL: Es la posibilidad que tiene EL CLIENTE de solicitar suspensiones voluntarias en el servicio Internet Extremo de ETB de acuerdo con las políticas definidas por **ETB**.
X. SPLITTER: Dispositivo que puede ser conectado a la toma principal del inmueble de **EL CLIENTE** en el momento de hacer la instalación del Servicio Internet Extremo de ETB, con el propósito de independizar la señal de datos de la señal de voz, permitiendo así su uso simultáneo. El uso de un Splitter puede sustituir el uso de microfiltros sobre las extensiones telefónicas.
Y. TPBC: Es el servicio público domiciliario de telefonía pública básica conmutada, prestada por **ETB**.
Z. USUARIO: Es la persona natural o jurídica que se beneficia con la prestación del servicio de TPBC de **ETB**.

Previas las anteriores definiciones, a continuación se establecen las condiciones especiales y características del Servicio Internet de Banda Ancha de ETB:

1. Las Condiciones Generales de prestación del servicio de Internet de **ETB**, son aplicables en todo lo que no contradiga las presentes condiciones especiales. **EL CLIENTE** declara que conoce y ha leído una copia de dichas Condiciones Generales, que ha tenido a la mano y acepta integralmente. Con el fin de asegurar un mejor servicio, **ETB** ajustará periódicamente las "Condiciones Generales" así como las "Condiciones Especiales" y las características del Plan escogido por EL CLIENTE, condiciones y ajustes que aparecerán publicados en la página web www.etb.com.co .

2. Las Condiciones de Privacidad de clientes inscritos en los planes de servicio de Internet ETB, son aplicables a **EL CLIENTE** del servicio objeto de las presentes condiciones especiales. **EL CLIENTE** declara que conoce y ha leído una copia de las condiciones de privacidad, que ha tenido a la mano y acepta integralmente. Las Condiciones de Privacidad permanecen publicadas en la página web www.etb.com.co.

3. Las condiciones específicas correspondientes a algunas de las facilidades ofrecidas que aparecen publicadas en la página web señalada anteriormente y que han sido suministradas a **EL CLIENTE**, también son aplicables al Servicio Internet Extremo de ETB. **EL CLIENTE** declara que conoce y ha leído copia de las condiciones específicas de algunas de las facilidades ofrecidas y las acepta.

4. EL CLIENTE podrá suspender o cancelar en cualquier momento el Servicio Internet Extremo de ETB, previa comunicación sobre tal decisión vía e-mail, fax o por escrito a **ETB** con treinta (30) días de antelación a la fecha de terminación deseada, salvo que haya aceptado las cláusulas de permanencia mínima, prórroga automática y multa por terminación anticipada, tal como se establecen más adelante.

5. EL CLIENTE podrá solicitar a **ETB** suspensiones temporales en su servicio Internet Extremo de ETB, con siete [7] días de anticipación a la fecha deseada para realizar la suspensión. Estas podrán solicitarse hasta por dos veces en el año y el tiempo total de la suspensión no podrá exceder los 30 días calendario sumando las dos suspensiones y tampoco podrán ser inferiores a siete [7]días calendario cada una. En estos casos el contrato se entiende extendido por el tiempo que solicitó las suspensiones. **ETB** procederá a hacer los descuentos sobre el tiempo de suspensión en la factura correspondiente al mes siguiente de cumplimiento del tiempo de suspensión solicitado. **ETB** mantendrá publicados en el Portal de ETB los parámetros, montos y descuentos a efectuar por concepto de dichas suspensiones.

6. Para la buena prestación del Servicio Internet Extremo de ETB, **EL CLIENTE** debe contar con una línea telefónica **ETB**, además el equipo informático de **EL CLIENTE** deberá contar con las siguientes características: (i) un puerto USB disponible, y para los casos en que se desee tener un servicio multiusuario, debe tener una tarjeta interfaz (PCI) para redes ethernet en cada equipo con conector RJ45; (ii) un procesador con velocidad recomendada de 150 MHz o superior (Pentium o compatible); (iii) 32 Mb de memoria RAM como mínimo; (iv) sistema operativo Windows 95 o superior; y, (v) un Hub, Router o Concentrador, en los casos en los cuales se desee tener un servicio multiusuario.

7. ETB instalará los Equipos ADSL en el lugar, en los equipos informáticos y en las líneas telefónicas señaladas por **EL CLIENTE**, dentro de los ocho (8) días hábiles siguientes a la aprobación por **ETB** de la solicitud de aquél.

8. EL CLIENTE se compromete a conservar en el mismo lugar indicado en la solicitud, los Equipos ADSL instalados por **ETB**, los equipos informáticos y las líneas telefónicas a través de las cuales se presta el Servicio Internet Extremo de ETB.

9. ETB garantiza por un (1) año contado a partir de la instalación, el buen funcionamiento del Equipos ADSL que ella misma suministre e instale, siempre que la incidencia diagnosticada se deba a vicios o defectos originados en los mismos. En estos casos, **ETB** procederá a reemplazar los Equipos ADSL sin costo alguno para EL CLIENTE.

10. ETB prestará el servicio de mantenimiento sobre los Equipos ADSL que ella misma instale, en forma gratuita, durante el término y por los eventos cubiertos por la garantía.

11. Terminado el período de garantía, **ETB** prestará el servicio de mantenimiento correctivo, previa solicitud de **EL CLIENTE**, al precio que aquélla establezca y si fuere necesaria la sustitución de alguno de los Equipos ADSL, **EL CLIENTE** asumirá el valor de cada uno de ellos. El valor por el servicio de mantenimiento y los valores de los Equipos ADSL sustituidos, una vez vencida la garantía, serán cargados en la siguiente factura de servicios públicos de **ETB** que se expida después de la sustitución o del mantenimiento. Si **EL CLIENTE** adquiere de un proveedor diferente a **ETB** el Módem ADSL, ésta cobrará el correspondiente valor del servicio de mantenimiento en la factura de servicios públicos de **ETB**.

12. ETB prestará el servicio de mantenimiento ó soporte técnico en el lugar donde se encuentre instalado el servicio, en los casos en que **EL CLIENTE** lo requiera. **EL CLIENTE** deberá asumir el valor de esta actividad y de los conceptos que se generen de la misma, los cuales serán cargados en la siguiente factura de servicios públicos de **ETB**.

13. EL CLIENTE deberá dar a **ETB** información precisa y completa a fin de mantener actualizados sus datos. Así mismo, deberá notificar a **ETB** dentro de los treinta (30) días calendario siguientes, de cualquier cambio en sus datos o información.

14. ETB podrá modificar las presentes condiciones o sus políticas de uso en cualquier momento a su criterio. Cualquier modificación tendrá efecto inmediato ya sea a través de la aparición de un mensaje en la página de Internet de **ETB**, el portal de ETB o por medio de un mensaje de **ETB** enviado a **EL CLIENTE** por correo electrónico. Si **EL CLIENTE** considera inaceptable la modificación puede solicitar la cancelación del servicio, mediante el envío de un correo electrónico a la dirección electrónica que **ETB** señale dentro de los diez [10] días calendario siguientes a la aparición del mensaje o de la notificación por correo electrónico que haya hecho **ETB**. Si pasado este término **EL CLIENTE** continua haciendo uso del servicio, tal situación se considerará una aceptación de la(s) modificación(es). En el evento en que **EL CLIENTE** haya aceptado las cláusulas de permanencia mínima, prórroga automática y multa por terminación anticipada y solicita la cancelación del servicio dentro del periodo de permanencia mínima por la causa prevista en este numeral, deberá pagar la multa establecida, así como, cualquier concepto relacionado con el servicio de Internet Extremo de ETB.com, de acuerdo con lo previsto en el anexo de las presentes condiciones.

15. Como requisito para la prestación del Servicio Internet Extremo de ETB, **EL CLIENTE** debe ostentar y mantener la calidad de usuario del servicio de TPBC de **ETB**.

16. ETB realizará los cobros derivados de la prestación del Servicio Internet Extremo de ETB y demás servicios inherentes, por mensualidades vencidas, valores que se incorporarán en la factura de servicios públicos de **ETB**, con cargo a la línea telefónica indicada por **EL CLIENTE** al diligenciar la solicitud del servicio. Los pagos deberán realizarse de acuerdo con la fecha límite establecida en la factura.

17. Corresponde pagar a **EL CLIENTE**, en forma oportuna el valor del Servicio Internet Extremo de ETB de acuerdo con las tarifas establecidas para el cargo mensual, el cargo de instalación, el valor de los equipos ADSL y demás cargos inherentes al servicio. **ETB** ofrecerá al **EL CLIENTE** la posibilidad de financiar a través de la factura de servicios públicos de **ETB** los conceptos generados por el cargo de instalación y los cargos relacionados con los EQUIPOS ADSL en los casos en que aplique. Los plazos de financiación ofrecidos por **ETB** estarán comprendidos entre los 2 y 12 meses. **EL CLIENTE** asumirá los costos de financiación de acuerdo a las tasas de interés fijadas por **ETB**.

18. Los valores correspondientes al servicio de TPBC y demás conceptos cobrados a través de la factura de servicios públicos no incluyen las sumas generadas por la prestación del Servicio Internet Extremo de ETB. Estos se cobrarán independientemente y se sujetarán a lo establecido en la Ley 142 de 1994, en el contrato de servicios públicos de **ETB** y en la regulación vigente sobre la materia.

19. En caso de no pago de la segunda factura por parte de **EL CLIENTE** por los conceptos asociados a la prestación del Servicio Internet Extremo de ETB, este servicio será suspendido en

forma inmediata. Si **EL CLIENTE** efectúa el pago de los valores adeudados a **ETB** antes del vencimiento de la cuarta factura, el servicio Internet Extremo será reactivado. Si **EL CLIENTE** no cancela la cuarta factura de servicios públicos, **ETB** terminará unilateralmente el presente acuerdo y procederá al corte del servicio de Internet ADSL; como consecuencia de lo anterior, las conexiones serán retiradas, y **EL CLIENTE** deberá pagar las deudas y sanciones a favor de **ETB**. En este evento, si **EL CLIENTE** desea volver a obtener el servicio deberá tramitar una nueva solicitud.

20. El incumplimiento en el pago oportuno de las facturas por parte de **EL CLIENTE** dará lugar al cobro de intereses moratorios de acuerdo con la tasa máxima permitida por la ley, al igual que de los costos por el cobro prejurídico de tales obligaciones.

21. ETB podrá exigir la suscripción de un título valor, a fin de garantizar el pago por los conceptos derivados del Servicio Internet Extremo de ETB.com de conformidad con las condiciones especiales de este servicio, incluyendo la cláusula de multa por terminación anticipada y los intereses que se causen por mora en el pago, de acuerdo con el plan escogido por **EL CLIENTE**.

22. EL CLIENTE se obliga previa solicitud y una vez concertada la cita correspondiente, a permitir el acceso del personal de **ETB** o el que ésta designe, al lugar en donde se encuentren ubicados los "Equipos ADSL" con el fin de proceder a la instalación, reactivación, mantenimiento o cualquier otra actividad que a juicio de **ETB** resulte necesaria para la prestación del Servicio Internet Extremo de ETB.

23. El Servicio Internet Extremo de ETB será prestado por **ETB** durante las veinticuatro (24) horas del día, los siete (7) días de la semana. Ello no obsta para que este servicio se interrumpa o se suspenda de acuerdo con lo establecido en las Condiciones Generales del Servicio de Internet de **ETB**.

24. ETB no responderá ni reconocerá descuentos por el mal funcionamiento del Servicio Internet Extremo de ETB, especialmente en los siguientes eventos: (i) sí **EL CLIENTE** no cumple con los requisitos mínimos necesarios en su equipo informático para este servicio; (ii) sí **EL CLIENTE** introduce algunos elementos de hardware o software a su equipo informático; (iii) sí los equipos ADSL instalados no fueron suministrados, instalados u homologados por **ETB**; (iv) sí el número de equipos informáticos conectados al servicio objeto de las presentes condiciones excede la recomendación dada por **ETB**; (v) **EL CLIENTE** previa cita concertada con **ETB**, manifiesta su imposibilidad de cumplir y pide el aplazamiento de la cita; (vi) en los casos en que trabajadores de **ETB** o quién esta designe deban realizar una visita al domicilio de **EL CLIENTE** y éste no permita el ingreso de éstos funcionarios para la ejecución de las actividades necesarias tendiente a superar el problema; ó (viii) cuando el servicio sea interrumpido o suspendido por razones de equipamiento, trabajos de ingeniería o cualquier trabajo de reparación o actividades similares necesaria a juicio de **ETB** para su correcto o mejor funcionamiento, de conformidad con lo estipulado en las Condiciones de Prestación del Servicio de Internet de **ETB**.

25. ETB se obliga a prestar a **EL CLIENTE** el servicio de soporte telefónico durante las veinticuatro (24) horas, los siete (7) días a la semana.

26. Las presentes condiciones no podrán ser cedidas por **EL CLIENTE**, salvo previa autorización expresa y escrita de **ETB**. Para tal propósito, **ETB** estudiará la posibilidad de autorizar dicha cesión teniendo en cuenta entre otros la viabilidad técnica de prestar el servicio, siempre que el cesionario

cumpla con las características exigidas por **ETB** para la prestación del Servicio Internet Extremo de ETB. Los gastos que se ocasionen en virtud de la cesión, serán asumidos por el cesionario.

27. EL CLIENTE entiende y acepta que le está prohibida la comercialización a terceras personas del servicio y que en consecuencia los beneficios que obtenga en virtud del mismo no son objeto de venta ó comercialización, y que de hacerlo, su conducta constituye causal de cancelación del servicio.

28. Sin perjuicio de las condiciones previstas para la prestación del Servicio Internet Extremo de ETB, **ETB** podrá terminar las presentes condiciones, entre otras por cualquiera de las siguientes causas: (i) por el incumplimiento total o parcial de cualquiera de las obligaciones asumidas por **EL CLIENTE** en relación con el servicio; (ii) por el suministro de información falsa o adulterada; (iii) por razones de fuerza mayor, caso fortuito, orden de autoridad competente o causales establecidas en la ley. La terminación de las presentes condiciones no dará lugar a favor de **EL CLIENTE** de pago, reconocimiento o indemnización alguna.

Al hacer click en "Enviar" declaro haber leído el contrato en su totalidad, y declaro que lo entiendo, lo acepto plenamente y me comprometo a cumplir todos sus términos. En caso contrario debo llamar a la línea de atención al cliente 170 para que se me cancele el servicio.

Anexo B
Empresa contratada IFX para el canal de Internet

EMPRESA CONTRATADA IFX PARA EL CANAL DE INTERNET

INFRAESTRUCTURA DE RED DE IFX

IFX Networks opera una de las redes privadas más extensas de América Latina. La empresa está comprometida a construir la red pan-regional más avanzada y completa, contando con 15 centros de operaciones de red, más de 60 puntos de presencia y más de 45.000 puertos de acceso remoto. La red de IFX cuenta con circuitos de fibra óptica complementados con conexiones nacionales que aumentan la capilaridad total de la red.

IFX Networks ha implementado la tecnología más moderna y establecido acuerdos de peering- en el NAP de las Americas (punto de acceso a red para Latinoamérica), con capacidad de múltiples circuitos OC-3. Adicionalmente, la empresa ha firmado acuerdos de peering a nivel local y cuenta con proveedores alternativos para el enrutamiento en la región con el objetivo de mejorar la calidad de transmisión y capacidad de recuperación. El compromiso de excelencia de IFX Networks está respaldado por circuitos físicos y virtuales que cruzan de país a país dentro de la red, permitiéndonos ofrecer una gran variedad de beneficios, tales como la disponibilidad de trayectos varios para evitar puntos individuales de falla, óptimo enrutamiento y flujo de tráfico, rápida conectividad a Internet, fácil manejo y calidad de servicio superior, además de una amplia variedad de servicios y productos basados en ATM (modo de transferencia asincrónico) e IP (protocolo de Internet).

IFX Networks aprovecha la capilaridad e infraestructura de su red para extender su alcance hasta el cliente gracias a las tecnologías alámbrica e inalámbrica, que le permiten mantener el más alto nivel de servicio. Adicionalmente, los clientes de IFX Networks aprovechan la disponibilidad y tecnología de avanzada de centros de datos operados por la empresa a lo largo de la región -- instalaciones completamente acondicionadas para sus aplicaciones de misión crítica.

IFX Networks mejora constantemente su tecnología y expande su red de manera tal de continuar ofreciendo soluciones llave en mano de conectividad y servicio personalizado a todo cliente operando en la región.

BACKBONE

***Conectividad Internacional**:* Múltiples circuitos STM-1 (155 Mbps cada uno) desde Miami hasta Argentina, Brasil, Chile, Colombia y Venezuela.

**Vea tabla de implementación en la siguiente página.*

***Conectividad Nacional**:* Contratos locales con al menos dos proveedores de conectividad por fibra y un proveedor de comunicaciones satelital, para ofrecer redundancia y prevenir interrupciones en el servicio. El Backbone nacional por fibra en Argentina, Chile, Colombia y México permite ofrecer alta calidad de servicio (QoS) y conexión dedicada en numerosas ciudades.

ULTIMA MILLA

Conectividad de circuito cerrado inalámbrico en once países con expansión regional progresiva.
Más de 45,000 Puertos de Acceso Remoto (RAS) instalados en la región y capacidad en expansión para asegurar la calidad de servicio.

Líneas tradicionales: implementando estrategia de acceso a DSL (Chile).

INSTALACIONES

Más de 60 POPs propiedad de la empresa en 13 países, más los Estados Unidos.
Presencia en el Punto de Acceso de Red (NAP) de las Américas ubicado en Miami. Los circuitos de fibra de IFX Networks terminan en el NAP, desde donde se interconectan al Backbone de Internet a través de múltiples OC-3 de proveedores varios.

IFX Networks está expandiendo rápidamente su capacidad de Centro de Datos y Co-location:
-Centro de Datos ("Data Center") de Miami con múltiples conexiones OC-3 de proveedores varios al Backbone de Internet y acuerdos paritarios.
-Data Center redundante de los Estados Unidos, funcionando actualmente y que permite la conmutación automática y el balance de capacidad de la red internacional de IFX Networks. (*En operación)

DESPLIEGUE DE RED

Mejoramiento de la infraestructura central de la red con productos Nortel Passport y Juniper a nivel de portadores.
Uso de los productos Cisco y Juniper para dirigir el tráfico de manera más eficiente a lo largo de la red (nacional e internacional).
Despliegue de sistemas Crosskeys Dyband para garantizar calidad de servicio.
Aplicación de los sistemas de caché Inktomi para mejorar el rendimiento de la entrega de contenidos --IFX Networks está desarrollando una red de intercambio de contenidos en la región y los Estados Unidos.
Despliegue de sistemas IBM Tivoli Suite, HP Openview Suite y Micromuse Netcool para monitorear, administrar y mejorar el rendimiento y operación de la red en la región y los Estados Unidos.
Tabla de implementación de la red de fibra óptica de IFX Networks:

Fecha Estimada	País	Ciudad	**Capacidad (Mbps)**	**Total**
Activo	Argentina	Buenos Aires	155	
Activo	Brasil	São Paulo	155	
Activo	Chile	Santiago de Chile	155	
Activo	Venezuela	Caracas	45	
Activo	Brasil	Río de Janeiro	155	
Activo	Colombia	Santa Fe de Bogotá	155	
Activo	Venezuela	Caracas	155	

IFX Networks utiliza la red a un máximo de capacidad del 85%. Una vez que el ancho de banda alcanza el 70% de utilización, IFX Networks planifica mejoramiento(s), activado(s) antes de llegar al 85% del uso de capacidad de la red.

Adicionalmente a su Centro de Operaciones de Red (NOC) en Miami, IFX Networks ha establecido Centros de Operaciones de Red en otros países, de manera tal de monitorear el rendimiento de los equipos de la red IFX Networks. Al implementar herramientas tales como IBM Tivoli Suite, HP

Openview Suite y Nortel Preside Suite. IFX Networks puede identificar y corregir problemas de la red de forma remota o local eficientemente.

El Centro de Operaciones de Red proporciona asistencia técnica las veinticuatro horas del día, los siete días de la semana. El NOC es responsable de recibir aviso de problemas(s) en la red y ofrece asistencia, coordinando servicio y prestando soluciones.

Oferta

ENLACES DEDICADOS A INTERNET

***Incluye el alquiler de los equipos de conexión.**

***Instalación 0.**

***Oferta económica para servicio Dedicated I.P.**

***Call Center 7*24 Horas.**