UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SERVICIO DEDICADO DE TRANSMISIÓN DE DATOS ENTRE REDES DE AREA LOCAL

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO ELECTRÓNICO

PRESENTADO POR:

IGOR FRANZ VILLANES VERGARA

PROMOCIÓN 2000 – II

LIMA – PERU
2003

A mis Padres: Lucio y Francisca
por todo lo que me han brindado.

A mis Hermanos: Iván y Liz
por su apoyo constante.

SERVICIO DEDICADO DE TRANSMISIÓN DE DATOS ENTRE REDES DE ÁREA LOCAL

SUMARIO

En el presente informe se hace una breve introducción a los diferentes conceptos de Redes de Computadoras. Se revisa el protocolo Frame Relay y la utilización de sus Circuitos Virtuales Permanentes para implementar Redes Privadas Virtuales, como un servicio dedicado de transmisión de datos entre redes LAN separadas geográficamente. Asimismo se estudia el concepto de las Redes Privadas Virtuales IP (IP VPN) bajo el protocolo MPLS, detallando el funcionamiento de esta última tecnología. Por último se analiza el tema de Seguridad de la Información, indicando las políticas de seguridad a tener en cuenta para el resguardo de los datos y se detalla el funcionamiento de algunos equipos de seguridad como son los Firewalls.

ÍNDICE

PRÓLOGO 1

CAPÍTULO I 3

INTRODUCCIÓN A LAS REDES DE COMPUTADORAS 3

1.1 Redes de Computadoras. 3

1.2 Historia de las redes. 3

1.3 Redes de acceso. 5

1.4 Tipos de Redes. 8

1.4.1 Redes de Difusión (Broadcast). 8

1.4.2 Redes Punto a Punto (Point to Point). 8

1.4.3 LAN (Local Area Networks). 8

1.4.4 WAN (Wide Area Networks). 9

1.5 Fundamentos de Interconectividad de Redes. 10

1.6 Modelo de referencia OSI. 11

1.6.1 Especificaciones de las capas OSI. 13

1.7 Servicios de red orientados y no orientados a la conexión. 19

1.7.1 Servicios orientados a la conexión. 20

1.7.2 Servicios no orientados a la conexión. 20

CAPÍTULO II 21

PROTOCOLO FRAME RELAY 21

2.1 Introducción. 21

2.2 Frame Relay. 23

2.2.1 Principios básicos. 26

2.2.2 Terminología Frame Relay. 27

2.2.3 Funcionamiento del Protocolo. 28

2.2.4 Ventajas y beneficios. 33

CAPÍTULO III 35

MULTIPROTOCOL LABEL SWITCHING (MPLS) 35

3.1 Introducción. 35

3.2 Tecnología MPLS. 36

3.2.1 Terminología MPLS. 37

3.2.2 Etiquetas. 38

3.2.3 LSP (Label Switched Path). 42

3.3 Ingeniería de tráfico. 44

3.3.1 Método TE-RSVP. 45

3.3.2 Método CR-LDP. 47

3.3.3 Comparación de ambos métodos. 48

CAPÍTULO IV 50

REDES PRIVADAS VIRTUALES IP (IP VPN) 50

4.1 Introducción. 50

4.2 Redes Privadas. 52

4.3 Red Privada Virtual (VPN, *Virtual Private Network*). 53

4.4 Ventajas de las VPN. 54

4.5 Proceso de Túnel (*Tunneling*). 55

4.6 Tipos de VPN. 57

4.7 Tecnologías para implementar una VPN. 58

4.7.1 IPSEC (*Internet Protocol Secure*). 58

4.7.2 PPTP (*Point to Point Tunneling Protocol*). 59

4.7.3 L2TP (*Layer-2 Tunneling Protocol*). 60

4.8 Diagramas de conexión. 61

4.8.1 De Cliente a Servidor (*Client to Server*). 61

4.8.2 De Cliente a Red Interna (*Client to LAN*). 62

4.8.3 De Red Interna a Red Interna (*LAN to LAN*). 62

4.9 Requerimientos para implementar una VPN. 63

CAPÍTULO V 64

ASPECTOS DE SEGURIDAD INFORMÁTICA 64

5.1 Seguridad Informática. 64

5.2 Ataques contra Sistemas Informáticos. 65

5.3 Importancia de políticas y procedimientos de seguridad. 67

5.4 Importancia de la protección física y ambiental. 68

5.5 Dispositivos y equipos de seguridad. 69

5.5.1 Router Apantallado (Screening router). 69

5.5.2 Firewalls. 71

CONCLUSIONES Y RECOMENDACIONES 80

BIBLIOGRAFÍA 82

ÍNDICE DE FIGURAS

Figura 1.1 Comunicación entre capas. 10

Figura 1.2 Modelo de referencia OSI. 12

Figura 2.1 Ejemplo de red X.25. 23

Figura 2.2 Ejemplos de redes Frame Relay. 25

Figura 2.3 Formato de trama Frame Relay. 29

Figura 2.4 Protocolos encapsulados dentro de Frame Relay. 30

Figura 2.5 Especificaciones del campo Dirección. 30

Figura 2.6 Nodo Frame Relay. 31

Figura 2.7 Parámetros Frame Relay. 32

Figura 4.1 Diagrama Lógico de una VPN. 53

Figura 4.2 Túnel VPN. 56

Figura 4.3 Client to Server 62

Figuira 4.4 Client to LAN. 62

Figura 5.1 Screening router. 69

Figura 5.2 Packet Filter. 76

ÍNDICE DE TABLAS

Tabla 1.1 Tecnologías usadas para redes. 9

Tabla 1.2 Clases de protocolo de Transporte. 17

PRÓLOGO

A medida que las LANs se hacen cada vez más comunes, existe una creciente necesidad de interconectarlas. La demanda del mercado en cuanto a conexión de redes de área local separadas geográficamente no ha pasado desapercibida. Soluciones como las Redes Privadas Virtuales bajo Frame Relay y MPLS están siendo desplegadas rápidamente por un número creciente de proveedores.

En el primer capítulo se hace una breve introducción a las redes de computadoras, los conceptos básicos sobre ellas, su clasificación, servicios que pueden implementarse y los fundamentos de interconexión entre componentes de red. Se estudia también el modelo de referencia OSI, detallándose la funcionalidad de cada capa.

En el segundo capítulo se presenta el protocolo Frame Relay como aquella norma capaz de interconectar redes LAN dispersas en diferentes geografías, su funcionamiento y el formato de sus tramas son explicados y analizados. Mediante este protocolo es posible implementar Redes Privadas Virtuales utilizando sus Circuitos Virtuales Permanentes.

En el tercer capítulo se estudia la tecnología MPLS, su terminología y los componentes de hardware que se utilizan para implementar esta solución. Asimismo se detalla la ingeniería de tráfico empleada en MPLS, para evitar que la red se sature, evitando cuellos de botella y mejorando la red global.

En el cuarto capítulo se trata el tema de Redes Privadas Virtuales IP (IP VPN), sus ventajas de implementación, las tecnologías más usadas para poner en marcha una red de éste tipo y los diferentes diagramas de conexión con el cliente VPN.

En el quinto y último capítulo se resaltan los aspectos de seguridad de la información , tanto para el resguardo de los datos como para la protección del hardware principal. Se hace mención a uno de los dispositivos más populares de seguridad como es el caso del Firewall, describiendo sus funciones. ventajas y limitaciones.

CAPÍTULO I

INTRODUCCIÓN A LAS REDES DE COMPUTADORAS

1.1 Redes de Computadoras.

Una Red de Computadoras es un conjunto de ordenadores autónomos interconectados, los cuales pueden comunicarse e intercambiar información entre ellos a través de un medio de transmisión.

El principal objetivo de estas redes es la de compartir recursos tales como hardware, software, datos, etc. los cuales pueden encontrarse localmente o dispersos geográficamente. De manera que sea confiable, disponiendo de alternativas de almacenamiento; económica, obteniendo una buena relación costo / beneficio; y escalable.

1.2 Historia de las redes.

En los inicios de las computadoras, los recursos eran de un costo muy elevado, el poder de cómputo era uno de los más valiosos y más costosos. En los centros de investigación se hacía necesario que todos los investigadores tuvieran acceso a este tipo de recursos y que estos recursos fueran distribuidos en forma tal que no se tuviese un desperdicio de tiempo

de procesamiento. Es así como surge la necesidad de compartir recursos de alto costo entre varias personas y se da inicio al desarrollo de las redes.

Las primeras redes de computadoras que se crearon eran del tipo centralizado, es decir, un procesador central tenía el poder de cómputo y ejecutaba las tareas que eran enviadas por los terminales. Estas redes exigían que la conexión se realizara punto a punto.

Al desarrollarse la tecnología se permitió tener redes que comunicaban computadoras desde sitios distantes, este avance obligó a crear protocolos de comunicación entre las computadoras. Estos protocolos eran propietarios de los fabricantes de los ordenadores. Aquí es donde comienza la necesidad de crear protocolos estándares para comunicar máquinas y redes de diferentes fabricantes y de diferentes tipos.

En 1973, la Agencia de Investigaciones Avanzadas de la Defensa de los Estados Unidos (DARPA) inició un programa para investigar las técnicas y tecnologías para la interconexión de redes de diversos tipos. El objetivo era desarrollar protocolos de comunicación los cuales puedan permitir a redes de computadoras comunicarse en forma transparente a través de múltiples redes. Este proyecto fue llamado *Internetting project*, y el sistema de redes que emergió de estas investigaciones fue conocido como Internet. El sistema de protocolos desarrollados en el transcurso de esta investigación, dio forma a lo que después se conocería como la suite del protocolo TCP/IP.

En 1986, la *National Science Foundation* (NSF) de Estados Unidos inició el desarrollo de la NSFNET, la cual provee un servicio de comunicación muy importante para la Internet.

La NASA y el Departamento de Energía de los Estados Unidos contribuyeron con otra parte del canal principal de Internet con la NSFNET y ESNET respectivamente. En Europa también hay una gran parte del canal principal de Internet, esta red es conocida como NORDUNET.

Actualmente Internet enlaza computadoras de Universidades, Oficinas Gubernamentales, Instituciones Públicas y Privadas, Centros de Investigación, etc. Durante el curso de la evolución de Internet, particularmente después de 1989, el sistema de Internet comenzó a integrar el soporte para otras suites de protocolos en su estructura de red básica. Se puso énfasis en una red multi-protocolo y en particular en la integración de los protocolos de Interconexión de Sistemas Abiertos (OSI, *Open System Interconnection*) dentro de la arquitectura.

En la década de los 80 se crearon cerca de 100 aplicaciones públicas y comerciales de protocolos de la suite TCP/IP. Durante los comienzos de 1990 también se crearon aplicaciones del protocolo OSI.

1.3 Redes de acceso.

Entre las más conocidas tenemos:

ARPAnet (*Advanced Research Projects Agency Network*), Red experimental que vincula universidades y otras instituciones dedicadas a la investigación sobre redes de computadoras. Es la porción no clasificada de la Red de Defensa de los Estados Unidos(DDN). La familia de protocolos TCP/IP fue desarrollada por ARPAnet.

BITNET (*Because Its Time NETwork*), Red académica cooperativa fundada en 1981, que provee correo electrónico y transferencia de archivos a más de 2,700 nodos distribuidos por todo el mundo. La mayoría de ellos se encuentran en instituciones de educación superior y centros de investigación. BITNET provee pasarelas a las redes de otros países, en particular a Europa, Canadá, Asia y Oceanía. Actualmente, BITNET está siendo fusionada con CSNET.

CSNET (*Computer Science Research Network*).

CUNET (*Carribean University NETwork*), Red Universitaria del Caribe, la cual es dominio de INTERNET. Actualmente, está integrada por los miembros de PRUnet.

INTERNET Colección de redes, que incluye ARPAnet, NSFNET, redes regionales (NYSERNET), redes locales de numerosas universidades e instituciones de investigación (incluyendo CUNET y por tanto, UPREnet), y varias redes militares. El término INTERNET aplica al conglomerado de dichas redes. La porción de ellas, liderada por el departamento de Defensa, recibe el nombre de DDN (*Defense Data Network*). Los usuarios de ésta pueden enviarse mensajes unos a otros, excepto cuando hay alguna restricción impuesta por razones de seguridad. Cuando está en letras minúsculas (**internet),** se refiere a una red genérica que resulta de interconectar diversas redes.

NSFNET (*National Science Foundetion NETwork*), Red de la Fundación Nacional de Ciencias. Consiste en una red nacional de computadoras que interconectan cientos de campos universitarios y centros de investigación del

gobierno. Por medio de ésta red, los investigadores pueden acceder a las más modernas facilidades de computación de los Estados Unidos, incluyendo 6 de los supercentros de cómputo financiados por NSF. Entre las redes de investigación conectadas a NSFNET está el internet científico de la NASA.

NYSERNET, Red Educacional y de Investigación del estado de Nueva York.

PRUnet (*Puerto Rico Universities Network*), Red de las Universidades de Puerto Rico. Entre las universidades con las que se pueden interconectar están: Universidad de Puerto Rico, Observatorio de Arecibo (Cornell University), Federal Forest Service, Universidad del Sagrado Corazón y la Universidad Interamericana.

UPREnet (*University of Puerto Rico Educational Network*), Red de comunicaciones de la Universidad de Puerto Rico. Esta interconectada a todas las unidades y dependencias de la Universidad de Puerto Rico entre sí, y con otras universidades dentro y fuera de la Isla. UPREnet también está interconectada con otras redes como TELNET, BITNET e INTERNET.

SURANET, Red de la Asociación de Universidades del Sudeste de los Estados Unidos. Escogido como punto de enlace de UPREnet con INTERNET.

TELENET, Permite acceso a una gran cantidad de servicios tales como: establecer sesiones interactivas, intercambio de archivos y correo electrónico. Además, permite la comunicación a otras redes.

1.4 Tipos de Redes.

Según el tipo de transmisión utilizada, las redes de datos pueden enmarcase en dos tipos:

1.4.1 Redes de Difusión (Broadcast).

Donde se comparte el mismo medio de transmisión entre todos los integrantes de la red. Cada mensaje (típicamente llamado "paquete") emitido por una máquina es recibido por todas las otras máquinas de la misma red. Cada paquete dispone de la información de "Origen" y "Destino" y de esta manera se discrimina quien debe procesar cada mensaje. Por ejemplo, Ethernet es una red de difusión.

1.4.2 Redes Punto a Punto (Point to Point).

Donde existen muchas conexiones entre pares individuales de máquinas. Para enviar mensajes hasta máquinas distantes puede ser necesario pasar por varias máquinas intermedias. Por ejemplo, las conexiones por MODEM son redes punto a punto.

En forma independiente a la tecnología utilizada, las redes de datos pueden ser clasificadas en dos categorías, según el alcance o tamaño de las mismas:

1.4.3 LAN (Local Area Networks).

Las Redes de Área Local (LAN) son de alcance limitado. Generalmente son redes privadas que están instaladas dentro de un mismo edificio,

oficina o campus. Su objetivo principal típicamente es compartir recursos (impresoras, discos, etc.). Estas redes pueden tener velocidades de transmisión de hasta 1000 Mb/s y pueden tener topologías del tipo bus, estrella o anillo.

1.4.4 WAN (Wide Area Networks).

Las Redes de Área Amplia (WAN) se extienden en una amplia zona geográfica, que eventualmente puede ser dividida en subredes interconectadas con equipos de conversión de interfases y/o protocolos. Estos equipos se conectan con diferentes medios de transmisión. Una de las funciones típicas de las redes WAN es la interconexión de dos o varias redes LAN. La topología de las redes WAN puede ser del tipo estrella, anillo, árbol o malla.

En la Tabla 1.1 se muestra que las redes según su alcance geográfico: LAN y WAN pueden utilizar ambos tipos de transmisión: Difusión (Broadcast) y Punto a Punto (Point to Point).

	LAN	WAN
Broadcast	La mayoría de las LANs (Ethernet, FDDI, Token Ring, etc.), Fibre Channel	Redes de transmisión vía satélite
Punto a punto	HIPPI, Fibre Channel, LANs Conmutadas	La mayoría de las WANs (todas las basadas en enlaces telefónicos, X.25, Frame Relay, RDSI, ATM, etc.)

Tabla 1.1 Tecnologías usadas para redes.

1.5 Fundamentos de Interconectividad de Redes.

Los tipos de redes vistas anteriormente requieren de programas dedicados al control, mantenimiento y diseño; así como para llevar acabo sus conexiones.

Para reducir la complejidad del diseño, la mayoría de las redes están organizadas en "niveles" o "capas". El propósito de cada capa es ofrecerle servicios a su capa inmediatamente superior. Cada capa se comunica con su similar en otra máquina, mediante reglas bien establecidas, llamadas "protocolos". Esta comunicación se realiza a través de las capas inferiores, como se observa en la Figura 1.1.

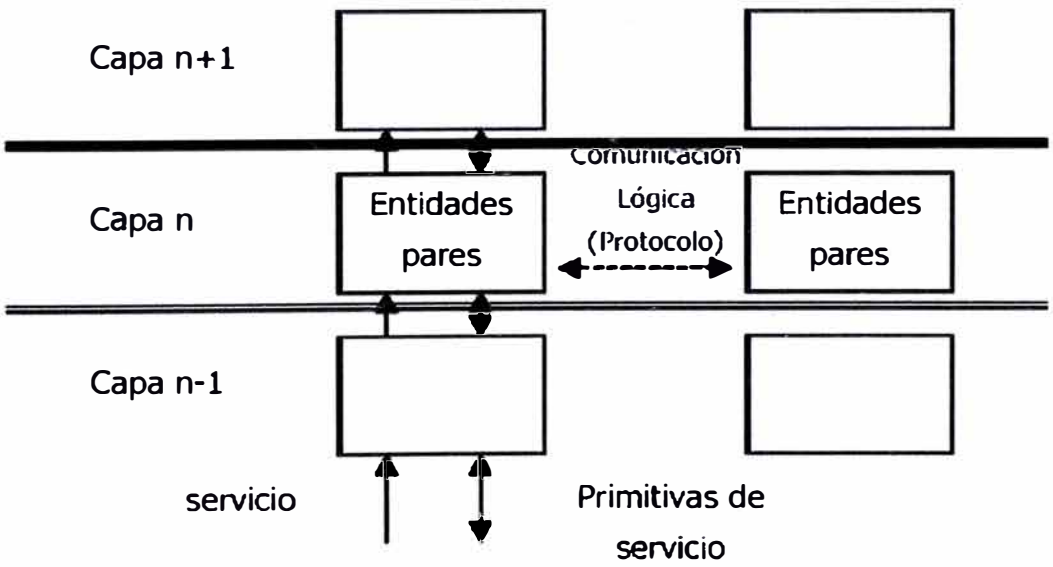


Figura 1.1 Comunicación entre capas.

Los protocolos aseguran que cada una de las partes de la comunicación entienda a la otra sin ambigüedad. En el contexto de la tecnología de redes de datos, un protocolo es un conjunto formal de reglas y convenciones que gobiernan el modo en que las computadoras intercambian información por un medio de transmisión.

Cada capa tiene sus propias interfases, hacia las capas superiores e inferiores. Estas deben ser bien definidas para poder intercambiar información de un nivel a otro. Un conjunto de capas y protocolos se denomina "arquitectura de red". Actualmente existen muchas arquitecturas de red, entre las que figuran OSI, TCP/IP, SNA, etc.

La mayoría de los protocolos y funciones de las capas de una arquitectura están desarrolladas en software (programas) pero últimamente se están desarrollando muchos protocolos, interfases y funciones, en hardware (equipos) y/o firmware (equipos programables).

1.6 Modelo de referencia OSI.

La Organización Internacional para Estandarización (ISO) desarrolló un modelo de referencia, de siete capas, para estandarizar los protocolos de red. Este modelo es conocido como el modelo de referencia para Interconexión de Sistemas Abiertos, (OSI, *Open System Interconection*). Tal como se muestra en la Figura 1.2.

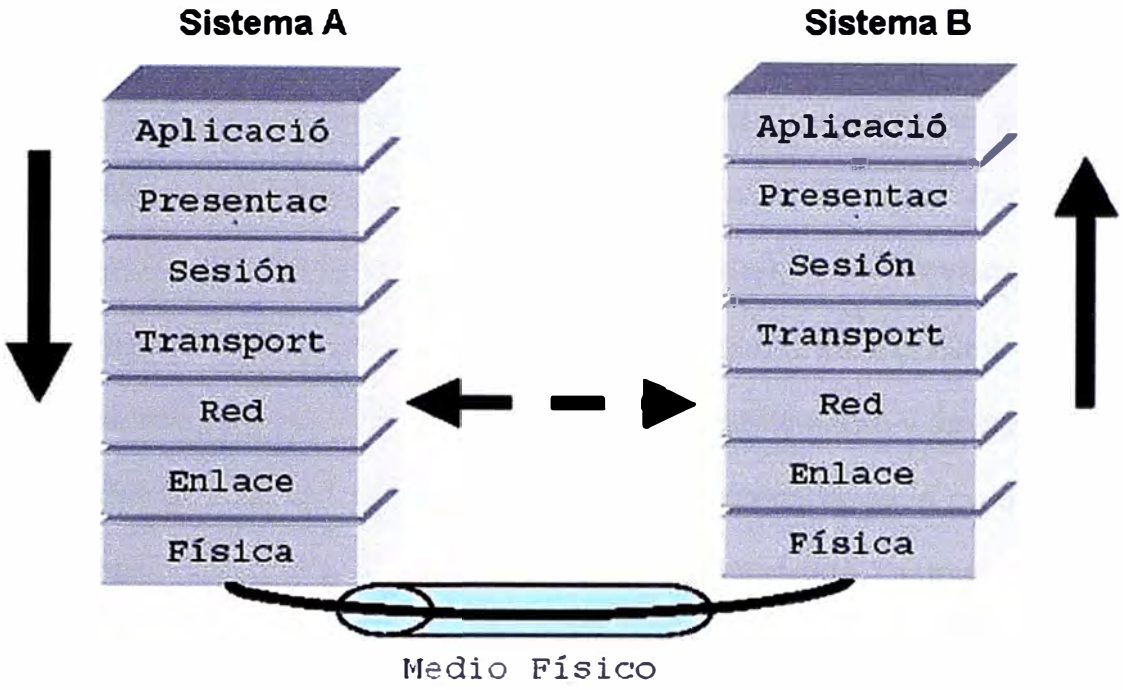


Figura 1.2 Modelo de referencia OSI.

Por lo general una capa determinada del modelo OSI se comunica con otras tres capas: la capa que se encuentra directamente sobre ella, la capa que se encuentra directamente debajo de ella y su capa equivalente en otro sistema de computadoras en red. Por ejemplo, la capa de red (Capa 3) de un sistema A se comunica con la capa de enlace de datos (Capa 2) y con la capa de transporte (Capa 4) de su mismo sistema y , además, con la capa de red de un sistema B. Esto da flexibilidad al momento de cambiar o agregar nuevas opciones a las especificaciones.

1.6.1 Especificaciones de las capas OSI.

a) Capa Física.

Esta capa describe las especificaciones mecánicas y eléctricas para la estructura del cableado. Define como serán convertidos los bits en corriente eléctrica, pulsos luminosos o cualquier otra forma física. Determina el método por el cual las ráfagas de bits son enviadas a través del medio de transmisión. Esta capa proporciona los servicios de enlace que están asociados con la adquisición, mantenimiento y desconexión de circuitos físicos que conforman la ruta de conexión de la comunicación. La capa física esta encargada de la sincronización de los bits y de la identificación de un elemento como un uno (1) o un cero (0). La unidad de datos de este protocolo es el Bit.

Protocolos típicos en la capa física incluyen la familia RS-232, la familia RS-449, las interfaces CCITT X.25 y X.21, otra serie de recomendaciones de la CCITT (V y X), y los aspectos físicos de los protocolos de acceso al medio de la IEEE 802.X para redes LAN.

En resumen, las especificaciones de la capa física definen características como niveles de voltaje, temporización de cambios de voltaje, velocidades de transferencia de información, distancias máximas de transmisión y conectores físicos. Las implementaciones de esta capa se pueden categorizar como especificaciones LAN o WAN

b) Capa de Enlace de Datos.

Es responsable de hacer que el enlace físico sea confiable. Esta encargada de iniciar y terminar los enlaces, además de detectar y controlar los errores.

El trabajo del comité IEEE 802.3 ha subdividido esta capa en dos subcapas. La capa que sirve como interfaz con la capa física es llamada capa de Control de Acceso al Medio (MAC) y la capa que sirve de interfaz con la capa de red es llamada capa de Control Lógico de Enlace (LLC). La capa LLC es responsable de ensamblar y particionar los frames, agregando direcciones origen y destino, facilidades para el control y detección de errores en el receptor. Los Puentes (Bridges) funcionan en esta capa. LLC es la capa responsable de controlar el intercambio de datos entre usuarios que se están comunicando a través de la capa de Control de Acceso al Medio.

Con excepción de la capa física, los servicios y protocolos proporcionados por la capa de enlace deben de ser familiares a aquellos que están en la industria de la comunicación de datos.

Los servicios de la capa de enlace están relacionados con el intercambio confiable de datos a través de un enlace punto a punto o multipunto que ha sido establecido en la capa física. Los protocolos de la capa de enlace de datos manejan el establecimiento, control y terminación de la conexión lógica. Controla el flujo de datos del usuario, supervisa la recuperación de errores y condiciones anormales, mantiene la sincronización de los bloques o frames y caracteres.

c) Capa de Red.

Esta capa provee aquellos servicios asociados con el traslado de los datos de los usuarios a través de una red constituida por enlaces encadenados, teniendo muchas rutas disponibles entre los puntos. Estos servicios incluyen ruteo, switcheo, secuenciación de datos, control de flujo y recuperación de errores. Funciones como control de flujo y recuperación de errores aparecen duplicados en el nivel de enlace, estos están relacionados con conexiones a través de múltiples enlaces.

Esta capa es la responsable de establecer y monitorear las conexiones entre redes de área local. Esta capa es independiente de la capa física, es decir, esta capa puede estar sobre cualquier protocolo de capa 2.

En esta capa se realiza el control y selección de las rutas lógicas y conexiones entre usuarios de puntos finales en una red. Un ejemplo seria un circuito virtual en una red publica de datos.

Los capa de paquetes del CCITT X.25 es el mejor protocolo de capa de red para redes de switcheo de paquetes. X.21 es usado para redes de switcheo de circuitos. El Departamento de Defensa de los Estados Unidos ha desarrollado un protocolo de internet conocido como IP. Otros ejemplos de protocolos de red incluyen el CCITT Q.931 y el protocolo ISO 8473 no orientado a conexión, después veremos la diferencia entre un servicio orientado a la conexión y uno no orientado a la conexión.

d) Capa de Transporte.

Es la capa más alta asociada con el movimiento de datos a través de la red. Esta capa provee un mecanismo universal transparente para ser usado por las capas mas altas que representa a los usuarios de los servicios de comunicación. De la capa de Transporte se espera la optimización del uso de los recursos disponibles.

Los protocolos de transporte son responsables de la integridad del intercambio de datos y deben de ser el puente conector entre los servicios proporcionados por las capas inferiores y los requeridos por las capas superiores. Se han desarrollado numerosas clases de protocolos de transporte desde algunas muy simples hasta otras muy complejas. Las capas de transporte simples pueden ser utilizadas cuando la red provee un servicio confiable y de calidad. Un protocolo de transporte complejo es usado cuando los servicios de la capa inferior es incapaz de proporcionar el nivel de servicio requerido. La complejidad es necesaria debido a que esta capa duplica los mecanismos de recuperación que deben haber sido proporcionados por las capas inferiores.

La ISO ha promulgado el estándar internacional 8073 como un protocolo de transporte. Este estándar define 5 clases de protocolos, desde el más simple (clase 0) hasta el más complejo (clase 4). Ver Tabla 1.2.

Un ejemplo de protocolo de transporte es TCP, desarrollado por el Departamento de Defensa de los Estados Unidos y que forma parte de la suite de protocolos de TCP/IP .

Clase	Nombre	Tipo de Red	Caracteristicas
0	Clase Simple	Tasa aceptable de errores residuales (no detectables). Linea Dedicada confiable o red de conmutación de paquetes confiable.	No multiplexa. No se Recupera de Errores reportados por la capa de red, no detecta ni se recupera de errores no reportados por la capa de red.
1	Clase de recuperación básica de errores	Tasa aceptable de errores detectados. Tasa aceptable de errores residuales(No detectados), tasa no aceptable de errores detectados. Red de conmutación de paquetes no confiable.	No multiplexa, se recupera de errores reportados por la capa de red, no detecta ni se recupera de errores no reportados por la capa de red.
2	Clase de Multiplexaje	Tasa aceptable de errores residuales (no detectables) Linea Dedicada confiable o red de conmutación de paquetes confiable.	Multiplexa, no se recupera de errores reportados por la capa de red, no detecta ni se recupera de errores no reportados por la capa de red.
3	Clase de Multiplexaje y recuperacion de errores	Tasa aceptable de errores detectados . Tasa aceptable de errores residuales(No detectados), tasa no aceptable de errores detectados. Red de conmutacion de paquetes no confiable.	Multiplexa, se recupera de errores reportados por la capa de red, no detecta ni se recupera de errores no reportados por la capa de red.
4	Clase de detección y recuperación de errores.	Tasas no aceptables de errores detectados y no detectados. Red no orientada a conección.	Multiplexa, divide la conexión de transporte entre muchas conexiones de red, permite el uso de redes no orientadas a conexión, recuperación de errores reportados por la capa de red, detección y correción de errores no reportados por la capa de red.

Tabla 1.2 Clases de protocolos de Transporte.

e) Capa de Sesión.

Una sesión enlaza dos procesos de aplicación en una relación cooperativa durante cierto tiempo. La capa de sesión proporciona un servicio administrativo que maneja el establecimiento y liberación de una conexión entre dos entidades de presentación. Las sesiones son establecidas cuando un proceso de aplicación pide acceso a otro proceso de aplicación.

Cuando una sesión es establecida, los servicios de control dialogan y supervisan el intercambio de datos actual. El propósito de esta capa es proporcionar el control sobre la comunicación entre las aplicaciones. Esta asume que la conexión física es confiable y es controlada por las capas inferiores. Una simple sesión puede mantener varias conexiones de transporte o muchas sesiones consecutivas pueden ser mantenidas en

una conexión de transporte única. Actualmente los protocolos de sesión incluyen el ISO 8327, el CCITT X.25, ECMA 75 y el CCITT T.62 el cual esta orientado a servicios de Teletex.

f) Capa de Presentación.

Esta capa permite a una aplicación interpretar en forma adecuada la información transferida. Esta capa esta involucrada con la traducción, transformación, formato y sintaxis de la información. Esas funciones son requeridas para adaptar las características de manejo de la información de un proceso de aplicación a otro. Algunos ejemplos de las acciones que se realizan en esta capa, serían, la traducción de códigos, estructuración de los datos para el despliegue en pantalla, control de formato y protocolos de terminales virtuales.

Esta capa es la responsable de presentar los datos a aplicaciones diferentes en un formato que ambos puedan reconocer. También controla características tales como cifrado y compresión de datos. Un ejemplo de la función de esta capa es la de convertir datos ASCII, usados por la mayoría de las PCs y el sistema de códigos EBCDIC usado en las mainframes IBM.

La ISO realizo una selección internacional de estándares de presentación, conocido como DIS 8823. La representación sintáctica de datos ha sido definida en DIS 8824 y 8825. La CCITT ha descrito el protocolo de presentación para manejo de mensajes en X.409 y para Telex en X.61.

g) Capa de Aplicación.

La capa de aplicación incluye una parte de la administración de la red y tareas de aplicación general tales como transferencia de archivos. Aunque esta es la capa superior de la arquitectura del modelo OSI, la capa de aplicación no es la casa de las aplicaciones. Esta es simplemente la ventana a través de la cual las aplicaciones obtienen el acceso a los servicios proporcionados por la arquitectura de comunicaciones.

Esta capa proporciona servicios de comunicación que son más directamente comprensibles al usuario. Estas incluyen identificación de procesos cooperativos, autentificación del comunicante, verificación de autoridad, determinación de los recursos disponibles y acuerdo de sintaxis.

La capa de aplicación puede ser visualizada como una conexión de elementos de usuario que son específicos al proceso de aplicación; un elemento de aplicación específica tiene funciones como transferencia de archivos, intercambio de datos de negocio, u operaciones de terminales virtuales y un elemento común constituido de funciones generales.

1.7 Servicios de red orientados y no orientados a la conexión.

Las capas de una arquitectura pueden ofrecer dos tipos de servicios: orientados a la conexión y no orientados a la conexión.

1.7.1 Servicios orientados a la conexión.

Son muy similares a los servicios de telefonía, donde se establece una conexión marcando un número determinado. Una vez establecida la conexión, se puede intercambiar información en forma segura y ordenada. Luego de terminado el intercambio de información, puede liberarse la conexión.

1.7.2 Servicios no orientados a la conexión.

Toman su modelo del servicio de correos, donde el mensaje es enviado sin establecer previamente una conexión entre origen y destino. Cada mensaje debe contener la dirección completa de su destino. Dos mensajes enviados al mismo destino (dos cartas, en el ejemplo), pueden viajar por caminos completamente diferentes antes de llegar al destino, e incluso puede suceder que el mensaje enviado en segundo lugar llegue a destino antes que el enviado en primer lugar.

CAPÍTULO II

PROTOCOLO FRAME RELAY

2.1 Introducción.

La aparición de Frame Relay se debe a los trabajos realizados por un consorcio de compañías entre las que se encontraban Cisco, Northern Telecom, Digital Equipment, Stratacom y Convex Computer, que se involucraron activamente en la generación de la norma, en el año 1990. Fue en este contexto donde se escogió un subconjunto de LAPD como protocolo generador y núcleo de Frame Relay .

El primer servicio público basado en Frame Relay apareció en Estados Unidos en 1992 bajo los auspicios de AT&T y BT North America . Los primeros nodos se situaron en las ciudades más importantes de forma que sus habitantes podían acceder al servicio de forma directa; para los usuarios situados en el resto de ciudades el acceso al servicio de los nodos se proporcionaba mediante unos puntos de presencia (lugares físicos donde un portador de larga distancia sitúa el interface con un LEC o Local Exchange Carrier) facilitados por las compañías telefónicas locales .

Desde su aparición, Frame Relay atrajo la atención de los administradores de sistemas de comunicaciones de datos de todo el mundo. Los diseñadores de redes y los administradores de redes de área local ven en Frame Relay una solución a sus problemas de interconexión de redes locales.

Al continuar el crecimiento de las instalaciones LAN, su interconexión se está convirtiendo rápidamente en la mayor fuente de tráfico de datos en redes de área amplia (WANs).

Las interconexiones entre redes de área local son voraces en cuanto a ancho de banda, ya que se les exige disponer de enormes anchos de banda durante las transferencias de archivos, pero necesitan escaso ancho de banda en los periodos ociosos entre transferencias. Esa naturaleza de transmisión no encaja bien con las tecnologías de las WANs tradicionales, las cuales fueron originalmente diseñadas para manejar tráfico a tasa constante.

Los protocolos de las redes de área local como TCP/IP asumen una serie de premisas relativas al enlace, que tienen validez en comunicaciones locales pero no en redes de área amplia. Requisitos como la capacidad de transmitir con retardo ínfimo, o la capacidad de acceder a cualquier computador central desde cualquier otro, complican la conexión de LANs a través de WANs.

Las soluciones para redes de datos desarrolladas hasta hace poco, presentan desventajas al enfrentarse al tráfico de las redes locales. X.25 (ver Figura 2.1), el protocolo conmutado por paquetes usado originalmente en redes de área amplia, está bastante limitado. Diseñado para trabajar con

medios de transmisión analógicos propensos a errores, su sistema de corrección y recuperación de errores mediante almacenamiento y reenvío es excesivo para los enlaces digitales y ópticos actuales.

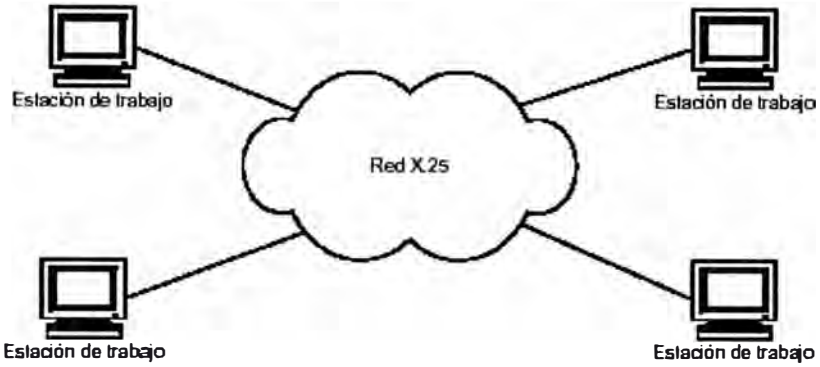


Figura 2.1 Ejemplo de red X.25.

Frame Relay ataca algunos de los problemas más importantes en la conexión de redes locales, a la vez que ofrece un ahorro en los costos y una complejidad menor.

2.2 Frame Relay.

Es un protocolo de conmutación rápida de paquetes de datos, llamados tramas (frames), que puede utilizarse como un protocolo de transporte y acceso en redes públicas o privadas, a fin de brindar servicios de telecomunicaciones

Frame Relay constituye una tecnología de enlace de datos eficiente y de alto rendimiento a nivel mundial, ha sido especialmente adaptado para velocidades de hasta 2 Mbps, aunque nada le impide superarlas. Es una forma de enviar información por una WAN dividiendo los datos en paquetes. Cada paquete viaja por una serie de *switches* en una red Frame Relay para

llegar a su destino. Funciona en las capas física y de enlace de datos del modelo de referencia OSI, pero se fundamenta en protocolos de capa superior, como TCP, para la correción de errores.

La red que proporciona la interfaz Frame Relay puede ser o bien una red pública que habilita un proveedor de servicios, o bien una red compuesta de equipamiento privado que presta servicios a una sola empresa. Frame Relay define el proceso de interconexión entre un router y el equipo de conmutación de acceso local del proveedor de servicios.

Una red Frame Relay puede estar compuesta de computadoras, servidores, etc., en el lado del usuario; y de equipamiento de acceso Frame Relay, como routers o módems, y de dispositivos de red Frame Relay, como switches, routers o multiplexores, en el lado del proveedor (ver Figura 2.2). Cabe señalar que a los dispositivos de usuario suelen denominarse equipo terminal de datos (DTE), mientras que el equipo de red que hace de interfaz con el DTE suele denominarse equipo de comunicación de datos (DCE).

El protocolo Frame Relay está basado en el concepto de uso de Circuitos Virtuales (Virtual Circuit). Un Circuito Virtual son dos vías (definidas por software) de un trayecto entre dos puertos que actúa como una línea privada en la red.

En la actualidad, hay dos tipos de conexiones Frame Relay: el Circuito Virtual Permanente (PVC, *Permanent Virtual Circuit*) y el Circuito Virtual Conmutado (SVC, *Switched Virtual Circuit*). El PVC fue el primer servicio originalmente ofrecido, pero los productos y servicios SVC están creciendo en popularidad.

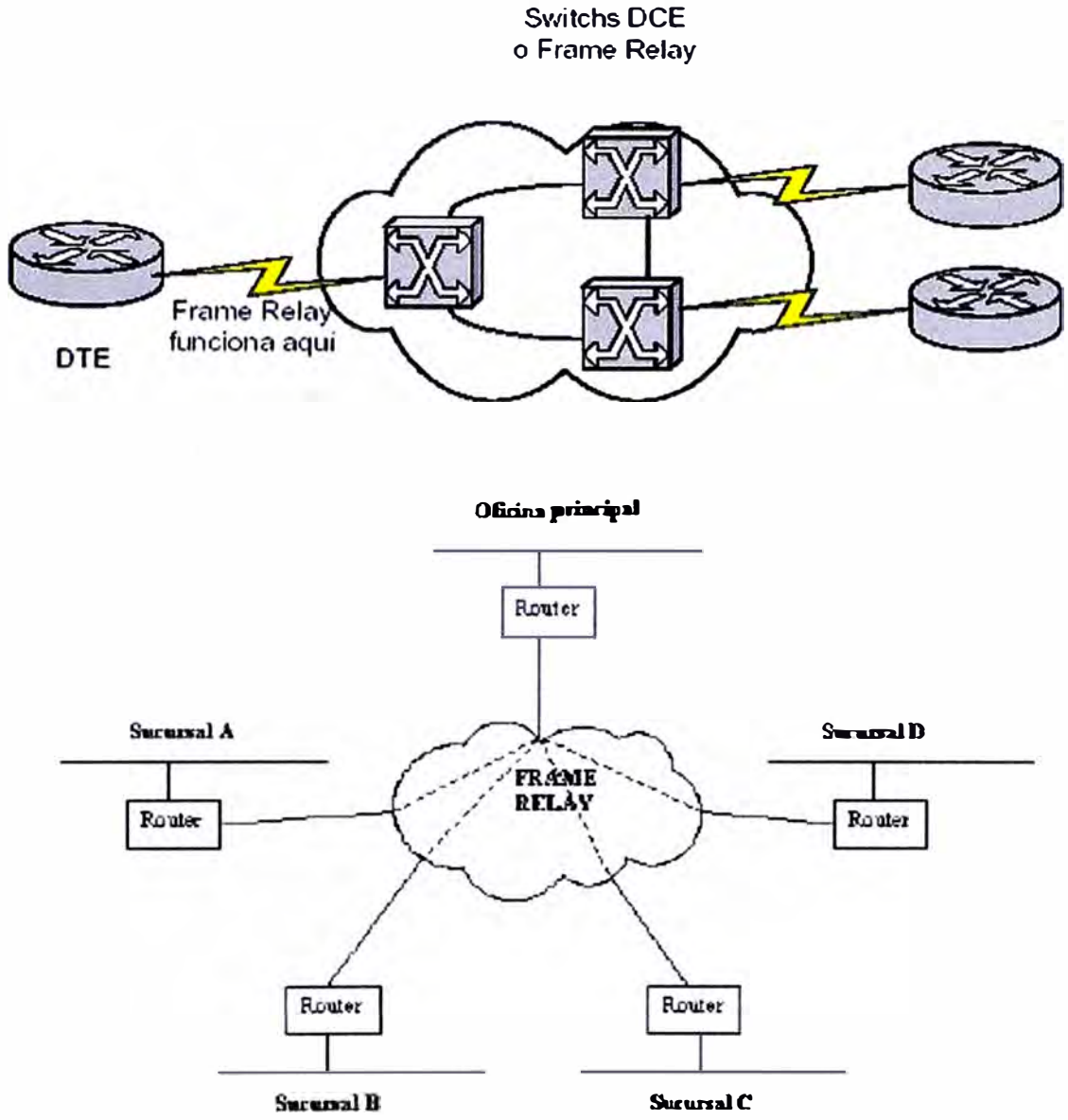


Figura 2.2 Ejemplos de redes Frame Relay.

El PVC está configurado por el ordenador de la red, desde el sistema de gestión. Los PVCs son trayectos fijos, no disponibles por demanda o sobre la base de una llamada. No obstante, el trayecto en cuestión toma a través de la red varias formas de tiempo en tiempo, nos referimos al enrutamiento automático del circuito que cambia sin afectar el comienzo y el fin del

circuito. En este sentido se puede decir que el PVC es similar a un circuito dedicado punto a punto.

La popularidad de los PVC se debe a que proveen una alternativa costo/beneficio superior a las líneas dedicadas. Para suministrar un PVC se requiere de una minuciosa planificación, un conocimiento del patrón de tráfico y la utilización del ancho de banda.

2.2.1 Principios básicos.

El protocolo Frame Relay se basa en tres principios:

- El medio de transmisión y las líneas de acceso están prácticamente libres de errores.
- La corrección de errores es proporcionada por los niveles superiores de los protocolos de las aplicaciones de usuario.
- La red (en estado normal de operación), no está congestionada, y existen mecanismos estándares de prevención y tratamiento de la congestión.

El primer principio básico señala que muchos de los protocolos más antiguos, tales como X.25, se diseñaron para operar mediante circuitos analógicos con errores. Esto exigía al protocolo de comunicación el uso de procedimientos complejos de control de errores y confirmación de información transmitida y recibida correctamente. Con la aparición de líneas de transmisión digitales, se redujo considerablemente la necesidad de estos procedimientos.

De acuerdo al segundo principio básico de Frame Relay, se requiere menos carga de proceso en la red para asegurar que los datos se transportan de manera fiable. Por tanto, es lógico el uso de procedimientos simplificados como los de Frame Relay. Esta tecnología ofrece mejor velocidad y rendimiento, porque realiza solamente un mínimo control de errores. Si se produce un error, el protocolo se limita a desechar los datos. Cuando Frame Relay desecha datos erróneos, puede hacerlo sin comprometer la fiabilidad de los datos de usuario, porque los niveles superiores de los protocolos transportados sobre él proporcionarán la corrección de errores.

Bajo el tercer principio básico, Frame Relay supone que existe una cantidad ilimitada de ancho de banda disponible. Si se produce una congestión, el protocolo desecha los datos e incluye mecanismos para "notificar explícitamente" al usuario final la presencia de congestión, y confía en que reaccionará ante estas notificaciones explícitas.

2.2.2 Terminología Frame Relay.

• **Velocidad de acceso** : la velocidad de reloj (velocidad de puerto) de la conexión a la nube Frame Realy. Es la velocidad a la que viajan los datos por la red .

• **Identificador de conexión de enlace de datos (DLCI)** : es un número que identifica el circuito lógico entre los dispositivos de origen y de destino. EL *switch* Frame Relay asigna los DLCI entre cada par de routers para crear un circuito virtual permanente (PVC)

• **Interfaz de administración local (LMI)** : es un estándar de señalización entre el dispositivo equipo terminal del abonado y el switch Frame Relay, que es el encargado de administrar la conexión y mantener el estado entre los dispositivos. Se soportan tres tipos: cisco, ansi y q933a.

• **Velocidad de información suscrita (CIR)** : la velocidad garantizada, en bits por segundo, que el proveedor de servicios se compromete a proporcionar.

• **Ráfaga suscrita (Bc)** : el máximo de bits que el switch se compromete a transferir durante un espacio de tiempo

• **Ráfaga excesiva** : el máximo de bits no comprometidos que el switch Frame Relay trata de transferir más allá de la CIR

• **Notificación explícita de la congestión (FECN)** : un bit que se establece en la trama que notifica a un DTE que el dispositivo receptor debe iniciar los procedimientos de evasión de la congestión

• **Notificación de la congestión retrospectiva (BECN)** : un bit que se establece en una trama que notifica a un DTE que el dispositivo remitente debe iniciar los procedimientos de evasión de la congestión

• **Indicador de la posibilidad de descarte (DE)** : un bit establecido que en el caso de congestión indica que trama puede ser descartada antes que otras tramas.

2.2.3 Funcionamiento del Protocolo.

a) Estructura y transmisión de tramas.

Las redes Frame Relay se construyen partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los

protocolos existentes en una única trama Frame Relay. También incorporan los nodos que conmutan las tramas Frame Relay en función del identificador de conexión, a través de la ruta establecida para la conexión en la red. Este equipo se denomina FRAD o "Ensamblador Desensamblador Frame Relay" (*Frame Relay Assembler Disassembler*) y el nodo de red se denomina FRND o "Dispositivo de Red Frame Relay" (*Frame Relay Network Device*).

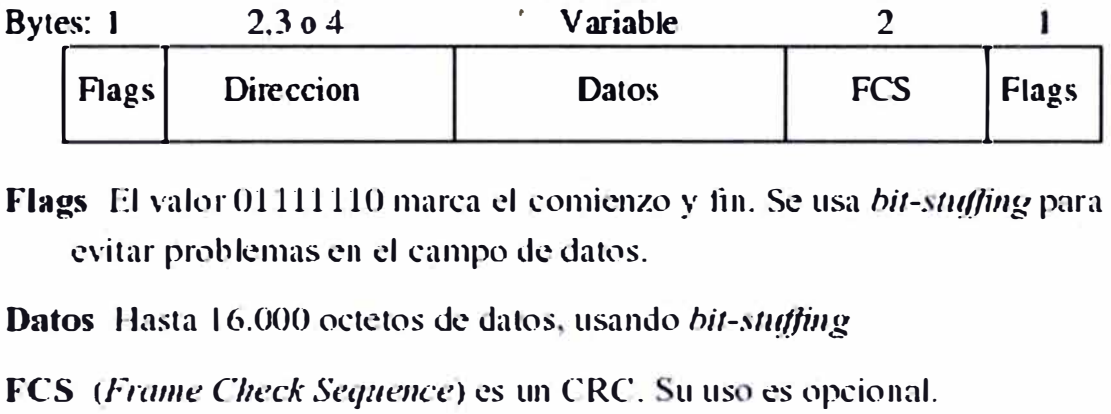


Figura 2.3 Formato de trama Frame Relay.

Las tramas y cabeceras de Frame Relay pueden tener diferentes longitudes, ya que hay una gran variedad de opciones disponibles en la implementación, conocidos como anexos a las definiciones del estándar básico. El campo Datos es de longitud variable y lleva la información transmitida en una trama Frame Relay y podrá tener hasta 16,000 bytes. Ver Figura 2.3.

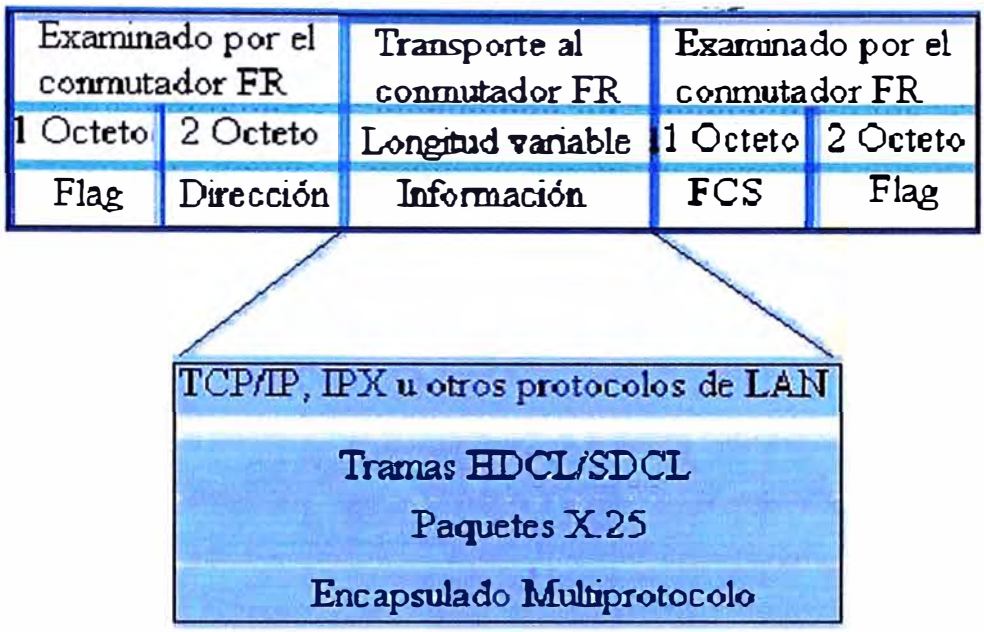


Figura 2.4 Protocolos encapsulados dentro de Frame Relay.

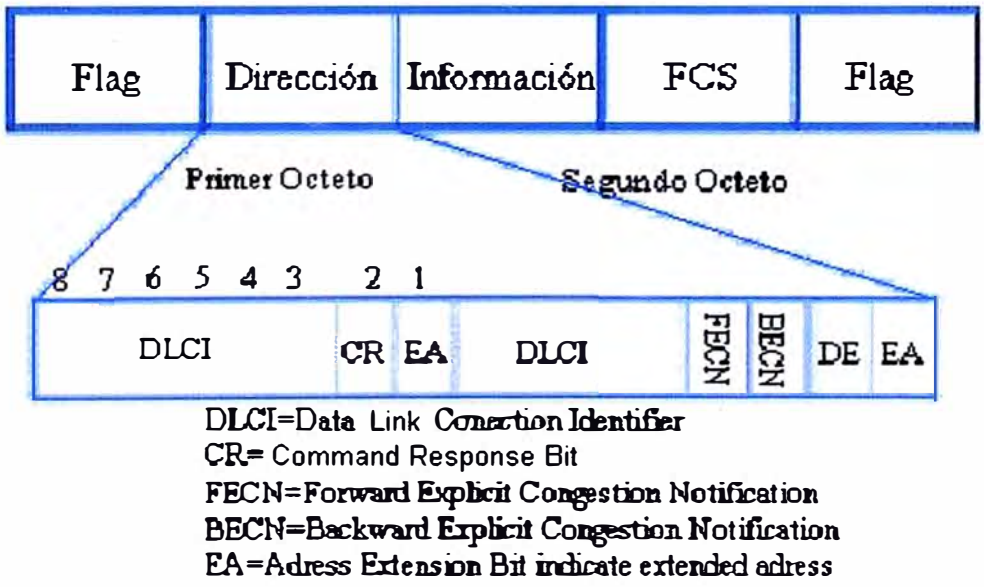


Figura 2.5 Especificaciones del campo Dirección.

La Figura 2.6 representa cómo se transmite la información de dos usuarios. Lo primero es conectar a los usuarios mediante un acceso Frame Relay (puerto en el nodo de la red más línea de acceso). Después

hay que definir en la red un CVP entre los accesos, que es el camino lógico para la transmisión de información. Un usuario puede definir más de un CVP hasta distintos destinos a través de un único acceso Frame Relay. Este concepto se llama multiplexación estadística.

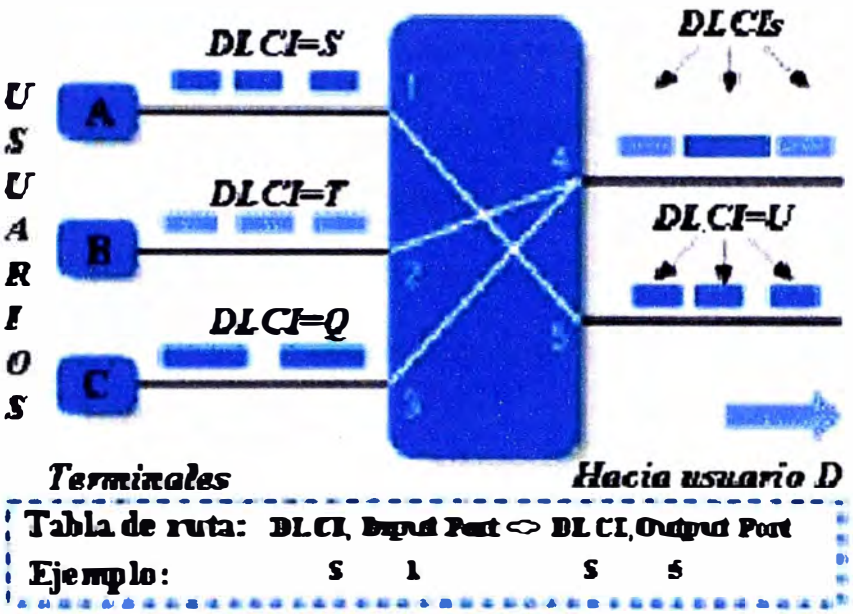


Figura 2.6 Nodo Frame Relay.

b) Parámetros de dimensionamiento de CVP (CIR, Bc, Be).

CIR (Tasa de Información Comprometida, o *Committed Information Rate*): Tasa a la cual la red se compromete, en condiciones normales de operación, a aceptar datos desde el usuario y transmitirlos hasta el destino. Puede ser distinto en cada sentido. Son las tramas 1 y 2 del ejemplo.

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

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

El tráfico entrante en la red, por encima de Bc + Be, es el descartado directamente en el nodo de entrada, (trama 4 del ejemplo). Ver Figura 2.7.

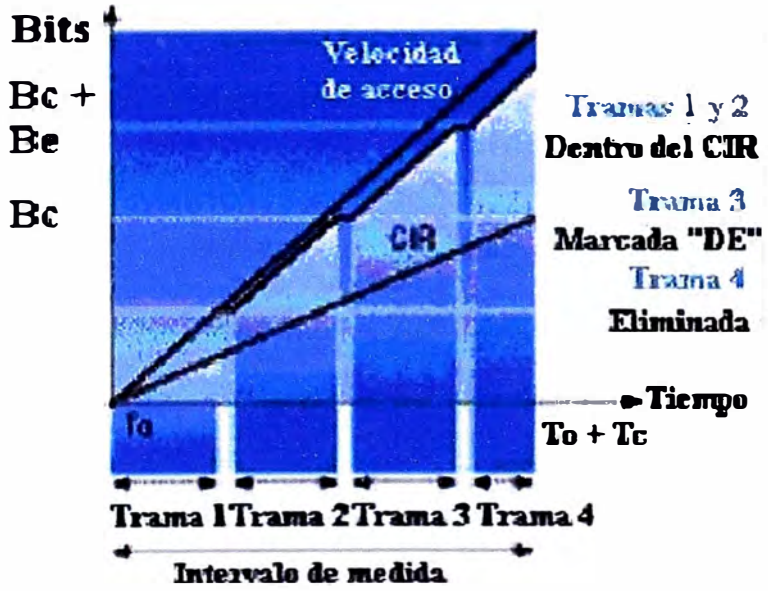


Figura 2.7 Parámetros Frame Relay.

c) Señalización de estado de líneas de acceso y CVP.

Es el conjunto de mensajes de señalización transmitidos entre la red y el equipo de acceso acerca del estado del acceso y de todos los CVP definidos.

d) Gestión y prevención de la congestión.

En la trama, y dentro del campo de "Dirección" está el DLCI y otros bits que se utilizan para la gestión de la congestión. Ver Figura 2.5.

Los FECN y BECN son activados por la red cuando empieza a detectar que el tráfico aumenta y debe evitar congestionarse. Así, todas las tramas que pasan por el nodo, hacia el destino (forward), hacia el origen (backward), con FECN y BECN activados, se entregan a cada equipo de acceso del usuario.

El equipo de acceso que recibe tramas con BECN activo puede reducir la cantidad de información enviada a la red hasta que ya no reciba más. El equipo de acceso conectado en el destino, que recibe tramas con el FECN activo, puede controlar al equipo de acceso conectado en el origen, utilizando mecanismos de control de flujo y ventana de transmisión de niveles superiores. Las tramas con DE activo pueden ser descartadas por la red si sigue habiendo congestión.

2.2.4 Ventajas y beneficios.

a) Alta velocidad y bajo retardo.

b) Soporte eficiente para tráficos a ráfagas.

c) Flexibilidad y escalabilidad debido a la configuración de VPNs a través de PVCs.

d) Eficiencia.

e) Buena relación costos/prestaciones.

f) Transporte integrado de distintos protocolos de voz y datos.

g) Conectividad "todos con todos".

h) Simplicidad en la gestión.

i) Interfaces estándares.

CAPÍTULO III

MULTIPROTOCOL LABEL SWITCHING (MPLS)

3.1 Introducción.

La red IP se ha convertido en una extensa red en la que las posibilidades de negocio y los mercados de consumo inducen al desarrollo de nuevas aplicaciones.

Son las aplicaciones de voz y multimedia las que requieren mayor ancho de banda y, que éste, esté garantizado durante todo el servicio. Estos requerimientos hacen que los recursos de la red estén sobre utilizados en términos de velocidad y ancho de banda. Además de estos requerimientos, se debe poder ofrecer clases diferenciadas de servicio a los distintos usuarios que utilizan la red.

Se avanza más hacia una convergencia entre voz y datos en la red IP y su infraestructura y protocolos han sido optimizados sólo para datos, de modo que IGP (*Interior Gateway Protocol*) como RIP (*Routing Information Protocol*) y OSPF (*Open Shortest Path First*) y EGP (*Exterior Gateway Protocol*) como BGP4 (*Border Gateway Protocol v4*), no son la solución óptima. Muchos de

estos protocolos de *routing* están basados en algoritmos para obtener el camino más corto (como RIP y BGP4, basados en el vector distancia) sin tener en cuenta métricas adicionales como retardo, jitter y congestión del tráfico. Todo esto se traduce en una sobrecarga en el *router* IP, problemas de propagación de las rutas y la obligación de integrar redes IP con ATM.

MPLS ha sido desarrollado para eliminar varios de estos problemas. Tiene la capacidad de soportar cualquier tipo de tráfico en una red IP sin tener que supeditar el diseño de la red a las limitaciones de los diferentes protocolos de *routing*, capas de transporte y esquemas de direcciones.

3.2 Tecnología MPLS.

El MultiProtocol Label Switching es un grupo de trabajo específico del IETF (*Internet Engineering Task Force*) que trata sobre el encaminamiento, envío y conmutación de los flujos de tráfico a través de la red.

Las principales funciones de MPLS son:

- Especificar mecanismos para gestionar flujos de tráfico de diferentes tipos (Ejemplo: flujos entre diferente *hardware*).
- Quedar independiente de los protocolos de la capa de enlace y la capa de red.
- Disponer de medios para traducir las direcciones IP en etiquetas simples de longitud fija utilizadas en diferentes tecnologías de envío y conmutación de paquetes.
- Ofrecer interfaces para diferentes protocolos de *routing* y señalización.

- Soportar los protocolos de la capa de enlace de IP, ATM y Frame Relay.

En MPLS la transmisión ocurre en caminos de etiquetas conmutadas (LSP, *Label Switched Path*), que son secuencias de etiquetas en cada nodo del camino desde el emisor al receptor. Hay dos formas de requerir los LSPs: antes de la transmisión de datos (control-driven) y una vez detectado un cierto flujo de datos (data-driven).

Las etiquetas se distribuyen utilizando un protocolo de señalización como LDP (*Label Distribution Protocol*) o RSVP (*ReSource reserVation Protocol*), o también añadidas a protocolos de *routing* como BGP u OSPF.

Las etiquetas son insertadas al comienzo del paquete en la entrada de la red MPLS. En cada salto el paquete es encaminado según el valor de la etiqueta y sale por la interfaz correspondiente con otra etiqueta. Se obtiene una gran rapidez en la conmutación gracias a que las etiquetas son insertadas al principio del paquete y son de longitud fija, lo que hace que pueda hacerse una conmutación vía *hardware*.

3.2.1 Terminología MPLS.

a) FEC (*Forward Equivalence Class*).

Conjunto de paquetes que comparten unas mismas características para su transporte, así todos recibirán el mismo tratamiento en su camino hacia el destino. La asignación de un paquete a un determinado FEC se produce una vez que el paquete entra en la red. Cada FEC puede

representar unos requerimientos de servicio para un conjunto de paquetes o para una dirección fija.

b) LSR (*Label Switched Router*).

Router de gran velocidad en el núcleo de una red MPLS, cuyas funciones son las siguientes:

- Participar en el establecimiento de los LSPs usando un protocolo de señalización apropiado.
- Conmutar rápidamente el tráfico de datos entre los caminos establecidos.

Para que los LSPs puedan usarse, las tablas de envío de cada LSR deben contener: interfaz de entrada - etiqueta asociada e interfaz de salida - etiqueta asociada. A este proceso se le llama distribución de etiquetas. Como un LSP puede dar servicio a un *host* IP o a muchos, existe otra entrada en la tabla: FEC - etiquetas asociadas.

c) LER (*Label Edge Router*).

Router en la frontera de la red al que se pueden conectar diversas redes (Frame Relay, ATM, Ethernet). Envía el tráfico entrante a la red MPLS utilizando un protocolo de señalización de etiquetas y distribuye el tráfico saliente entre las distintas redes.

3.2.2 Etiquetas.

Las etiquetas identifican el camino que un paquete puede atravesar. La etiqueta es encapsulada en la cabecera de la capa de enlace. Una vez el paquete ha sido etiquetado viajará a través del *backbone* mediante

conmutación de etiquetas, es decir, cada *router* examinará la etiqueta, consultará en sus tablas de envío para saber con qué etiqueta y por qué interfaz debe salir, intercambiará las etiquetas y lo enviará por el interfaz correspondiente.

Pasos para la asignación de etiquetas:

- Cada paquete se clasifica como un nuevo FEC o se le asigna un FEC ya existente.
- Se asigna una etiqueta a cada paquete. Éstas se derivan de la capa de enlace, es decir, para redes Frame Relay, ATM o redes ópticas, los identificadores de la capa 2 (DLCIs, VPIs/VCIs y longitud de onda DWDM, respectivamente) pueden servir como etiquetas. Para redes como Ethernet y PPP (Point to Point Protocol), a la etiqueta se le añade una cabecera *shim* entre las cabeceras de la capa de enlace y la capa de red, que contendrá el campoTTL (Time To Live).

Las decisiones de asignación de etiquetas pueden estar basadas en criterios de envío como encaminamiento *unicast*, *multicast*, ingeniería de tráfico, VPN (Virtual Private Network) y QoS (Quality of Service).

Las etiquetas constan de 32 bits y tienen el siguiente formato:

- Etiqueta (20 bits): contiene la etiqueta asignada.
- CoS (3 bits): indica la clase de servicio que requiere el paquete.

Pila (1 bit): permite apilar etiquetas en un paquete para realizar un encaminamiento jerárquico.

- TTL (8 bits): tiene el mismo significado que en IP, se denomina cabecera *shim*.

Bucles: El campo TTL indica el tiempo máximo de vida del paquete contado en saltos entre LSRs, este mecanismo permite mitigar los efectos de la creación de un bucle en la red haciendo desaparecer el paquete en el momento que supere este tiempo.

En ATM o Frame Relay donde no es posible utilizar TTL, los efectos de los bucles se minimizan mediante la limitación del espacio en *buffers* para un único VC (*Virtual Channel*).

Otra alternativa para detectar bucles es mediante la técnica Vector de Rutas (Path Vector). Este vector contiene la lista de los LSRs que atraviesa el LSP, cuando un LSR propaga un mensaje de control del LDP (*Label Distribution Protocol*) añade su identificador al vector que irá en ese mensaje, por lo tanto, cuando un LSR reciba un mensaje en cuyo vector de caminos se encuentre su propio identificador se detectará el bucle.

Hay que hacer notar que los bucles sólo se producirán en el encaminamiento salto a salto y en el encaminamiento explícito tolerante que se verá más adelante.

Pila de etiquetas: Permite operaciones jerárquicas en MPLS, cada nivel en la pila de etiquetas pertenece a un nivel jerárquico, esto facilita la creación de túneles en MPLS.

Para realizar el encaminamiento mediante túneles veamos un ejemplo (Figura 3.1):

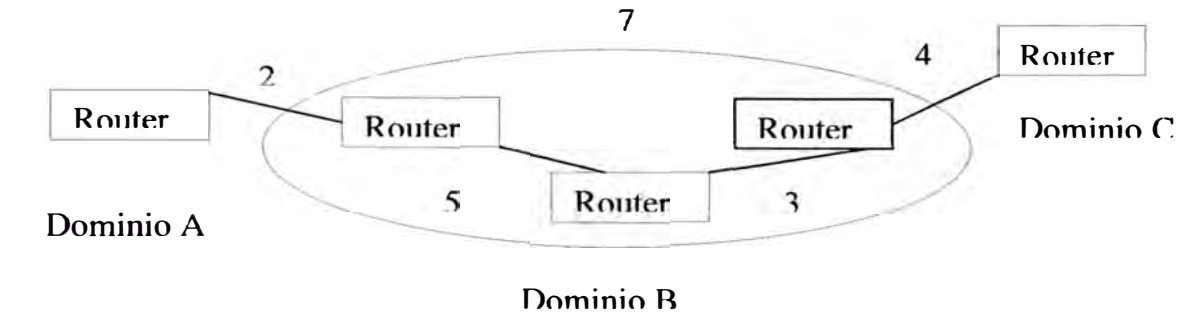


Figura 3.1 Encaminamiento por túneles.

Encaminamiento:

- La secuencia de etiquetas entre dominios es: 2-7-4
- La secuencia de etiquetas dentro del dominio B es: 5-3

Las operaciones que se realizarán son:

- Del dominio A al B el paquete llevará la etiqueta 2. En el *router* de entrada al dominio B se intercambiará la etiqueta 2 por la 7, que identifica al nuevo dominio, y apila la etiqueta 5 que indica el siguiente salto en esa red.
- En el siguiente *router* se intercambiará la etiqueta 5 por la 3.
- En el *router* de salida se desapila 3 y ve que la etiqueta de entrada que tiene es 7, e intercambia ésta con 4 para llegar al siguiente dominio.

Para la distribución de etiquetas:

- MPLS permite varios protocolos de señalización para la distribución de etiquetas entre LSRs, el uso de cada uno de ellos dependerá del *hardware* de la red MPLS y de las políticas de administración de ésta.

- Protocolos de *routing* como BGP permiten llevar *piggybacked* información sobre las etiquetas entre los contenidos propios del protocolo, se utilizan para etiquetas externas en VPNs.
- RSVP también ha sido extendido para soportar intercambio de etiquetas *piggybacked*.
- Además, MPLS tiene su propio protocolo LDP para señalización y gestión del espacio de etiquetas, a éste se le han añadido extensiones para soportar, también, requerimientos de QoS y CoS (*Class of Service*), así tenemos CR-LDP (*Constraint based* – LDP).
- RSVP y CR-LDP se utilizan para la ingeniería de tráfico y reserva de recursos.
- Para direcciones *multicast* tenemos PIM (*Protocol-Independent Multicast*).

3.2.3 LSP (Label Switched Path).

Cuando un paquete entra en la red MPLS se examina para determinar qué LSP debe asociársele y, a partir de aquí, qué etiqueta asignarle. Esta decisión se debe a factores como la dirección de destino, QoS y el actual estado de la red.

Un **Dominio MPLS** es un conjunto de dispositivos habilitados en MPLS. Dentro de un dominio MPLS, un camino es establecido para que un paquete dado viaje con un determinado FEC. Existen dos mecanismos para establecer un LSP:

- **Encaminamiento salto a salto:** Cada LSR selecciona independientemente el próximo salto para un FEC determinado (similar a la metodología utilizada en redes IP). El LSR utiliza cualquier protocolo de *routing* disponible como OSPF, ATM PNNI (*ATM Private Network-Node Interface*),etc.
- **Encaminamiento explícito:** El LER de entrada determina la secuencia de saltos explícita desde la entrada hasta la salida (ER-LSP, Explicit Routing LSP). Puede que la ruta no esté completamente especificada, es decir, puede haber un conjunto de nodos (Nodo Abstracto) que es representado como un único salto en la ruta. También puede contener un identificador de Sistema Autónomo que permite que el LSP sea encaminado a través de un área de la red que está fuera del control administrativo de quien inició el LSP.

Dentro de estos dos casos se hará un encaminamiento salto a salto. Puede clasificarse como **estricto** (*strict*), aquel camino que incluye todos los nodos, nodos abstractos y Sistemas Autónomos por los que pasa y el orden establecido; o como **tolerante** (*loose*), aquél que incluye todos los saltos y mantiene el orden, pero puede incluir saltos que sean necesarios para alcanzar algún salto específico.

El camino puede que no sea óptimo puesto que deben tenerse en cuenta los parámetros del servicio. Los recursos serán reservados a lo largo del camino para asegurar QoS. Esto facilita la ingeniería de tráfico y el poder

tener servicios diferenciados usando políticas de tráfico o métodos de gestión de red.

El establecimiento de un LSP para un FEC es unidireccional. El tráfico de vuelta debe tomar otro LSP.

Cuando se detecte un fallo en la red o la topología cambie se debe de proporcionar un nuevo LSP para reencaminar el tráfico. En una ruta explícita estricta sólo se puede reencaminar el tráfico en el LER de entrada que es quien decide la ruta, con lo que debe ser informado del error para proporcionar una ruta alternativa. En una ruta explícita tolerante cualquier LSP puede tomar un camino alternativo si es capaz de detectar el fallo del vecino, si la ruta ya está disponible o si un LSP de mayor prioridad requiere esos recursos reservados.

3.3 Ingeniería de tráfico.

La ingeniería de tráfico es el proceso que mejora la utilización de la red mediante la distribución del tráfico en ella; de acuerdo con la disponibilidad de los recursos, el tráfico actual y el esperado. CoS y QoS pueden ser factores a tener en cuenta en este proceso.

Como resultado, tenemos que se evita la congestión en cualquier camino. La mejora de la utilización de la red no implica necesariamente que se obtenga el mejor camino, pero sí el mejor camino para un determinado tipo de tráfico.

La ingeniería de tráfico permite al proveedor hacer un mejor uso de los recursos y permitir reservar enlaces para determinadas clases de servicio o clientes.

Aquí encontramos el caso de las rutas forzadas. La ruta que un LSP puede tomar puede forzarse para que cumpla unos requerimientos seleccionados en el LER de entrada (un caso particular de ellas son las rutas explícitas, donde el parámetro que fuerza este camino es el orden que debe seguir). Los parámetros que pueden ser utilizados para describir esas rutas son el ancho de banda, el retardo, la prioridad, etc., que se desea para un flujo de tráfico.

Para calcular estas rutas existen dos métodos:

1. Calcular en el LER de entrada toda la ruta basándose en información sobre el estado de la red.
2. Calcular la ruta salto a salto con información local a cada LSR sobre la disponibilidad de los recursos.

Los dos métodos pueden combinarse si en alguna parte de la ruta la información no está disponible (por ejemplo: en un Sistema Autónomo).

Pero no basta sólo con obtener la ruta, es necesario reservar los recursos para poder satisfacer el servicio requerido.

Existen dos aproximaciones: TE-RSVP y CR-LDP, ambas utilizan el encaminamiento explícito para crear los LSPs e introducen una sobrecarga de información adicional al crear, mantener y destruir un LSP, pero ésta, es mínima comparada con la generada al procesar la cabecera IP.

3.3.1 Método TE-RSVP.

TE-RSVP (*Trafic Engneering – RSVP*) es una extensión del protocolo RSVP.

TE-RSVP es un protocolo de señalización *soft state* que utiliza UDP o datagramas IP para la comunicación entre compañeros LSR (LSR *peers*).

Creación de un ER-LSP:

El LER de entrada quiere establecer un nuevo LSP hacia el LER de salida. Los parámetros de tráfico determinan por dónde debe pasar la ruta, así que el LER de entrada envía un mensaje PATH con la ruta explícita hacia el LER de salida y con los parámetros de tráfico que requiere la sesión.

- Cada nodo de la ruta que recibe el mensaje determina si es la salida para ese LSP, si no lo es, sigue enviando el mensaje PATH eliminándose de la ruta. En cualquier caso cada LSR creará una nueva sesión.
- Una vez llega al LER de salida, éste determina qué recursos ha de reservar y devuelve un mensaje RESV que distribuirá la etiqueta que ha elegido para ese LSP y contendrá los detalles de la reserva.
- Los LSRs intermedios emparejan los mensajes PATH y RESV que han recibido según el identificador de LSP, reservan los recursos que indica RESV, asignan una etiqueta para el LSP, rellenan la tabla de envío y envían la nueva etiqueta en otro mensaje RESV.
- El LER de entrada, cuando lo recibe, enviará un mensaje de confirmación RESVConf para indicar que se ha establecido el LSP.

Después de haberse establecido el LSP se enviarán mensajes periódicos para mantener el camino y las reservas.

3.3.2 Método CR-LDP.

CR-LDP (*Constraint based - LDP*), a diferencia de TE-RSVP, no necesita de implementaciones adicionales ya que está basado en LDP y utiliza su misma estructura para los mensajes.

Es un protocolo *hard state* y utiliza sesiones TCP entre compañeros LSR.

Creación de un ER-LSP:

- El LER de entrada quiere establecer un nuevo LSP hacia el LER de salida. Los parámetros de tráfico determinan por dónde debe pasar la ruta, así que el LER de entrada reserva los recursos que necesita y envía un mensaje LABEL_REQUEST con la ruta explícita hacia el LER de salida y con los parámetros de tráfico que requiere la sesión.
- Cada nodo de la ruta que recibe el mensaje reserva los recursos y determina si es la salida para ese LSP, si no lo es, sigue enviando el mensaje LABEL_REQUEST eliminándose de la ruta. Puede reducir la reserva si los parámetros de tráfico están marcados como negociables.
- Una vez llega al LER de salida, éste realiza cualquier negociación final sobre los recursos y hace la reserva. Asigna una nueva etiqueta al nuevo LSP y la distribuye en un mensaje LABEL_MAPPING que contiene los parámetros de tráfico finales reservados para el LSP.
- Los LSRs intermedios emparejan los mensajes LABEL_REQUEST y LABEL_MAPPING que han recibido según el identificador de LSP,

asignan una etiqueta para el LSP, rellenan la tabla de envío y envían la nueva etiqueta en otro mensaje LABEL_MAPPING.

- En cuanto llegue al LER de entrada se habrá establecido el LSP.

3.3.3 Comparación de ambos métodos.

- TE-RSVP es *soft state,* lo cual significa que la información es intercambiada cuando se establece el LSP, pero se deben enviar mensajes periódicos para notificar que la conexión todavía se requiere. Por el contrario, CR-LDP es *hard state*, es decir, toda la información se intercambia al iniciar la conexión y no se produce más información adicional hasta que el LSP se elimine.
- El hecho que TE-RSVP sea *soft state* e introduzca una sobrecarga adicional hace que no sea escalable ya que esta sobrecarga crecerá proporcionalmente con el número de sesiones RSVP. Para evitar esto se intenta resumir la información y aprovechar un único mensaje para enviar varios mensajes de refresco.
- CR-LDP utiliza conexiones TCP lo que hace que éstas sean más fiables y seguras, mientras que TE-RSVP utiliza UDP o datagramas IP para establecer las comunicaciones, lo que supone mayor vulnerabilidad aunque puede utilizar IPSec o algún otro esquema de encriptación.
- Las conexiones TCP de CR-LDP permiten detectar un fallo mediante notificaciones propias de TCP. Esta notificación se procesa rápidamente así que las acciones oportunas sean iniciadas.

Sin embargo, una conexión fallida en TE-RSVP será detectada cuando no se reciba un determinado mensaje de refresco y, dependiendo de cómo se haya configurado, detectar un fallo tardará segundos o minutos antes de que puedan iniciarse las acciones de recuperación.

- Ambos protocolos soportan re-encaminamiento (*re-routing*): TE-RSVP puede crear una nueva ruta a partir de un salto diferente en un LSR, así, en el momento en que se detecte el fallo refrescará esta nueva ruta que pasará a ser operativa y, la antigua se eliminará cuando deje de recibir mensajes de refresco. Otra alternativa que soportan ambos protocolos es crear una ruta completa alternativa mientras se usa la antigua, en el momento que se produzca un fallo la nueva ruta será operativa y se eliminará la antigua.
- CR-LDP soporta que un LSP dé servicio a muchos *hosts* mediante la designación de FECs, mientras que RSVP sólo reserva ancho de banda a una única dirección IP.

La elección entre los diferentes protocolos se deberá a factores como la complejidad de la red, si las conexiones van a ser cortas o permanentes, qué grado de tolerancia a fallos se requiere, etc.

CAPÍTULO IV

REDES PRIVADAS VIRTUALES IP (IP VPN)

4.1 Introducción.

En la actualidad es una necesidad vital en las empresas y organizaciones el compartir información, particularmente acuciante para aquellas cuyas oficinas se encuentran dispersas en diferentes secciones de la organización o separadas geográficamente.

Años atrás, todavía no era tan importante el conectar usuarios a Internet para cuestiones de trabajo, pero a medida que ha pasado el tiempo las compañías han querido que sus redes LAN trasciendan más allá del ámbito de sus oficinas e incluyeran a los trabajadores y centros de información de otros edificios, ciudades, estados o incluso otros países, teniendo que invertir en hardware y servicios de telecomunicaciones costosos para crear redes amplias de servicio, WAN. Sin embargo ya con Internet, las compañías tienen la posibilidad de crear una Red Privada Virtual que demanda una inversión relativamente pequeña de hardware y utiliza Internet global para la conexión entre los puntos de la red.

Durante un tiempo, grandes organizaciones habían solucionado el problema mediante sistemas de comunicación como líneas punto a punto y sofisticadas instalaciones de interconexión. Aunque efectivas, estas soluciones quedaban fuera del alcance de organizaciones de menor tamaño y con recursos económicos y técnicos más escasos.

Las redes tipo LAN que permiten comunicación entre varios ordenadores en una misma oficina, con la aparición de las nuevas tecnologías, hoy en día es posible conectar esta red LAN a Internet. Esta conexión puede ser de varias maneras:

- Unidireccional: conexión a Internet desde la red LAN para consulta de información.
- Bidireccional: el acceso es en ambas direcciones, desde la LAN hacia Internet o bien desde Internet hacia la LAN.

Las últimas alternativas de comunicación, han hecho que pequeñas y medianas empresas dispongan de su propia red de comunicación privada. Ahora, las centrales y tiendas o sucursales disponen de su propia red de comunicación privada. Ahora, pueden intercomunicarse y compartir información de forma sencilla y segura, con inversiones muy inferiores a las de hace algunos años atrás.

Las LAN tradicionales son redes esencialmente restringidas, por lo cual se puede intercambiar información entre las computadoras sin pensar en la seguridad de la información; pero Internet no es seguro, por lo tanto las VPN usan protocolos especiales que permiten encriptar información y permitir

únicamente a personal autorizado desencriptar esa información con un identificador que comprueba que la transmisión se ha hecho desde una fuente confiable.

4.2 Redes Privadas.

Una red privada está compuesta de ordenadores que son propiedad de una sola organización, los cuales intercambian información específica entre ellos. Los usuarios están seguros de que son los únicos en la red, y que la información enviada entre ellos sólo podrá ser vista por otros usuarios del grupo (en el peor de los casos). Las típicas LAN o WAN corporativas son un ejemplo de redes privadas.

La línea de separación entre una red pública y otra privada la establece un *router*, donde la compañía sitúa un *firewall* para evitar el paso de usuarios de una red pública a su red privada o para conseguir que los usuarios de la red privada no accedan a la red pública.

Tiempo atrás las compañías podían permitir que sus LAN operasen por separado, aisladamente. Cada oficina debía tener su propia LAN, con su propio esquema de nombres, sistema de correo electrónico e incluso su propio protocolo de red. Cuantos más recursos de las compañías se movían a los ordenadores, mayor era la necesidad de interconectar las oficinas. Esto tradicionalmente se hacía usando líneas telefónicas de velocidades variables. Usando líneas alquiladas, las compañías pueden asegurar que la conexión esté siempre disponible y sea privada; pero esto puede llegar a ser muy caro si la compañía tiene oficinas a lo largo de todo el país.

4.3 Red Privada Virtual (VPN, *Virtual Private Network*).

Se entiende por Red Privada Virtual o VPN a la interconexión de una o más redes por medio de una infraestructura pública (normalmente compartida), como por ejemplo Internet u otras infraestructuras WAN tales como: Frame Relay, ATM, etc. Esto para simular una infraestructura dedicada o privada. Se dice que es "virtual" porque el usuario tendrá la sensación de estar en una única red; y "privada" porque la comunicación a través de ella es segura y protegida. También un usuario remoto se puede conectar individualmente a una LAN utilizando una conexión VPN, y de esta manera utilizar aplicaciones, enviar datos, etc. de manera segura. Ver Figura 4.1.

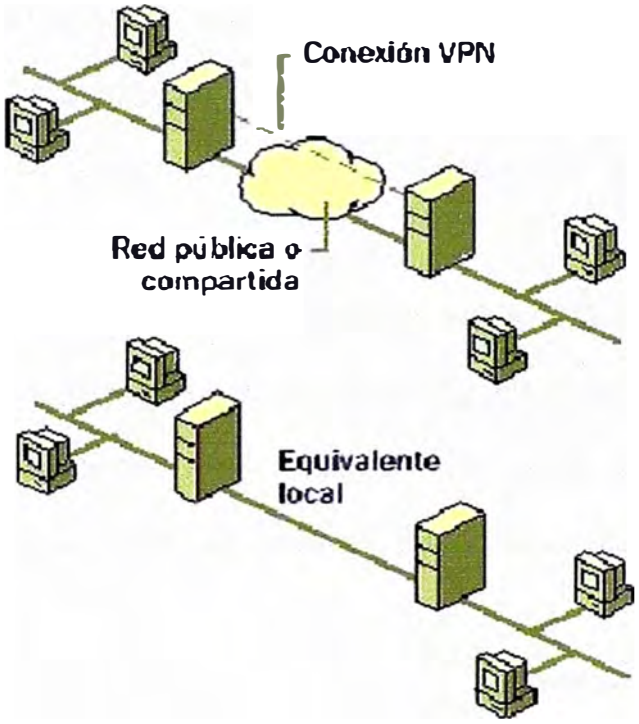


Figura 4.1 Diagrama Lógico de una VPN.

Las VPNs utilizan tecnología de túnel (*tunneling*) para la transmisión de datos mediante un proceso de encapsulación y en su defecto de encriptación, esto es importante a la hora de diferenciar Redes Privadas Virtuales y Redes Privadas, ya que esta ultima utiliza líneas telefónicas dedicadas para formar la red.

El objetivo a conseguir es que todo se haga de forma transparente a la aplicación, es decir, una aplicación debe seguir funcionando a través de la VPN exactamente igual que lo hace cuando se accede a ella desde la red corporativa sin necesidad de realizar ninguna modificación en la misma.

4.4 Ventajas de las VPN.

Una de las principales ventajas de una VPN es la seguridad, los paquetes viajan a través de infraestructuras publicas(Internet) en forma encriptada y a través del túnel de manera que sea prácticamente ilegible para quien intercepte estos paquetes.

Esta tecnología es muy útil para establecer redes que se extienden sobre áreas geográficas extensas. Por ejemplo diferentes ciudades y a veces hasta países y continentes. Para usuarios con poca experiencia es fácil conectarse a grandes redes corporativas transfiriendo sus datos de forma segura.

Para empresas que tienen oficinas remotas en puntos distantes, la idea de implementar una VPN haría reducir notablemente los costos de comunicación, dado que las llamadas telefónicas (en caso de usar dial-up) serian locales (al proveedor de Internet) o bien utilizar conexiones DSL, en

tanto que de otra manera habría que utilizar líneas dedicadas las cuales son muy costosas o hacer tendidos de cables que serian mas costosos aún.

Con una VPN se mejora la administración de red. Cada usuario que se conecta puede tener un numero de IP fijo asignado por el administrador, lo que facilita algunas tareas como por ejemplo mandar impresiones remotamente, aunque también es posible asignar las direcciones IP dinámicamente si así se requiere.

4.5 Proceso de Túnel (*Tunneling*).

La tecnología de túneles (*Tunneling*) es un modo de transferir datos entre 2 redes similares sobre una red intermedia. También se le llama "encapsulación", a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo. La tecnología de túneles VPN, añade otra dimensión al proceso de túneles con encapsulación, ya que los paquetes están encriptados de forma que los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original.

El principio de funcionamiento para el Proceso de Túnel es el siguiente: para enviar un paquete IP del Host1 al Host2, el Host1 construye el paquete que contiene la dirección IP del Host2, lo inserta en un marco ethernet dirigido al router multiprotocolo que enlaza la intranet1, y lo coloca en el marco ethernet. Cuando el router multiprotocolo recibe el marco, retira el paquete IP, lo inserta en el campo de carga útil del paquete de capa de red de la

WAN, y dirige este último a la dirección de la WAN del router multiprotocolo que enlaza con la intranet2. Al llegar ahí, el router retira el paquete IP y lo envía al Host2 en un marco ethernet.

Figura 4.2 Túnel VPN.

La WAN puede visualizarse como un gran túnel que se extiende de un router multiprotocolo a otro. El paquete IP simplemente viaja de un extremo del túnel al otro.

Sólo el router multiprotocolo tiene que entender los paquetes IP y WAN. Las Redes Privadas Virtuales crean un túnel o conducto dedicado de un sitio a otro.

La tecnología de autenticación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor.

El uso de la encriptación en la conexión VPN puede ser necesario en aquellos casos que la información que se vaya a pasar por el túnel sea sensible y requiera privacidad. La conexión encriptada VPN requiere de bastantes recursos tanto en el servidor del túnel como en el ordenador

cliente de VPN a parte de requerir la instalación de software especial en el cliente.

Existen muchas aplicaciones y programas que ya hacen dicha encriptación y el encriptar el túnel VPN no nos aporta seguridad adicional. Aplicaciones tales como el correo seguro leído por medio de un interfaz web seguro o una conexión ssh a una máquina multiusuario son suficientemente seguros para no requerir la encriptación adicional, a parte que al encriptar entre el servidor de la aplicación y el cliente de la misma la conexión es absolutamente segura en todo su recorrido, mientras que en una conexión VPN segura la encriptación sólo tiene lugar entre el servidor de túnel y el cliente VPN y la conexión entre el servidor de túneles y el servidor de la aplicación se realiza sin encriptación.

4.6 Tipos de VPN.

Las formas en que pueden implementar las VPNs pueden ser basadas en hardware o a través de software, pero lo más importante es el protocolo que se utilice para la implementación.

Las VPNs basadas en hardware utilizan básicamente equipos dedicados como por ejemplo los routers, son seguros y fáciles de usar, ofreciendo gran rendimiento ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema operativo el cual utiliza muchos recursos del procesador para brindar otros servicios, en síntesis, los equipos dedicados son de fácil implementación y buen rendimiento, solo que las

desventajas que tienen son su alto costo y que poseen sistemas operativos propios y a veces también protocolos que son propietarios.

4.7 Tecnologías para implementar una VPN.

Existen diferentes tecnologías para armar VPNs:

- DLSW: Data Link Switching(SNA over IP)
- IPX for Novell Netware over IP
- GRE: Generic Routing Encapsulation
- ATMP: Ascend Tunnel Management Protocol
- IPSEC: Internet Protocol Security Tunnel Mode
- PPTP: Point to Point Tunneling Protocol
- L2TP: Layer To Tunneling Protocol

Entre los mas usados y con mejor rendimiento estarían IPSEC, PPTP y L2TP.

4.7.1 IPSEC (*Internet Protocol Secure*).

Es un protocolo de seguridad creado para establecer comunicaciones que proporcionen confidencialidad e integridad de los paquetes que se transmiten a través de Internet.

IPSEC puede utilizar dos métodos para brindar seguridad: ESP (*Encapsulating Security Payload*) o AH (*Authentication Header*). La diferencia entre ESP y AH es que el primero cifra los paquetes con algoritmos de cifrado definidos y los autentica, en tanto que AH solo los

autentica. AH firma digitalmente los paquetes asegurándose la identidad del emisor y del receptor.

IPSEC tiene dos tipos de funcionamiento, uno es el modo transporte en el cual la encriptación se produce de extremo a extremo, por lo que todas las maquinas de la red deben soportar IPSEC, y el otro es el modo túnel, en el cual la encriptación se produce solo entre los routers de cada red. Esta ultima forma seria la mas ordenada de organizar una red VPN basada en IPSEC.

Existen diferentes productos para implementar VPN con IPSEC en GNU/Linux, pero sin dudas el mas utilizado es el Freeswan.

4.7.2 PPTP (*Point to Point Tunneling Protocol*).

Este es uno de los protocolos mas populares y fue originalmente diseñado para permitir el transporte (de modo encapsulado) de protocolos diferentes al TCP/IP a través de Internet.

Fue desarrollado por el foro PPTP, el cual esta formado por las siguientes empresas: Ascend Communications, Microsoft Corporations, 3 Com, E.C.I. Telematics y U.S. Robotics(ahora 3 Com).

Básicamente PPTP encapsula los paquetes del Protocolo Punto a Punto PPP(Point to Point Protocol) que a su vez ya vienen encriptados en un paso previo para poder enviarlos a través de la red.

El proceso de encriptación es gestionado por PPP y luego es recibido por PPTP, este ultimo utiliza una conexión TCP llamada conexión de control para crear el túnel y una versión modificada de la Encapsulación de

Enrutamiento Generico (GRE, Generic Routing encapsulation) para enviar los datos en formato de datagramas IP, que serian paquetes PPP encapsulados, desde el cliente hasta el servidor y viceversa.

El proceso de autenticación de PPTP utiliza los mismos métodos que usa PPP al momento de establecer una conexión, como por ejemplo PAP (Password Authenticaction Protocol) y CHAP (Challenge-Handshake Authentication Protocol).

El método de encriptación que usa PPTP es el Microsoft Point to Point Encryption, MPPE, y solo es posible su utilización cuando se emplea CHAP (o MS-CHAP en los NT) como medio de autenticación.

MPPE trabaja con claves de encriptación de 40 o 128 bits, la clave de 40 bits es la que cumple con todos los estándares, en cambio la de 128 bits esta diseñada para su uso en Norte América. Cliente y servidor deben emplear la misma codificación, si un servidor requiere de mas seguridad de la que soporta el cliente, entonces el servidor rechaza la conexión.

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

Se trata de un mecanismo del tipo Off-Load donde el usuario realiza un Dial-up para acceso a otro punto de la red mediante el servidor de acceso a la red LAC. Dispone de una tunelización compulsiva (el túnel es creado sin intervención del usuario) utilizando el protocolo PPP. El protocolo L2TP es un standard del IETF que surgió como combinación del PPTP de Microsoft y el L2F (*Layer 2 Forwarding*) de Cisco. En el ámbito de IPSEC el

IETF desarrolla la seguridad (autentificación, privacidad e integridad) para trabajar en forma compatible con L2TP y más robusta que MPPE.

En una llamada entrante el usuario remoto inicia la conexión mediante el protocolo de comunicación PPP hacia el proveedor del servicio ISP usando la red telefónica o ISDN. El LAC del ISP acepta la conexión y lo informa al punto de presencia POP; la conexión PPP queda establecida.

L2TP posee mecanismos de autentificación negociados. Sin embargo, bajo el protocolo PPP no existe autentificación por paquete. El cliente es el responsable por la criptografía; puede utilizarse el mecanismo de PPP criptografiado. L2TP posee información de secuenciamiento que puede ser usada para control de flujo dentro del túnel (paquetes hacia el usuario controlados mediante *windows* en IP). También puede negociarse la compresión de datos en PPP (por ejemplo mediante LSZ).

4.8 Diagramas de conexión.

Hay varias posibilidades de conexiones VPN, esto será definido según los requerimientos de la organización, por eso es aconsejable hacer un buen análisis a fin de obtener datos. Como por ejemplo si lo que se desea enlazar son dos o mas redes, o si sólo se conectarán usuarios remotos.

Las posibilidades son:

4.8.1 De Cliente a Servidor (*Client to Server*).

Un usuario remoto que solo necesita servicios o aplicaciones que corren en el mismo servidor VPN. Ver Figura 4.3.

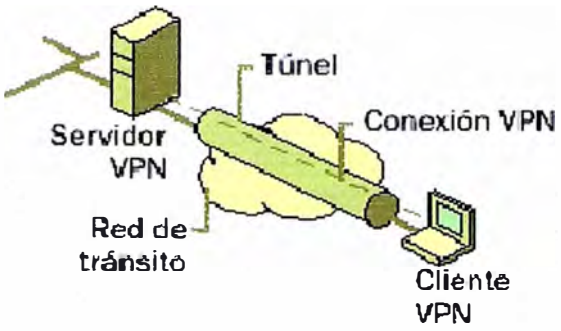
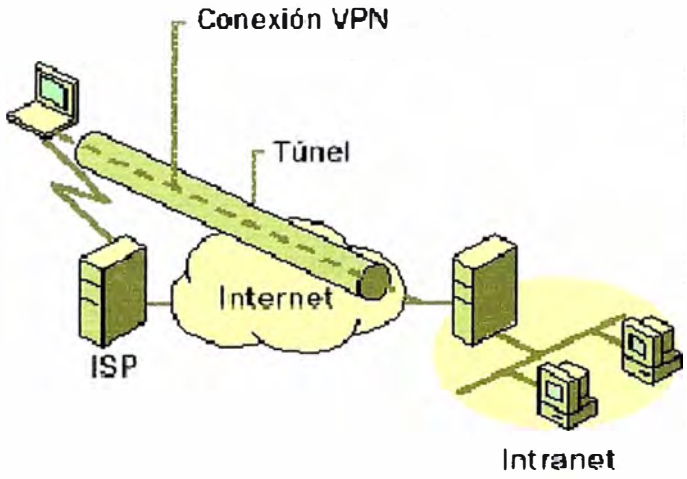


Figura 4.3 Client to Server

4.8.2 De Cliente a Red Interna (*Client to LAN*).

Un usuario remoto que utilizara servicios o aplicaciones que se encuentran en uno o más equipos dentro de la red interna. Ver Figura 4.4.



Figuira 4.4 Client to LAN.

4.8.3 De Red Interna a Red Interna (*LAN to LAN*).

Esta forma supone la posibilidad de unir dos intranets a través de dos enrutadores, el servidor VPN en una de las intranets y el cliente VPN en la otra. Aquí entran en juego el mantenimiento de tablas de ruteo y enmascaramiento. Ver Figura 4.5.

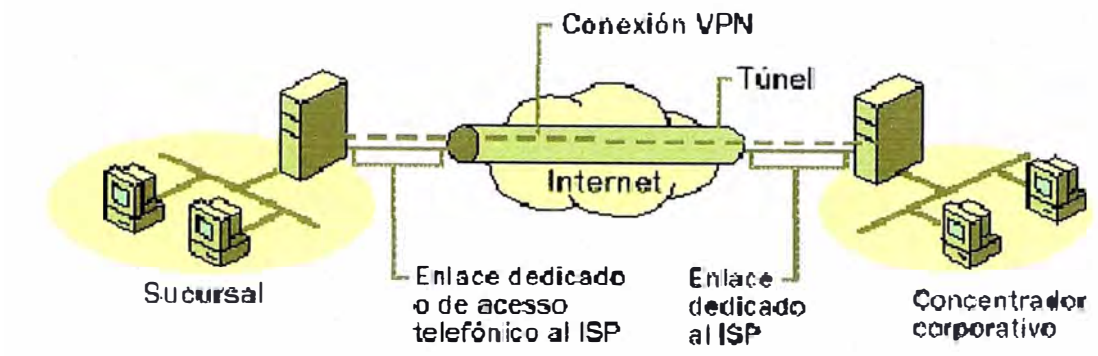


Figura 4.5 LAN to LAN.

4.9 Requerimientos para implementar una VPN.

Para la correcta implementación de una VPN, es necesario cumplir con una serie de elementos y conceptos que a continuación se detallan:

- **Tener una conexión a Internet:** Ya sea por conexión IP dedicada, ADSL o dial-up.
- **Servidor VPN:** Básicamente es una computadora personal conectada a Internet esperando por conexiones de usuarios VPN y si estos cumplen con el proceso de autenticación, el servidor aceptará la conexión y dará acceso a los recursos de la red interna.
- **Cliente VPN:** Este puede ser un usuario remoto o un router de otra LAN, tal como se especifica en la sección 4.8.
- **Asegurarse que la VPN sea capaz de:** Encapsular los datos, autentificar usuarios, encriptar los datos, Asignar direcciones IP de manera estática y/o dinámica.

CAPÍTULO V

ASPECTOS DE SEGURIDAD INFORMÁTICA

5.1 Seguridad Informática.

Consiste en realizar la protección de los recursos de la red, tanto físicos (equipamiento) como la información (sistemas de información y sus datos) y los servicios ofrecidos por la red a los usuarios internos (empleados) y externos (clientes y proveedores).

Tareas principales:

- Valorizar los recursos físicos y de información.
- Identificar riesgos y sus consecuencias para la calidad de servicio de la red y los sistemas de información.
- Implementar las medidas de seguridad adecuadas en cada área.
- Administrar los usuarios (internos y/o externos), sus claves y perfiles de acceso.
- Analizar los logs de auditoría, las violaciones reportadas o alarmas generadas por los IDS (Servicio de Detector de Intrusos).

Objetivos principales:

- Que su información esté protegida de la posible destrucción accidental o intencional (integridad).
- Que su información esté protegida de una visualización no autorizada (privacidad).
- Que las transacciones no sean modificadas en su trayecto desde el aplicativo cliente hasta el servicio y asegurar que quien las generó es quien dice ser o no lo niegue falsamente (integridad, autenticidad y no repudio).
- Que nadie hurte o robe los activos físicos tales como servidores, terminales, memorias, routers (protección de activos).
- Que nadie use los servicios o recursos de la red en forma no autorizada, indiscriminada o para beneficio propio (accounting, control de acceso discrecional).
- Que la red siempre funcione y sus servicios lo hagan con los parámetros de calidad exigidos (confiabilidad, tolerancia a fallos, disaster recovery plan).
- Que se cumpla con las exigencias planteadas por organismos externos de control u otros clientes o partners de negocio. (auditorías).

5.2 Ataques contra Sistemas Informáticos.

Podríamos definir como ataques a todas aquellas acciones que supongan una violación de la seguridad de nuestro sistema (confidencialidad,

integridad o disponibilidad). Dichas acciones las podemos clasificar de modo genérico según los efectos causados en nuestro sistema.

- **Interrupción:** Un recurso del sistema es destruido o se vuelve no disponible. Éste es un ataque contra la disponibilidad. Ejemplos de este tipo de ataque son los Nukes, que causan que los equipos queden fuera de servicio. También la destrucción o sabotaje de un elemento de hardware, como cortar una línea de comunicación.
- **Interceptación:** Una entidad no autorizada consigue acceso a un recurso. Éste es un ataque contra la confidencialidad. Ejemplos de este tipo de ataque consiste en la obtención de datos mediante el empleo de programas Troyanos, la copia ilícita de archivos o programas (interceptación de datos), o bien la lectura de las cabeceras de paquetes de datos para revelar la identidad de uno o más de los usuarios mediante el Spoofing o engaño implicados en la comunicación intervenida (interceptación de identidad).
- **Modificación:** Una entidad no autorizada no sólo consigue acceder a un recurso, si no que es capaz de manipularlo. Virus y troyanos poseen esa capacidad. Éste es un ataque contra la integridad. Un ejemplo de este tipo de ataque consiste en realizar una modificación de cualquier tipo en archivos de datos, alterar un programa para que funcione de forma distinta y modificar el contenido de información que esté siendo transferida por la red.
- **Fabricación:** Una entidad no autorizada inserta objetos falsificados en el sistema. Éste es un tipo de ataque contra la autenticidad. Un

ejemplo de este tipo consiste en la inserción de mensajes falsos en una red o añadir datos a un archivo. Asimismo, estos ataques se pueden clasificar en términos de ataques activos y ataques pasivos.

- **Ataques activos:** Esta modalidad de ataque implica algún tipo de modificación de los datos o la creación de falsos datos: Suplantación de identidad, Modificación de mensajes, Web Spoofing, etc.
- **Ataques pasivos:** En los ataques pasivos el atacante no altera la comunicación, únicamente la escucha o monitorea, para obtener de esta manera la información que está siendo transmitida. .Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos.

5.3 Importancia de políticas y procedimientos de seguridad.

Numerosos incidentes y problemas de seguridad en las organizaciones fueron originados por la falta de políticas y procedimientos escritos o por la existencia de ellos, pero mal escritos Para una organización es esencial contar con una política de seguridad actualizada y de aplicación obligatoria. Las organizaciones involucradas en el comercio electrónico parecerían ser las que están más en la mira de los competidores y de los intrusos. La defensa más segura es una política de seguridad bien desarrollada, y complementada por herramientas de seguridad bien seleccionadas.

Reforzar el mensaje con seminarios que expliquen por qué la seguridad es importante para la salud de la compañía, aún si es algo inconveniente para

los usuarios. Los seminarios son una forma efectiva para educar a los usuarios acerca de los riesgos de responder a pedidos de información de gente externa a la empresa, el método más elemental que los hackers utilizan para obtener la información necesaria para lograr el acceso.

Un ejemplo de implementación de política es hacer leer y firmar la política de seguridad periódicamente, como parte del proceso de revisión de los empleados, esto asegura que el personal debe leer la política de seguridad como mínimo una vez al año.

Recordar que La importancia y cuidado operativo del proceso de respaldo de información, es directamente proporcional a la criticidad estratégica que la misma tiene para el organismo.

5.4 Importancia de la protección física y ambiental.

Los sistemas de protección física y ambientales, incluyendo aquellos que realizan el control de acceso, proporcionan un complemento valioso a los recursos lógicos.

No obstante, ¿de qué nos sirve implementar medidas de seguridad sobre el sistema operativo para evitar el acceso no autorizado o la destrucción intencional, si los servidores y demás recursos físicos están sujetos a un riesgo de destrucción por incendio o robo?.

Es habitual que las organizaciones descuiden los más simples recursos de protección física y ambiental, concentrándose en complejas implementaciones de seguridad, firewalls y VPNs.

Sin embargo, los riesgos en numerosas oportunidades comprometen los activos y servicios cuando un simple extintor o detector de humo hubiese prevenido y evitado el daño.

5.5 Dispositivos y equipos de seguridad.

5.5.1 Router Apantallado (Screening router).

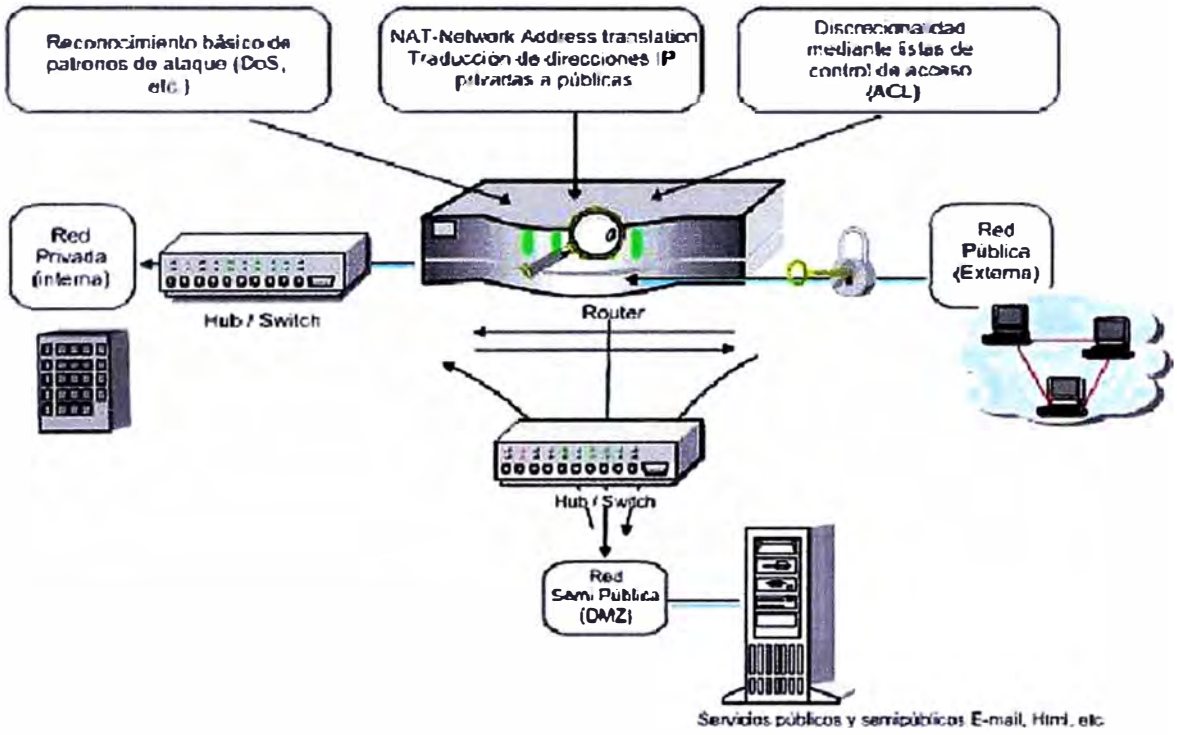


Figura 5.1 Screening router.

Previo al análisis de una implementación con Screening router, se sabe que un router tiene la tarea de redireccionado estándar, en el cual sólo se tiene en cuenta hacia dónde se dirige cada paquete de información, y selecciona cuál es la mejor vía para llegar a su destino. Este tipo de redireccionamiento no tiene en cuenta las políticas de seguridad o si la ruta es potencialmente segura o insegura. Únicamente su objetivo es el de llevar la información a su destino.

El Screening router, en cambio, analiza el paquete de información al detalle y establece si puede ser enviado a su destino en función de las políticas de seguridad del sistema. En el supuesto caso de que fuera el único sistema de protección, y ante su posible falla, la red o el equipo puede verse expuesto a las amenazas del exterior. El Screening router puede dar acceso a un servicio (o denegarlo). Pero, de haberse producido el acceso no autorizado, no puede realizar protecciones individuales dentro del mismo.

Para filtrar paquetes necesitamos un Firewall, que tiene la tarea de filtra o discriminar paquetes de información o de datos que va redirigiendo entre los host internos y externos del sistema, gracias a una selección que realiza siguiendo las políticas de seguridad establecidas. Éste redireccionamiento se conoce con el nombre técnico de "Screening router". La finalidad de esta redirección puede considerar algunos de los siguientes elementos:

- Bloqueo de todas las conexiones externas, salvo aquellas que trabajen bajo SMTP, para permitir la recepción de correo electrónico.
- Bloqueo de todas las conexiones que puedan considerarse potencialmente inseguras.
- Permitiendo el servicio de correo electrónico y de FTP, aunque manteniendo el bloqueo a servicios potencialmente peligrosos como TFTP, RPC, servicios del tipo "r": rlogin (acceso por clave no verificado), etc.

Un Screening Router, puede ser un router comercial o un nodo con capacidad de enrutamiento que posee aptitudes de filtrado de paquetes, teniendo la funcionalidad de bloquear o permitir el tráfico entre redes o nodos basados en direcciones, puertos, protocolos, interfaces, etc.

5.5.2 Firewalls.

El Firewall (cortafuego), constituye una segunda línea dentro de la defensa perimetral de una organización. Ya vimos la primera, que fue el router apantallado o Screening router.

Un Firewall es un equipo que inspecciona el tráfico y realiza un control de acceso a los recursos de la red basado en políticas predefinidas. Las mismas impiden que atacantes o personal no autorizado accedan a recursos o servicios internos de nuestras instalaciones. De estas políticas predefinidas distinguimos dos principios básicos:

- Admitir todo servicio, excepto lo denegado por las reglas.
- Negar todo servicio, excepto lo permitido por las reglas.

De este modo, un Firewall "sí" puede permitir servicios de web, correo y ftp desde una red local hacia Internet, pero "no" permitir el servicio ICQ que puede ser innecesario para nuestro trabajo.

También, podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegar todos, o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que éste sea accesible desde Internet). Dependiendo del Firewall que

tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Políticas de seguridad.

Existen una serie de elementos de seguridad que son similares en todos los Firewalls:

Un criterio de filtro de paquetes, que se establece para los puertos del dispositivo. Esta regla se conoce como "filtro de paquetes".

- Cuando un paquete de información llega al puerto establecido, cada uno de sus encabezados se analiza. Generalmente atañe a los del tipo IP, TCP o UDP.
- Las reglas de filtro de paquetes se guardan en un orden preciso para que cada una de ellas se ejecute en ese mismo orden, en función del tipo de paquete de información que llegue al sistema de red o al equipo.
- En el caso de que una regla (o parte de ella) se vea vulnerada, o no cumpla los requisitos establecidos, el paquete de información podrá recibirse en el sistema, pero, éste avisará mediante alertas de cuáles han sido los protocolos y normas que no cumple.
- Si la política de seguridad lo permite, la transmisión de los datos continúa y se recibe el paquete.
- Si un paquete no cumple ninguna de las reglas, se manda un aviso al sistema, que impide su acceso.

En función de los enunciados mencionados anteriormente, quedaría definida la importancia del mantenimiento adecuado del orden de las

reglas para el Firewall, ya que la aplicación las va leyendo una a una. Un Firewall no es un sistema autónomo que pueda ir de una regla a otra sino que las va procesando según el orden marcado por el administrador del sistema o por el usuario.

Si las reglas se establecieran en un orden equivocado, podría no permitir el acceso de servicios que serían válidos, y permitir el acceso a otros servicios

Beneficios e inconvenientes de tener un Firewall.

Como claros beneficios se pueden citar la seguridad frente a cierto nivel de ataques externos y la oportunidad de permitir acceder a determinados recursos de la red pública sólo a ciertas personas. De esta manera, el administrador sabe a qué elementos se accede y quién lo hace.

Tener uno de estos sistemas implica ciertas restricciones para los usuarios, que no suelen ser aceptadas con agrado. Además, puede constituir un cuello de botella en el acceso a ciertos recursos, debido a que todo el tráfico entre la red privada y la pública debe ser analizado y registrado por si se necesita un análisis posterior de estos datos.

También, hay que tener en cuenta que de fallar ambas redes podrían quedar virtualmente aisladas con todos los inconvenientes que ello pueda acarrear. No obstante, las alternativas son la falta de seguridad o la incapacidad de acceso a las redes públicas, y ninguna de estas posibilidades resulta aceptable.

Si bien son cada vez más necesarios en nuestras redes, "todos los expertos recomiendan que no se usen en lugar de otras herramientas, sino junto a ellas.

Tipos de Firewall.

Conocer la diversidad de los modelos de Firewalls que actualmente existen en el mercado, ayuda a clarificar qué tipo o tipos implementar.

Su clasificación básica es:

- Bastion Hosts.
- Filtros de paquetes (packet filters).
- Proxies (application gateways, application proxies).

a) Bastion Hosts.

Un "Bastion Host" es un servidor segurizado, que hace uso de los recursos internos de seguridad del SO, la auditoría y la autenticación al máximo. Los servicios no autorizados son desestimados, al igual que toda cuenta de usuario excepto la de gestión.

Usualmente, funciona en forma conjunta con el filtro de paquetes instalado en el router que conecta la red (LAN) a Internet.

Consideraciones a tener en cuenta en el momento de instalar un Bastion Host:

- Instalar una versión segura del S.O. desde cero, si el proveedor cuenta con una.

- Remover los servicios o daemons innecesarios. Ej.: FTP, Telnet, uucp, finger, inetd, servicios r-remotos, tales como el rshell, rloggin, rprint, etc. y utilizar el SSH (secure shell).
- Tener en cuenta que en UNIX, los servicios arrancan con el inetd daemon, por archivos de startup en el directorio /etc/rc.* o como parte del kernel.
- Considerar en Windows NT, el applet de Services en el Control Panel.
- Remover toda aplicación, comando, script o batch file, no necesario para la operación o funciones.
- Usar los recursos del S.O. para permitir el acceso controlado a los archivos y directorios.
- Configurar detalladamente la auditoría y logging.

b) Packet Filter.

Son aquellos dispositivos que estando conectados a ambos perímetros (interior y exterior), dejan pasar (a través de ellos mismos) paquetes IP en función de reglas predeterminadas.

Conceptualmente, estos Firewalls trabajan a nivel de red, y son capaces de filtrar tráfico en función de direcciones IP, protocolos, y números de puerto de TCP o UDP, tal como se lo puede apreciar en el Figura 5.2.

Normalmente, esta misión la pueden desempeñar tanto hosts con dos tarjetas de red, como routers. En el caso de Firewalls basados en filtrado de paquetes, los dispositivos de la red interna han de configurarse con la

ruta por defecto apuntando a este dispositivo, que en función de sus reglas, dejará pasar estos paquetes o los rechazará.

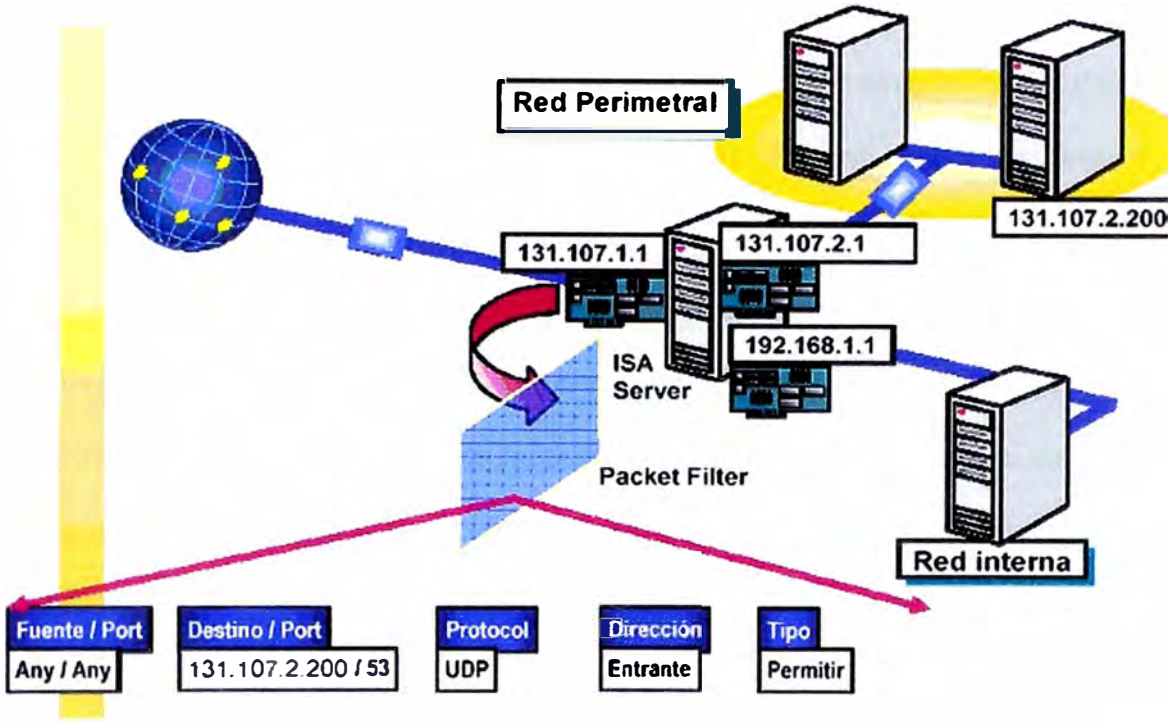


Figura 5.2 Packet Filter.

El principal problema de este tipo de Firewalls es la limitación a la hora de configurar reglas complejas y la falta de flexibilidad en la capacidad de "log" o registro de actividad. Otra limitación fundamental es la imposibilidad de filtrar tráfico en función de información contenida en niveles superiores, tales como URL's, o esquemas de autenticación fuertes.

Cualquier router IP utiliza reglas de filtrado para reducir la carga de la red; por ejemplo, se descartan paquetes cuyo TTL ha llegado a cero, paquetes con un control de errores erróneos, o simplemente tramas de broadcast. Además de estas aplicaciones, el filtrado de paquetes se

puede utilizar para implementar diferentes políticas de seguridad en una red, siendo el objetivo principal de todas ellas evitar el acceso no autorizado entre dos redes, pero manteniendo intactos los accesos autorizados. Su funcionamiento es habitualmente muy simple: se analiza la cabecera de cada paquete, y en función de una serie de reglas establecidas previamente, la trama es bloqueada o se le permite seguir su camino. Estas reglas suelen contemplar campos como el protocolo utilizado (TCP, UDP, ICMP...), las direcciones fuente y destino, y el puerto destino. Además de la información de cabecera de las tramas, algunas implementaciones de filtrado permiten especificar reglas basadas en la interfaz del router por donde se ha de reenviar el paquete y también en la interfaz por donde ha llegado hasta nosotros.

Si se resolviera utilizar un router como filtro de paquetes, es recomendable bloquear todos los servicios que no se utilicen desde el exterior (ejemplo: NIS, NFS, X-Window, TFTP, etc.), así como el acceso desde máquinas no confiables hacia nuestra subred.

c) Proxies.

Además del filtrado de paquetes, es habitual que los Firewalls utilicen aplicaciones (software) para reenviar o bloquear conexiones a servicios como por ejemplo Telnet, HTTP o FTP. A tales aplicaciones se les denomina "servicios proxy", mientras que al sistema donde se ejecutan suele llamarse "gateway de aplicación".

Los servicios proxy poseen una serie de ventajas tendientes a incrementar la seguridad; en primer lugar, permiten la utilización

únicamente de servicios para los que existe un proxy, por lo que si en la organización el "gateway de aplicación" contiene únicamente proxies para telnet, HTTP y FTP, el resto de servicios no estarán disponibles para nadie. Una segunda ventaja es que en el gateway es posible filtrar protocolos basándose en algo más que la cabecera de las tramas, lo que hace posible por ejemplo tener habilitado un servicio como FTP pero con órdenes restringidas (por ejemplo: bloqueando todos los comandos "put" para que nadie pueda subir ficheros a un servidor).

Además, los "gateways de aplicación" permiten un grado de ocultamiento de la estructura de la red protegida (por ejemplo, el gateway es el único sistema cuyo nombre está disponible hacia el exterior), facilita la autenticación y la auditoría del tráfico sospechoso antes de que alcance el host destino y, quizás más importante, simplifica enormemente las reglas de filtrado implementadas en el router; sólo se permitirá el tráfico hacia el gateway, bloqueando el resto.

El principal inconveniente a la hora de instalar un gateway de aplicación es que cada servicio que se quiera soportar necesita su propio proxy; además se trata de un sistema que frecuentemente es más caro que un simple filtro de paquetes.

Una variante de los "gateways de aplicación" la constituyen los gateways de nivel de circuito (Circuit-level Gateways), estos sistemas son capaces de redirigir conexiones (reenviando tramas) pero que no pueden procesar o filtrar paquetes en base al protocolo utilizado; se limitan simplemente a autenticar al usuario (a su conexión) antes de establecer el circuito virtual

entre sistemas. La principal ventaja de este tipo de gateways es que proveen de servicios a un amplio rango de protocolos; no obstante, necesitan software especial que tenga las llamadas al sistema clásicas sustituidas por funciones de librería seguras, como SOCKS.

CONCLUSIONES Y RECOMENDACIONES

1. Este informe hace una descripción general de las Redes Privadas Virtuales y describe los requerimientos básicos de tecnologías útiles de VPN como son: autenticación de usuarios, administración de direcciones, codificación de datos, administración de claves y soporte a protocolos. Analiza cómo los protocolos de capa 2 (PPTP y el L2TP) cumplen estos requerimientos, del mismo modo que lo hace IPSEC en capa 3.
2. Una VPN deberá proporcionar flexibilidad, para satisfacer las necesidades de interoperabilidad entre redes de las empresas. Además otorgará integración rica en aplicaciones y transparencia de infraestructuras para impulsar la economía y la productividad.
3. Una principal razón para usar Frame Relay es obtener una mejor conectividad entre redes de área local por un precio menor. Esta tecnología usa la infraestructura de comunicación existente de modo que típicamente se actualiza el software de los routers y en menor escala el software y hardware de algunos conmutadores de paquetes.
4. MPLS es un estándar de arquitectura multinivel capaz de soportar cualquier tipo de tráfico en Internet, proveer redes fácilmente

escalables, control de la calidad de servicio, ingeniería de tráfico, control de enrutamiento del tráfico y Redes Privadas Virtuales (VPNs).

5. La seguridad en los sistemas y tecnologías de la información ha pasado a ser una de las principales preocupaciones de todas las empresas y compañías. Hoy en día gestionar la seguridad significa prever no sólo agresiones externas, sino también riesgos internos.

BIBLIOGRAFÍA

[1] Merilee Ford, H. Kim Lew, Steve Spanier, Tim Stevenson. "Tecnologías de Interconectividad de Redes". Prentince Hall. 1998.

[2] William Stallings. "Comunicaciones y Redes de Computadoras". Prentice Hall. Sexta Edición, 2000.

[3] José Manuel Huidobro Moya. "Redes y Servicios de Telecomunicaciones". Paraninfo. Tercera Edición, 2001.

[4] Mischa Schwartz. "Redes de Telecomunicaciones - Protocolos, modelado y análisis". Addison-Wesley Iberoamericana. 1994.

[5] Michael J. Palmer. "Redes Informáticas - Guía Práctica". Paraninfo. 1998.

[6] Fred Halsall. "Comunicación de Datos, Redes de Computadores y Sistemas Abiertos". Pearson Educación. Cuarta Edición, 1998.

[7] INICTEL. "Aplicaciones de MPLS". Agosto 2003.

[8] "Multiprotocolo Label Switching (MPLS)". Trillium. The International Engineering Consortium. http://www.iec.org/tutoriales/.

[9] Lina María Martínez Restrepo, Catalina Andrea Ramos Rueda. "VPN – Virtual Private Network". Octubre 2000.

[10] Servisoft. "Virtual Private Networks". http://www.servisoft.es.

[11] Daniel Kofman. "Multiprotocol Label Switching – Traffic Engineering". Instituto de Ingeniería Eléctrica, Universidad de la República. 2003.

[12] Hugo Zamora. "Implementación de Redes MPLS-VPN. Casos de Estudios". TELMEX. 2002.

[13] Lucent Technologies. "Frame Relay". Universidad de Ciencias Aplicadas – UPC. Julio 2002.

[14] Álvaro Pachón. "Frame Relay". ORBITEL. Febrero 2001.

[15] César Cicerchía. "Seguridad Informática en entornos conectados a Internet". Agosto 2003.

[16] John Wack, Ken Cutler, Jamie Pole. " Guide to Firewall. Selection and Policy Recommendations". National Institute of Standars and Technology – NIST. Octubre 2001-