ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO EN INGENIERÍA

"DISEÑO DE REDES PRIVADAS VIRTUALES (VPN) BASADAS EN LA TECNOLOGÍA MPLS (MULTI-PROTOCOL LABEL SWITCHING)"

WINSTON JAVIER CASTILLO CEVALLOS

SANGOLQUÍ - ECUADOR

2006

CERTIFICACIÓN

Certificamos que el presente proyecto titulado: “Diseño de Redes Privadas Virtuales (VPN) basadas en la tecnología MPLS (Multi-Protocol Label Switching)” ha sido desarrollado en su totalidad, por el Sr. Winston Javier Castillo Cevallos bajo nuestra dirección.

_____	_____
Ing. Fabián Sáenz DIRECTOR	Ing. Carlos Romero CO-DIRECTOR

AGRADECIMIENTO

Si realizo un análisis cronológico de cómo nació este y de todas las personas que contribuyeron de alguna u otra forma a la culminación del mismo, debo empezar agradeciendo al Ing. Fabián Sáenz, quien fue la persona que me sugirió el presente tema, y además ha estado a mi lado desde un inicio y quién ha sido un apoyo incondicional, que aparte de ser excelente catedrático, es un excelente ser humano que no solo es mi director de tesis sino es un gran amigo, al Ing. Carlos Romero, mi co-director de tesis, el amigo que supo extenderme la mano en el momento oportuno y al Ing. Raúl Naranjo, por su ayuda constante en la resolución de problemas presentados en el desarrollo del proyecto.

A mis Padres que me proporcionaron su apoyo total y firmeza constante permitiendo culminar con éxito el presente proyecto.

A mis Tíos José y Yoice, a mis primos José, Yoice, David y Freddy, que durante todo este tiempo se han convertido en mi segunda familia, sin la cual estoy seguro nada se hubiera hecho.

A mis amigos y compañeros con quienes compartí muchas vivencias y experiencias diarias. A todas las personas que compartieron conmigo y supieron animarme en los momentos más difíciles.

DEDICATORIA

A mi Dios, que aunque yo le he dejado de lado muchas veces, el no me ha dejado de lado nunca y me tiene aquí concluyendo esta etapa tan importante en mi vida.

A Winston, mi Padre, de cuyas manos nacen las notas que alegran mi vida, que es la melodía de amor que siempre ha acompañado mis días, gracias a su enorme entrega pude realizar y culminar mis estudios, que es mi ejemplo a seguir en responsabilidad, pasión por el trabajo y sobre todo un ejemplo de amor hacia su familia.

A Patricia, mi Madre, que ha sido, es y será mi guía, el farolito que ha alumbrado siempre el barco de mi existencia, con su lenguaje de amor me ha exigido culminar cada nuevo proyecto y que ha sabido ser la brújula que guía mis días.

A Vanessa, Carlos y Luís, mis Hermanos, que siempre tuvieron una palabra de aliento para su hermano, espero compensar un poco con este trabajo toda la confianza que siempre me han brindado.

A María de los Angeles y Jackson, que son parte de mi familia, a ustedes hermanos también va dedicado este proyecto.

A mis abuelitos, mis tíos, mis primos, mis amigos, en fin a todas las personas que han confiado en mí.

PRÓLOGO

Vivimos en una era de continuos cambios, donde lo que ayer era sofisticado y una tecnología puntera, mañana será una reliquia del pasado. Año tras año se desarrollan nuevas tecnologías, un sin fin de aplicaciones nuevas, ideas, proyectos, etc.

Esto se cumple inevitablemente en el variado pero complejo mundo de las telecomunicaciones, donde el auge que ha tenido la Internet y con el significado que esta ha adquirido como el principal medio mundial de comunicación, las Redes Privadas Virtuales (VPN) han hecho su aparición y han ganado un espacio dentro del tan cambiante mundo de las redes de información.

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

Uno de los puntos clave al optarse por una VPN es la seguridad, ya que es condición necesaria que los datos que transitan por una red compartida o pública queden restringidos a terceros, siendo la encriptación y autenticación dos mecanismos vitales para garantizar la privacidad e integridad de la información.

En la actualidad, Multi-Protocol Label Switching (MPLS) constituye un escalón fundamental para una mejor escalabilidad y eficiencia, además es el último paso en la evolución de las tecnologías de conmutación multinivel, siendo considerado indispensable para los nuevos crecimientos de la Internet del siglo XXI. Así mismo, permite combinar velocidad, desempeño e inteligencia de las redes de conmutación por paquetes para proveer la mejor solución para integrar voz, video y datos.

Por otro lado, abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP, logrando de esta manera hacer ingeniería de tráfico, manteniendo clases de servicio, y sobretodo soportando con gran eficacia la creación de VPN.

Por todo ello y gracias a sus cualidades, MPLS aparece como la gran promesa y esperanza para poder mantener el ritmo actual de crecimiento de la Internet, llevando a las VPN a un nivel evolutivo, en donde las empresas que requieren unir puntos dispersos u oficinas remotas pueden acceder a una mayor calidad y variedad de servicios.

ÍNDICE

CAPÍTULO I: INTRODUCCIÓN

CAPÍTULO II: REDES PRIVADAS VIRTUALES (VPN)

CAPÍTULO III: MULTI-PROTOCOL LABEL SWITCHING (MPLS)

CAPÍTULO IV: DISEÑO DE REDES PRIVADAS VIRTUALES UTILIZANDO TECNOLOGÍA MPLS.

CAPÍTULO V: ANALISIS COMPARATIVO DE LAS VPN'S CON LA TECNOLOGÍA MPLS

CAPÍTULO VI: LAS AMENAZAS A MPLS VPN

ÍNDICE DE TABLAS

CAPÍTULO I

CAPÍTULO IV

CAPÍTULO V

ÍNDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

CAPÍTULO VI

GLOSARIO

AAA (Authentication, Authorization, and Accounting). Son los tres pasos fundamentales en la seguridad de datos en informática: Autenticación, Autorización y Auditoria.

ADSL (Asymmetric Digital Subscriber Line). Método de transmisión de datos a través de la línea telefónica de cobre tradicional a velocidad alta. Los datos pueden ser descargados a distinta velocidad que son cargados, esta es la razón por la cual se le denomina asimétrico.

AH (Authentication Header). Proporciona servicios de autenticación, aunque no de cifrado. Su función es asegurar la compatibilidad con homólogos IPSec que no admiten ESP, que suministra tanto autenticación como cifrado.

AS (Autonomous System). Conjunto de redes sobre la cual existe una autoridad administrativa.

ATM (Asynchronous Transfer Mode). Es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

BGP (Border Gateway Protocol). Es un protocolo mediante el cual se intercambian prefijos los ISPs registrados en Internet, en la actualidad la mayoría de los ISPs intercambian sus tablas de rutas con este protocolo.

CE (Customer Edge). Router frontera del cliente que solicita el servicio VPN con MPLS.

CEF (Cisco Express Forwarding). Es una técnica propietaria de Cisco para realizar switcheo a altas velocidades en WANs con garantía de velocidad y sin retraso.

CHAP (Challenge Handshake Authentication Protocol). Es un método de autenticación remota o inalámbrica. Diversos proveedores de servidores y clientes de acceso a la red emplean CHAP.

CIDR (Classless Inter-Domain Routing)**.** Método de asignar y especificar direcciones Internet utilizados en enrutadores interdominios con mayor flexibilidad que el sistema original de clases de direcciones del protocolo Internet. Como resultado se ha ampliado en gran medida el número de direcciones Internet disponibles.

CPE (Customer Premise Equipment). Es el conjunto de equipos instalado en los predios de los clientes y que permiten su conexión con las estaciones base de la red.

CR-LDP (Constraint-Based Routing Label Distribution Protocol). Protocolo de distribución de etiquetas que contiene extensiones del LDP para extender sus capacidades. Puede trabajar con explicit route constraints, QoS constraints, entre otras.

CsC (Carrier's Carrier). Servicio backbone a proveedores de servicio.

DD (Database Description). Descripción de base de datos.

DiffServ (Differentiated Services). Se utiliza para establecer diferentes tipos de servicio a diferentes usuarios.

DoS (Denial of Service). Es un incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar. Habitualmente, la pérdida del servicio supone la indisponibilidad de un determinado servicio de red, como el correo electrónico, o la pérdida temporal de toda la conectividad y todos los servicios de red

DSL (Digital Subscriber Line). Tecnología de transmisión que permite que los hilos telefónicos de cobre convencionales transporten hasta 16 Mbps (megabits por segundo) mediante técnicas de compresión.

ECN (Explicit Congestion Notification). Regula dinámicamente las sesiones de tiempo real admitidas en una red y trata por tanto de reestablecerlas en el caso de que sea necesaria.

ESP (Encapsulating Security Payload). Es un encabezado de red diseñado para proveer los servicios de seguridad de IPv4.

FEC (Forwarding Equivalence Classes). Nombre que se le da al tráfico que se reenvía bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

FTP (File Transfer Protocol). Protocolo de transferencia de archivos que permite transmitir ficheros sobre Internet entre una máquina local y otra remota.

GRE (Generic Routing Encapsulation). Protocolo de conexión virtual mediante túneles.

HTPP (Hypertext Transfer Protocol). Protocolo base de la Web.y que ofrece un conjunto de instrucciones para que los servidores y navegadores funcionen. Es el lenguaje usado para escribir documentos para servidores World Wide Web.

ICMP (Internet Control Message Protocol). Es usado principalmente por los sistemas operativos de las computadoras en una red para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o un host no puede ser localizado.

IETF (Internet Engineering Task Force). Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la Ingeniería de Internet. Se divide en áreas como: transporte, encaminamiento, seguridad, etc.

IGP (Internet Gateway Protocol). Hace referencia a los protocolos usados dentro de un sistema autónomo. Los protocolos IGP más utilizados son RIP y OSPF.

IKE (Internet Key Exchange). Se utiliza para establecer una SA en el protocolo IPSec.

IntServ (Integrated Services). Modelo de servicios diferenciados, realiza una reserva previa de recursos antes de establecer la comunicación

IP (Internet Protocol). Base del conjunto de protocolos que forman Internet y que permite que los paquetes de información sean direccionados y enrutados.

IPSec (IP Security). Es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autentificación y cifrado, y de esta manera asegurar las comunicaciones a través de dicho protocolo.

ISP (Internet Service Provider). Organización que provee la conexión de ordenadores a Internet, ya sea por líneas dedicadas o por líneas conmutadas.

L2TP (Layer 2 Tunneling Protocol). Fue diseñado por el IETF para corregir las diferencias de PPTP y establecerse como un estándar aprobado por el IETF.

L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado.

LAC (L2TP Access Control). Dispositivo que termina las llamadas a sistemas remotos y sesiones de túnel PPP entre sistemas remotos y LNS.

LAN (Local Area Network). Red de datos para dar servicio a un área geográfica máxima de unos pocos kilómetros cuadrados, por lo cual pueden optimizarse los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps.

LCP (Link Control Protocol). Protocolo de Control de Enlace.

LDP (Label Distribution Protocol). Protocolo de distribución de etiquetas, utilizado principalmente en MPLS.

LER (Label Edge Router). Elemento que inicia o termina el túnel (pone y quita encabezados), es decir el elemento de entrada/salida a la red MPLS. Un router de entrada se conoce como Ingress Router y uno de salida como Egress Router.

LFT (Label Forwarding Table). Tabla de Reenvío de Etiquetas, la cual usa el componente de datos para reenviar los paquetes etiquetados a través de la red MPLS.

LNS (L2TP Network Server). Dispositivo que puede terminar túneles L2TP desde un LAC y sesiones PPP a sistemas remotos mediante sesiones de datos L2TP.

LSA (Link State Advertisiment). Paquetes OSPF que contienen información del estado, métrica y otros de las interfaces del router.

LSP (Label Switched Path). Nombre genérico de un camino MPLS (para cierto FEC), es decir, del túnel MPLS establecido en los extremos.

LSR (Label Switch Router). Elemento que conmuta etiquetas.

MAC (Media Access Control). Número exclusivo asignado por el fabricante a cada computadora u otro dispositivo de una red.

MPLS (Multi-Protocol Label Switching). Es un mecanismo de transporte de datos estándar creado por la IETF. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y basadas en paquetes

NAT (Network Address Translation). Estándar creado por la IETF el cual utiliza una o más direcciones IP para conectar varios computadores a otra red, por lo general Internet.

NCP (Network Control Protocol). Protocolo de Control de Red. Es un protocolo del Network Layer.

NetBEUI (NetBios Extended User Interface). Es un protocolo de nivel de red sencillo utilizado en las primeras redes Microsoft. La comunicación entre equipos se consigue gracias al intercambio de sus nombres en una red de área local, es un protocolo sin encaminamiento por lo que no dispone de mecanismos para conectar equipos que estén en redes separadas.

NOC (Network Operations Center). Representa al centro de operaciones en el cual se realiza el monitoreo y resolución de fallas en una red de servicios.

NSP (Network Service Provider). Proveedores de servicio IP/Internet.

OSI (Open System Interconnection). Modelo definido por la Organización Internacional de Normalización, es uno de los más importantes y el más utilizado. Se divide en 7 capas sucesivas: Física, Enlace de Datos, Red, Transporte, Sesión, Presentación y Aplicación.

OSPF (Open Shortest Path First). Propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red con información sobre sistemas locales y vecinos, esto con el fin de conocer la ruta más corta.

PAP (Password Authentication Protocol). Método básico de autenticación, en el cual el nombre de usuario y la contraseña (clave) se transmiten a través de una red y se compara con una tabla de parejas nombre-clave, la no coincidencia provocará la desconexión. Típicamente, las contraseñas almacenadas en la tabla se encuentran encriptadas.

PDU (Protocol Data Unit). Es la unidad de datos de protocolo de la capa de red. Las PDU tienen encapsuladas en su área de datos otras PDU.

PE (Provider Edge). Router frontera del proveedor del servicio VPN con MPLS.

PoP (Point Of Presence). Punto geográfico, especialmente una ciudad, desde donde un Proveedor de Servicios Internet ofrece acceso a la red Internet.

PPP (Point to Point Protocol). El protocolo PPP permite establecer una comunicación a nivel de enlace entre dos computadoras. Generalmente se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un modem telefónico.

PPTP (Point-to-Point Tunneling Protocol). Es un protocolo para implementar redes privadas virtuales desarrollado por Microsoft, Ascend Communications,

3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum. Actualmente PPTP ya no se utiliza.

PVC (Permanent Virtual Circuit). Conexión que reemplaza las líneas privadas por un solo enlace en la red.

QoS (Quality Of Service). Es la capacidad de las tecnologías de conmutación de paquetes de proveer todos los recursos necesarios a cada aplicación en un momento determinado dentro de la red.

RAS (Remote Access Server). Servidor dedicado a la gestión de usuarios que no están en una red pero necesitan acceder remotamente a ésta. Permite a los usuarios, una vez autenticados, obtener acceso a los archivos y servicios de impresora de una LAN desde una localización remota.

RD (Route Distinguisher). Es un clasificador de direcciones utilizado por MPLS para distinguir rutas VPN de diferentes clientes que se conectan al proveedor de servicio.

RDSI (Integrated Services Data Network). Una red que procede de la Red Digital Integrada (RDI) y que facilita las conexiones digitales extremo a extremo con el fin de proporcionar una amplia gama de servicios, tanto de voz como de otros tipos.

RFC (Request for Comments). Conjunto de notas técnicas y organizativas donde se describen los estándares de Internet.

RSVP (Resource Reservation Protocol). Protocolo que se encarga de reservar recursos para que estén disponibles cuando las aplicaciones lo necesiten.

RT (Route Target). Identifica las VFR en que se instalan las rutas. Permite el control y manejo de prefijos VPNv4.

SA (Security Associations). Describe un flujo unidireccional seguro de datos a través de dos puertas de enlace. Se utiliza en IPSec con IKE.

SAD (Security Association Database). Base de datos donde se almacena todos los parámetros concernientes a las SAs, cada una de ellas tiene una entrada donde se especifican todos los parámetros necesarios para que IPSec realice el procesamiento de paquetes IP.

SMTP (Simple Mail Transfer Protocol). Protocolo de envío de correo electrónico.

SP (Service Provider). Proveedor de servicio. Empresa que proporciona el servicio de acceso a la red.

SPD (Security Policy Database). Base de datos donde existe una lista ordenada de políticas de seguridad a ser aplicadas a los paquetes IP. Dichas políticas son en general reglas que especifican como los paquetes IP deben ser procesados.

SSL (Secure Sockets Layer). Es un protocolo criptográfico que proporciona comunicaciones seguras en Internet. Proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.

SVC (Switched Virtual Circuit). Conexión virtual entre dos extremos variables de la red. El conmutador establece la conexión al comienzo de la llamada y la interrumpe al finalizar esta.

TCP (Transmission Control Protocol). Protocolo en los que se basa buena parte de Internet. Se encarga de dividir la información en paquetes en origen, para luego recomponerla en destino.

TFTP (Trivial File Transfer Protocol). Se trata de un sencillo protocolo utilizado para transferir archivos. Se ejecuta en UDP.

ToS (Type of Service). Campo dentro de un datagrama IP que indica el modo en que se debe manejar el datagrama

UDP (User Datagram Protocol). Es un protocolo que opera en el nível de transporte del modelo OSI que se basa en intercambio de datagramas. Permite enviar los datagramas sin establecer previamente una conexión ya que su encabezado contiene suficiente información de direccionamiento.

VC (Virtual Circuit). Conexiones virtuales que utiliza ATM para reemplazar las líneas privadas por un solo enlace de red, puede ser permanentes o conmutadas.

VLL (Virtual Leased Lines). Enlaces punto a punto orientados a conexión entre los sitios de los clientes.

VPDN (Virtual Private Dial Network). Enlaces que permiten a los clientes que el SP le aprovisione y gestione los accesos conmutados a su red.

VPLS (Virtual Private LAN Segments). Es una forma de proveer comunicación multipunto a multipunto basado en Ethernet para redes IP/MPLS.

VPN (Virtual Private Network). Red en la que al menos alguno de sus componentes utiliza la red Internet pero que funciona como una red privada, empleando para ello técnicas de cifrado

VPRN (Virtual Private Routed Network). Simulan redes dedicadas de enrutadores IP entre los sitios de los clientes, aunque transporte tráfico IP, esta debe ser tratada como un dominio de enrutamiento separado.

VRF (VPN Routing and Forwarding). Es una tecnología utilizada en redes de computadoras que permite la coexistencia de múltiples instancias las tablas de

ruteo de un mismo router. Esta tecnología es utilizada comúnmente en MPLS VPNs de capa 3.

WAN (Wide Area Network). Es una red muy extensa que abarca computadoras separadas físicamente. Opera en la capa física y de enlace del modelo de referencia.

CAPÍTULO I

INTRODUCCIÓN

1.1 TCP/IP

En este capítulo comenzaremos con una introducción a TCP/IP y describiendo sus propiedades básicas, tales como la formación de redes, el sistema de direccionamiento, el formato utilizado en sus cabeceras, la distribución de protocolos por capas y el encaminamiento.

1.1.1 Modelo Arquitectónico

TCP/IP es un conjunto de protocolos utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con hardware y software incompatibles, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas de TCP/IP, pues este conjunto de protocolos se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware [1].

TCP/IP no es un único protocolo, sino que en realidad se lo conoce así por dos de sus protocolos más importantes que cubren los distintos niveles del modelo OSI (Open System Interconnection). Los protocolos son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto.

1.1.2 Modelo TCP/IP

La arquitectura TCP/IP consta de cuatro niveles o capas (ver figura 1.1) en las que se agrupan los protocolos y que se relacionan con los niveles OSI [1].

Este sistema permite una independencia entre las diferentes capas y obliga a que la conexión entre dos ordenadores se realice mediante una comunicación entre las capas del mismo nivel de los dos ordenadores [2].

En este esquema, la capa superior accede únicamente a los servicios prestados por la capa situada justo en el nivel inferior a ella. De esta forma, independizamos una capa del resto de capas inferiores, lo que nos permite tener un esquema modular.

Nivel TCP/IP		Nivel OSI
4	Aplicación	7,6,5
3	Transporte	4
2	Red	3
1	Enlace y físico	1,2

Figura 1.1: Modelo TCP/IP

1.1.2.1 Capa de aplicación

Los diseñadores del TCP/IP sintieron que los protocolos de nivel superior deberían incluir los detalles de las capas de sesión y presentación. Simplemente crearon una capa de aplicación que maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y da por sentado que estos datos están correctamente empaquetados para la siguiente capa [3]. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol) y otros como el protocolo HTTP (Hypertext Transfer Protocol) [1].

1.1.2.2 Capa de transporte

Es la encargada de proporcionar un flujo de datos entre dos procesos/aplicaciones, este flujo de datos puede ser fiable o no fiable. Los protocolos de este nivel son TCP y UDP (User Datagram Protocol) [2].

1.1.2.3 Capa de red

El propósito de la capa de Internet es enviar mensajes desde un origen de cualquier red y que estos mensajes lleguen a su destino independientemente de la ruta y de las redes que se utilizaron para llegar hasta allí. El protocolo específico que rige esta capa se denomina IP. En esta capa se produce la determinación de la mejor ruta [3].

1.1.2.4 Capa de enlace y físico

También denominada capa de datos, incluye los mecanismos que permite al sistema operativo enviar y recibir información a través de la red a la que se encuentra físicamente conectado [2].

Esta capa incluye los detalles de las capas física y de enlace de datos del modelo OSI.

1.1.3 Redes IP

Definiremos las redes IP como aquellas redes que utilizan los protocolos TCP/IP para su funcionamiento. Internet es una red IP [2].

Las familias de protocolos TCP/IP permiten la comunicación entre diferentes tipos de ordenadores con independencia del fabricante, red a la que se encuentren conectados y sistema operativo utilizado.

Las redes IP se caracterizan por haber sido construidas siguiendo un esquema de capas (layers). Cada capa es la responsable de cada una de las diferentes facetas de la comunicación.

1.1.3.1 El Protocolo IP

El protocolo IP es la pieza fundamental en la que se sustenta el sistema TCP/IP y por tanto todo el funcionamiento de Internet. La unidad de datos del protocolo IP es el datagrama, cuyo tamaño máximo es de 65535 bytes (64K) [2].

El protocolo IP facilita un sistema sin conexión (connectionless) y no fiable (unreliable) de entrega de datagramas entre dos ordenadores cualesquiera conectados a Internet. Sus características básicas son [3]:

- IP no está orientado a conexión. Esto significa que los mensajes IP pueden llegar desordenados e incluso pueden llegar duplicados si la red es mallada, porque el camino que siguen para ir del dispositivo origen al de destino puede variar en función del estado de la red. Una de las razones por las que este protocolo IP es no orientado a conexión es porque así se minimiza la dependencia de otras redes que utilizan redes jerárquicas orientadas a conexión.
- El protocolo IP no mantiene ningún tipo de estado de información entre sucesivos datagramas. Cada datagrama IP es tratado independientemente respecto a otros datagramas.
- Los datagramas IP pueden ser entregados sin un orden determinado.
- Debido al propio funcionamiento del protocolo IP, se pueden producir situaciones de pérdida de mensajes, duplicado de los mismos, la llegada al destino fuera de secuencia, o con errores. En todos estos casos es el protocolo de nivel superior (TCP) quien se encarga del tratamiento de la pérdida o duplicación de la información.

El protocolo IP es totalmente independiente de la tecnología de red, debajo puede haber cualquier nivel de enlace.

IP da un servicio de entrega basado en el mejor intento (best - effort). Esto implica que cuando hay algún funcionamiento anómalo de Internet, como podría ser un router colapsado, se contempla un sistema muy simple de tratamiento de errores [2].

Este mecanismo de control de errores viene regulado por el protocolo ICMP (Internet Control Message Protocol).

La estructura de un datagrama IP (ver figura 1.2) está dividida en bloques de 32 bits (4 bytes). El datagrama IP se transmite enviando primero el bit 0, luego el bit 1, 2, 3... y así sucesivamente hasta finalizar el datagrama.

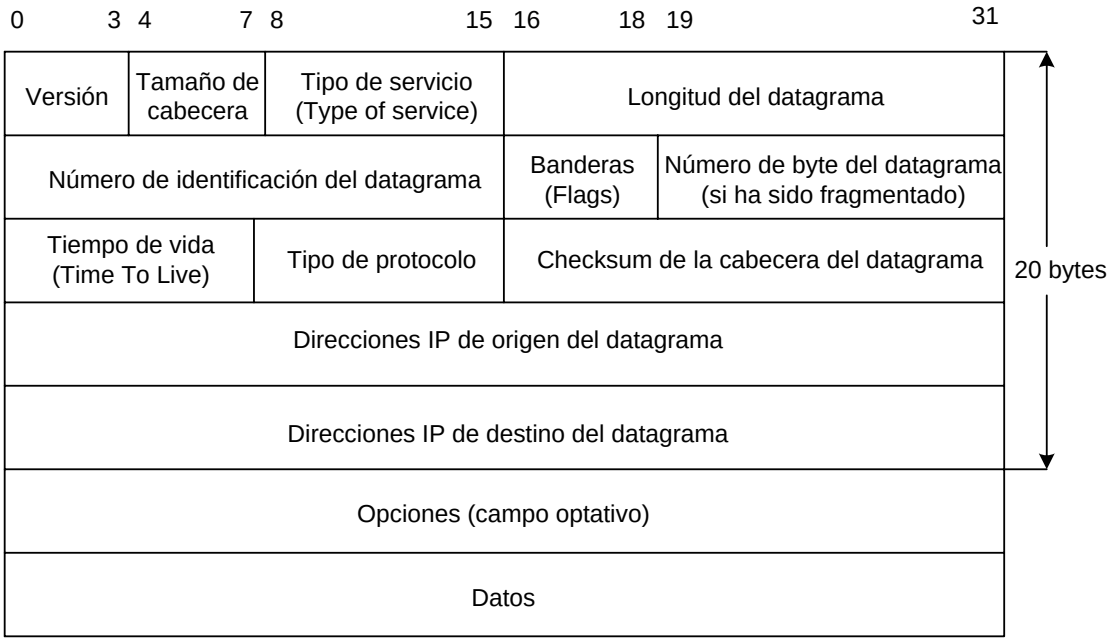

Figura 1.2: Estructura de un Datagrama IPv4

La versión (4 bits), sirve para identificar a que versión hace referencia el formato del datagrama. Esta información sólo es utilizada por los routers y capa IP de origen y final del datagrama. Esto permite la coexistencia de diferentes versiones del protocolo IP de una forma transparente al usuario. La versión actual es la 4 (conocida también cómo IPv4).

El tamaño de la cabecera (Header Length), son 4 bits que indican el número de palabras de 32 bits que ocupa la cabecera. Estos 4 bits de tamaño máximo nos limitan a un tamaño de cabecera máximo de 60 bytes.

El campo del tipo de servicio (Type Of Service), ahora DiffServ (Differentiated Services) y ECN (Explicit Congestion Notification), se compone de 8 bits. Los primeros 6 bits ocupan el campo DiffServ que determinan un codepoint

que sirve para especificar el grado de servicio deseado. El valor del codepoint para los paquetes de tiempo real deberá ser escogido, mientras que el valor recomendado para los paquetes best-effort es la secuencia de bits ‘000000’. El mecanismo de notificación de congestión explicita ECN, regula dinámicamente las sesiones de tiempo real admitidas y trata por tanto de reestablecerlas en el caso de que sea necesaria. Concretamente se marcan los bits ECN-Capable Transport y Congestion Experienced, que son los dos últimos bits del campo ToS.

La longitud del datagrama (Total Length), es un número de 16 bits que indica la longitud total del datagrama. Este valor es muy importante, ya que nos permite saber que tamaño de memoria debemos reservar para la recepción del datagrama. Además, nos indica el número de bytes a leer, lo que nos permite un simple control de error. De esta forma, si el valor es incorrecto, el número de bytes leídos será como máximo de 65535, acotando el error. Además nos limita el número de bytes a enviar en un datagrama.

El número de identificación del datagrama (Identification Field), es un número de 16 bits que en caso de fragmentación de un mensaje nos indica su posición en el datagrama original. Esto nos permite recomponer el datagrama original en la máquina de destino. Este valor nos indica que un datagrama puede ser fragmentado en máximo de 65535 fragmentos.

Las banderas (Flags) son 3 bits. El primero permiten señalar si el datagrama recibido es un fragmento de un datagrama mayor, bit M (More) activado. El segundo especifica si el datagrama no debe fragmentarse, bit DF (Don’t fragment) activado y el tercero no se utiliza actualmente, asignándole el valor 0.

El número de byte en el datagrama (Fragmentation Offset), nos indica la posición en bytes que ocupan los datos en el datagrama original. Sólo tiene sentido si el datagrama forma parte de uno mayor que ha sido fragmentado. Este campo tiene un máximo de 13 bits. De esta forma, siempre podemos reconstruir el datagrama original con los fragmentos.

El tiempo de vida (Time To Live), es un campo de 8 bits que indica el tiempo máximo que el datagrama será válido y podrá ser transmitido por la red. Esto permite un mecanismo de control para evitar datagramas que circulen eternamente por la red (por ejemplo en casos de bucles). Este campo se inicializa en el ordenador de origen a un valor y se va decrementando en una unidad cada vez que atraviesa un router. De esta forma si se produce un bucle o no alcanza su destino en un máximo de 255 saltos, es descartado. En este caso se envía un datagrama ICMP de error al ordenador de origen para avisar su pérdida.

El tipo de protocolo (Protocol), es un valor que indica a que protocolo de nivel superior pertenece el datagrama (TCP, UDP, ICMP). Es necesario debido a que todos los servicios de Internet utilizan IP como transporte, lo cual hace necesario un mecanismo de discriminación entre los diferentes protocolos.

El checksum de la cabecera del datagrama (Header Checksum), es una suma de comprobación que afecta sólo a la cabecera del datagrama IP. Su función es simplemente la de un mecanismo de control de errores. De esta forma, si se encuentra un error en el checksum de un datagrama IP, este es simplemente descartado y no se genera ningún mensaje de error.

La dirección IP de origen como la de destino (IP address), están formadas por dos números de 32 bits.

1.1.3.2 Direccionamiento en IP

Las direcciones IP identifican a la red y al sistema (equipo) dentro de la red. Las direcciones IPv4 tienen 4 octetos, y están divididas en dos partes: identificador de red, e identificador de equipo dentro de dicha red. Todos los equipos conectados a una misma red comparten el mismo identificador de red [4].

El protocolo IPv4 utiliza un modelo de direccionamiento, de forma que a cada interface de cada dispositivo se le asigna una dirección independientemente de su dirección MAC (Media Access Control), que es la que utilizan los protocolos

de nivel de enlace. La dirección IP destino es un dato que debe ser suministrado por las aplicaciones que corren en el propio dispositivo al protocolo IP. La dirección IP origen la obtiene de los datos de configuración de la interfaz [3].

Estas direcciones IP constan de 32 bits y para su representación se emplea la notación decimal de puntos. Ésta consiste en 4 números decimales separados por un punto, por ejemplo 194.110.100.220

El valor más a la derecha sólo puede oscilar entre 1 y 254 porque el 255 está reservado a la dirección de broadcast y el 0 es indicativo de toda la red. Todos los dispositivos tienen como dirección local propia 127.0.0.1 que se identifica como localhost.

En Internet, para acomodar la estructura de direccionamiento a las diferentes necesidades de utilización, el ámbito de direcciones IP se ha agrupado en clases (ver figura 1.3) de forma la simple inspección de una dirección IP permite conocer a que clase pertenece.

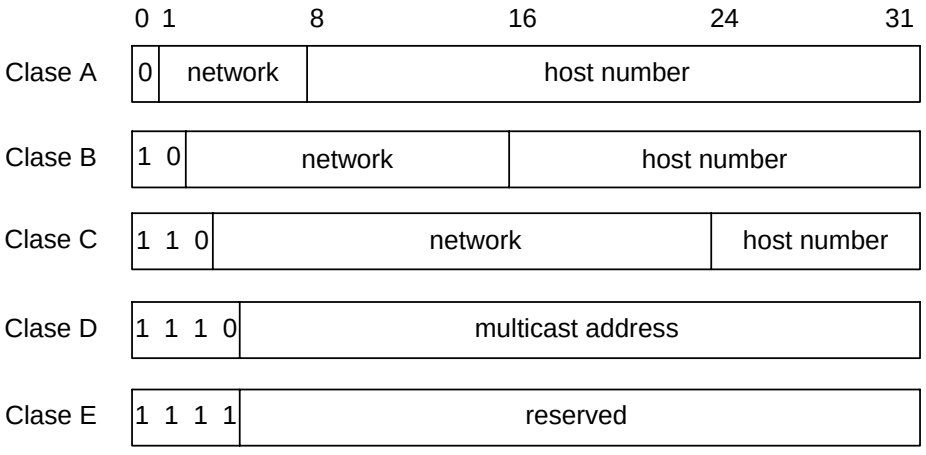

Figura 1.3: Clases asignadas de dirección de Internet

En función del valor que tome el primer número de la dirección, podemos distinguir cinco tipos o clases de direcciones [4]:

- Clase A: Son aquellas que tienen un 0 en el bit más significativo del primer octeto (números menos de 127 en decimal). En estas direcciones, el primer octeto es el Identificador de red, y los tres siguientes identifican al equipo.
- Clase B: Son aquellas cuyos dos primeros bits más significativos son: 10 (primer número entre 128 y 191). En ellas, los dos primeros octetos son el identificador de red, los dos siguientes el del equipo.
- Clase C: Los tres bits más significativos del primer octeto son: 110 (primer número entre 192 y 223). En ellas, los tres primeros octetos identifican a la red, y el último al equipo.
- Clase D: Los cuatro bits más significativos del primer octeto son: 1110 (primer número entre 224 y 239). Son utilizadas para el direccionamiento punto a multipunto (multicast).
- Clase E: Los cuatro bits más significativos del primer octeto son: 1111 (primer número entre 240 y 255). Se encuentran reservados para usos futuros.

La clase de dirección a utilizar dependerá del número de equipos presentes en una red (ver tabla 1.1). Cuando un equipo se encuentra conectado a múltiples redes deberá tener una IP por cada red que interconecte.

Clase	Rango
A	0.0.0.0 - 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 247.255.255.255

Tabla 1.1: Rango de direcciones IP en Internet

Existen algunas direcciones especiales que no pueden ser utilizadas por equipos, como son:

- Direcciones de red: Para identificar una red en su conjunto, se usa una dirección IP con el identificador de equipo puesto a cero. Por ejemplo, direcciones como 122.0.0.0 o 193.23.121.0 son direcciones de red.
- Dirección de difusión local: Se utiliza para hacer llegar un paquete a todos los equipos conectados a la red, y consiste en la dirección con todos los bits de la parte de equipo puestos a 1. Por ejemplo, 122.255.255.255 o 193.23.121.255.
- Dirección de difusión total: Utilizada para hacer llegar un paquete a todos los equipos de todas las redes. Consiste en todos los bits de la dirección puestos a 1 (255.255.255.255). Normalmente los encaminadores no la propagan, con lo cual equivale a la difusión local.
- Dirección de bucle local: utilizada para indicar el propio equipo, es cualquiera en la red de clase A con identificador de equipo 127, es decir, 127.XXX.XXX.XXX. Generalmente se suele emplear 127.0.0.1
- Dirección desconocida: utilizada para indicar la entrada por defecto en la tabla de encaminamiento: todos los bits a cero (0.0.0.0).

Además de estas direcciones especiales, existen algunos rangos de direcciones que están reservados para uso privado (ver tabla 1.2), es decir, pueden ser utilizados en redes privadas que no necesiten conectarse con el exterior, y está prohibido utilizarlos en redes públicas (Internet).

Clase	Rango
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

Tabla 1.2: Rango de direcciones IP reservadas

1.1.3.3 Máscaras

La máscara de red es un número con el formato de una dirección IP que nos sirve para distinguir cuando una máquina determinada pertenece a una subred

dada, con lo que podemos averiguar si dos máquinas están o no en la misma subred IP. En formato binario todas las máscaras de red tienen los "1" agrupados a la izquierda y los "0" a la derecha [5].

Estas máscaras constan de 4 octetos (32 bits), igual que una dirección IP y por como se utilizan deben contener unos a la izquierda y ceros a la derecha, es decir, no pueden haber mezclas de unos y ceros [3]. Por ejemplo

Máscara = 1111 1111.1111 1111.1111 0000.0000 0000

Como siempre la máscara va asociada a la dirección IP, se indica con /XX a continuación de la dirección IP, siendo XX el número de unos de la máscara, para el ejemplo sería /20. En Internet es habitual el empleo de las siguientes máscaras para cada clase:

Clase	Máscara
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Tabla 1.3: Clases de Máscaras

Si a una dirección IP aplicamos la máscara con el operador AND, en realidad dividimos la dirección IP en 2 partes:

- La parte izquierda que corresponde a la identificación de la red física.
- La parte derecha que identifica al dispositivo dentro de cada red.

Con las máscaras introducimos el concepto de número de red dentro del campo de dirección IP. Las máscaras no viajan en los mensajes IP, es decir, se emplean de forma local en cada dispositivo.

1.1.3.4 CIDR (Classless Inter-Domain Routing)

CIDR es un estándar basado en prefijos de red para la interpretación de direcciones IP. CIDR facilita el encaminamiento al permitir agrupar bloques de direcciones en una sola entrada de tablas de rutas. Estos grupos llamados comúnmente bloques CIDR, comparten una misma secuencia inicial de bits en la representación binaria de direcciones IP.

Los bloques CIDR IPv4 se identifican usando una sintaxis similar a las de las direcciones IPv4: cuatro números decimales separados por puntos, seguidos de una barra de división y un número de 0 a 32; *A.B.C.D/N.*

Los primeros cuatro números decimales se interpretan como una dirección IPv4 y el número tras la barra es la longitud del prefijo, contando desde la izquierda y representa el número de bits comunes a todas las direcciones incluidas en el bloque CIDR [6].

Una dirección IP esta incluida en un bloque CIDR y encaja con el prefijo CIDR, si los N bits iniciales de la dirección y el prefijo son iguales. Por tanto, para entender CIDR es necesario visualizar la dirección IP en binario. Dado que la longitud de una dirección IPv4 es fija de 32 bits, un prefijo CIDR, de N bits deja 32-N bits sin encajar y hay $2^{(32-N)}$ combinaciones posibles con los bits restantes. Esto quiere decir que $2^{(32-N)}$ direcciones IPv4 encajan en un prefijo CIDR de N bits.

Los prefijos CIDR cortos (números cercanos a 0) permiten encajar un mayor número de direcciones IP, mientras que prefijos CIDR largos (números cercanos a 32) permiten encajar menos direcciones IP.

1.1.3.5 CIDR y Máscaras de Red

CIDR usa máscaras de subred de longitud variable (VLSM) para asignar direcciones IP a subredes de acuerdo a las necesidades de cada subred. De esta forma, la división red/host puede ocurrir en cualquier bit de los 32 que componen

la dirección IP. Este proceso puede ser recursivo, dividiendo una parte del espacio de direcciones en porciones cada vez menores, usando máscaras que cubren un mayor número de bits. Las direcciones CIDR/VLSM se usan a lo largo y ancho de la Internet pública y en muchas grandes redes privadas.

1.1.4 El protocolo TCP

El protocolo TCP se podría definir como un protocolo orientado a conexión, fiable y orientado a un flujo de bytes [2].

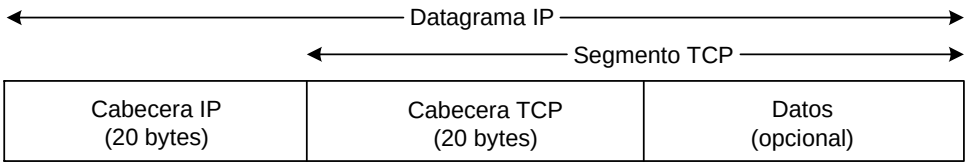

Figura 1.4: Estructura de un segmento TCP

Aunque el protocolo TCP utiliza los servicios de IP para su transporte por Internet (ver figura 1.4), es un protocolo orientado a conexión. Esto significa que las dos aplicaciones envueltas en la comunicación (usualmente un cliente y un servidor), deben establecer previamente una comunicación antes de poder intercambiar datos.

TCP es también un protocolo fiable. La fiabilidad proporcionada por este protocolo viene dada principalmente por los siguientes aspectos:

- Los datos a enviar son reagrupados por el protocolo en porciones denominadas segmentos. El tamaño de estos segmentos lo asigna el propio protocolo.
- Cuando en una conexión TCP se recibe un segmento completo, el receptor envía una respuesta de confirmación (Acknowledge) al emisor confirmando el número de bytes correctos recibidos. De esta forma, el emisor da por correctos los bytes enviados y puede seguir enviando nuevos bytes.

- Cuando se envía un segmento se inicializa un temporizador (timer). De esta forma, si en un determinado plazo de tiempo no se recibe una confirmación (Acknowledge) de los datos enviados, estos se retransmiten.
- TCP incorpora un checksum para comprobar la validez de los datos recibidos. Si se recibe un segmento erróneo (fallo de checksum por ejemplo), no se envía una confirmación. De esta forma, el emisor retransmite los datos (bytes) otra vez.
- Como IP no garantiza el orden de llegada de los datagramas, el protocolo TCP utiliza unos números de secuencia para asegurar la recepción en orden, evitando cambios de orden o duplicidades de los bytes recibidos.
- TCP es un protocolo que implementa un control de flujo de datos. De esta forma, en el envío de datos se puede ajustar la cantidad de datos enviada en cada segmento, evitando colapsar al receptor [2].

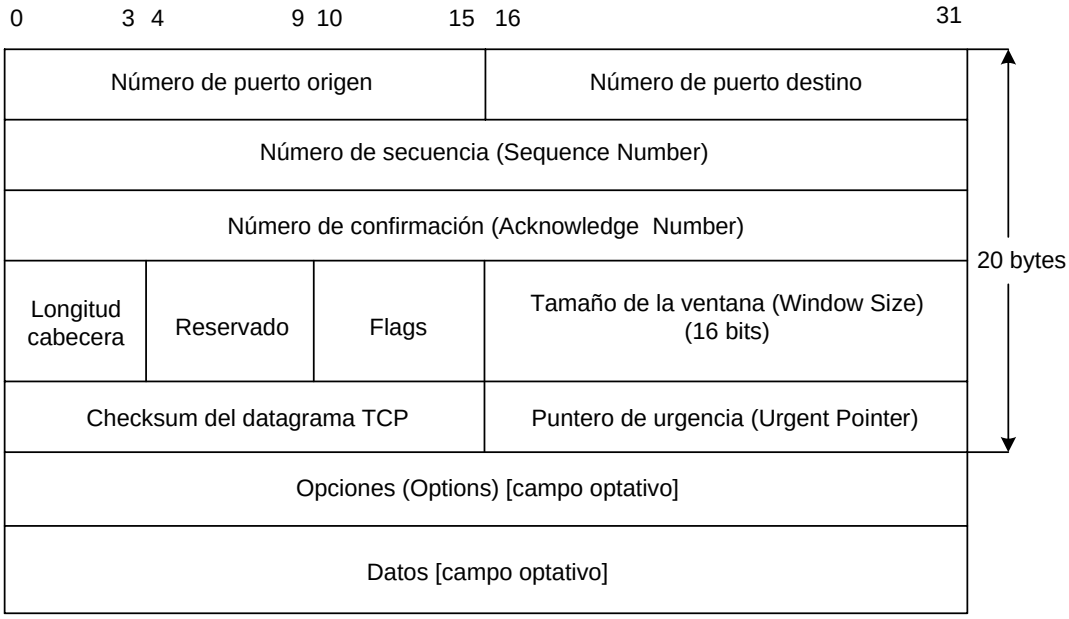

Figura 1.5: Cabecera de un segmento TCP

La cabecera del segmento TCP esta dividida en bloques de 32 bits (ver figura 1.5). La información se divide en segmentos que son enviados en datagramas IP utilizando mecanismos de control de flujo que regulan la velocidad de envío de segmentos en función del nivel de carga de la red.

El número de puerto origen y número de puerto destino, sirven para diferenciar una comunicación en un ordenador de las demás. La cuádrupla formada por la dirección IP y el número de puerto se denomina socket.

El número de secuencia (Sequence Number), identifica el byte de inicio del segmento del flujo de datos que actualmente se envía del emisor al receptor. De esta forma, TCP numera los bytes de la comunicación de una forma consecutiva a partir del número de secuencia inicial. Cuando se establece una comunicación, emisor y receptor eligen un número de secuencia común, lo que nos permite implementar mecanismos de control como asegurar que los datos lleguen en el orden adecuado.

El número de confirmación (Acknowledge Number), es el número de secuencia más uno. De este modo se especifica al emisor que los datos enviados hasta este número de secuencia menos uno son correctos. De aquí la importancia de la elección al principio de la comunicación de un número de secuencia común.

La longitud de la cabecera (header Length), especifica en palabras de 32 bits (4 bytes) el tamaño de la cabecera del segmento TCP incluyendo las posibles opciones. De esta forma el tamaño máximo es 60 bytes. No obstante, lo usual es tener un tamaño de 20 bytes (cabecera dónde no se incluyen opciones).

Las banderas (Flags), son las encargadas de especificar los diferentes estados de la comunicación. Así mismo, también validan los valores de los distintos campos de la cabecera de control. Puede haber simultáneamente varios flags activados.

El tamaño de la ventana (Window Size), es el número de bytes desde el número especificado en el campo de confirmación, que el receptor está dispuesto a aceptar. El tamaño máximo es de 65535 bytes. De esta forma, el protocolo TCP permite la regulación del flujo de datos entre el emisor y el receptor.

El checksum del segmento TCP, al igual que el de IP, tiene la función de controlar los posibles errores que se produzcan en la transmisión. Este checksum engloba la cabecera TCP y los datos. En caso de error, el datagrama/segmento queda descartado y el propio protocolo es el encargado de asegurar la retransmisión de los segmentos erróneos o perdidos.

El puntero de urgencia (Urgent Pointer), es válido sólo si el flag de URG se encuentra activado. Consiste en un valor positivo que se debe sumar al número e secuencia especificando una posición adelantada dónde podemos enviar datos urgentes.

Las opciones (Options), nos permiten especificar de forma opcional características extras a la comunicación, como el tamaño máximo de segmento a utilizar.

Los datos (Data) son opcionales. Esto significa que podemos enviar simplemente cabeceras TCP con diferentes opciones. Esta característica se utiliza por ejemplo al iniciar la comunicación o en el envío de confirmaciones. De esta manera, minimizamos el overhead ya que tan sólo enviamos/recibimos lo necesario para establecer o confirmar la comunicación.

1.1.5 Características

Dentro de un sistema TCP/IP los datos transmitidos se dividen en pequeños paquetes, éstos resaltan una serie de características [1].

- La tarea de IP es llevar los datos de un sitio a otro. Las computadoras que encuentran las vías para llevar los datos de una red a otra (denominadas enrutadores) utilizan IP para trasladar los datos. En resumen IP mueve los paquetes de datos, mientras TCP se encarga del flujo y asegura que los datos estén correctos.

- Las líneas de comunicación se pueden compartir entre varios usuarios. Cualquier tipo de paquete puede transmitirse al mismo tiempo, y se ordenará y combinará cuando llegue a su destino.
- Los datos no tienen que enviarse directamente entre dos computadoras. Cada paquete pasa de computadora en computadora hasta llegar a su destino. Se necesitan algunos segundos para enviar un archivo de buen tamaño de una máquina a otra, aunque estén separadas por miles de kilómetros y pese a que los datos tienen que pasar por múltiples computadoras. Una de las razones de la rapidez es que, cuando algo anda mal, sólo es necesario volver a transmitir un paquete, no todo el mensaje.
- Los paquetes no necesitan seguir la misma trayectoria. La red puede llevar cada paquete de un lugar a otro y usar la conexión más idónea que esté disponible en ese instante. No todos los paquetes de los mensajes tienen que viajar por la misma ruta.
- La flexibilidad del sistema lo hace muy confiable. Si un enlace se pierde, el sistema usa otro. Cuando se envía un mensaje, el TCP divide los datos en paquetes, ordena éstos en secuencia, agrega cierta información para control de errores y después los distribuye. En el otro extremo, el TCP recibe los paquetes, verifica si hay errores y los vuelve a combinar para convertirlos en los datos originales. De haber error en algún punto, el programa TCP destino envía un mensaje solicitando que se vuelvan a enviar determinados paquetes.

1.1.6 Encaminamiento de datagramas

El proceso de rutado o encaminamiento (routing) hace referencia a cómo los distintos datagramas IP enviados circulan y seleccionan el camino hacia su destino [2].

Debido a la construcción de la Internet para que fuera tolerante a fallos, estos caminos no son fijos o estáticos, sino que existen diferentes vías que se actualizan dinámicamente para que un paquete alcance su destino sin necesidad de usar siempre la misma ruta. De esta forma, tenemos que cada paquete se encamina de forma independiente hacia su destino.

Los ordenadores encargados de recibir y enrutar los datagramas hasta su siguiente paso hacia el destino se denominan routers. Estos routers se encargan de leer la dirección destino del paquete y seleccionar su vía de salida.

En la figura 1.6 podemos ver el proceso de encaminamiento, dónde un router recibe un datagrama IP y lo conduce hasta el siguiente router.

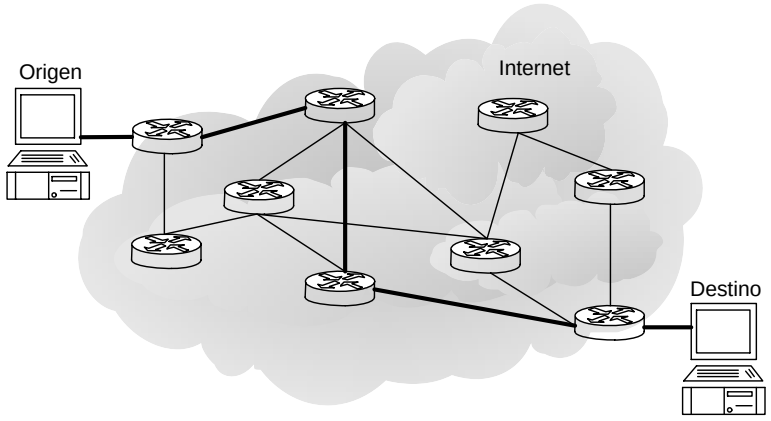

Figura 1.6: Rutado de paquetes en Internet

Podemos ver pues que está comunicación se produce mediante saltos unitarios (hops) de router a router hasta que alcanza su destino o el paquete es descartado. Una vez que el datagrama llega hasta el router final, este se propaga por la red local hasta su destino.

1.2 El Protocolo OSPF

En 1988, la Internet Engineering Task Force (IETF) comenzó a trabajar en un protocolo más sofisticado que llegaría a convertirse en estándar en 1990. Este protocolo fue el OSPF (Open Shortest Path First) [7].

En OSPF, cada enrutador construye y mantiene una base de datos que refleja la topología de la red, expresada en forma de grafo dirigido. Los nodos de dicho grafo son los enrutadores y las redes, a su vez divididas en *redes de tránsito*. Los enlaces pueden conectar dos enrutadores entre sí o un enrutador a

una red. También es posible la conexión de un enrutador a un terminal. Se asocia un coste no nulo a los enlaces de salida de los enrutadores hacia las redes, y un coste nulo a los enlaces que parten desde la red hacia los enrutadores. Si un enrutador está conectado a un sistema autónomo (AS) distinto, se representa cada red del otro sistema como una red terminal conectada al enrutador a través de un enlace cuyo coste es determinado por un protocolo de encaminamiento exterior.

1.2.1 Estructura Jerárquica

Debido a que muchos AS son grandes y difíciles de manejar, OSPF permite su división en *áreas numeradas*, donde un área es una red o grupo de redes contiguas. Un área es una generalización de una subred y fuera de ella su topología no es visible. Cada AS tiene un área principal o *backbone*, al que están conectadas el resto de las áreas en una distribución de estrella. OSPF clasifica los enrutadores en cuatro tipos, en función del área o áreas a las que pertenezcan:

- Enrutadores *internos*, contenidos en una única área.
- Enrutadores *de borde de área*, conectados a varias áreas. Estos enrutadores necesitan la base de datos de ambas áreas y deben realizar, para cada una por separado, la obtención de rutas optimas.
- Enrutadores *de backbone*. Estos enrutadores aceptan información de los enrutadores de borde de área con el fin de calcular la mejor ruta a todos los enrutadores. Esta información se propaga de regreso a la enrutadores de borde de área, quienes la divulgan a su área. Usando esta información, un enrutador a punto de enviar un paquete puede seleccionar el mejor enrutador de salida al backbone. A continuación, el paquete atraviesa el backbone hasta alcanzar el enrutador de borde perteneciente al área de destino. Finalmente, el mensaje se desplaza desde el enrutador conectado al backbone hasta el nodo destino. Todos los enrutadores de borde de área son automáticamente parte del backbone.

- Enrutadores *de frontera de AS*, que se relacionan con enrutadores de otros AS.

Para asimilar cambios de topología, OSPF opera realizando intercambios de información entre enrutadores adyacentes. Es muy frecuente que estos estén conectados a través de una red LAN (Local Area Network). En estas situaciones, todos ellos consideran al resto como sus vecinos inmediatos, lo que conlleva que la sobrecarga añadida por el mecanismo de encaminamiento se incremente considerablemente. Estos efectos indeseables se evitan mediante la elección de un *enrutador designado*, el cual asume que sólo él es adyacente a todos los demás. El enrutador designado intercambia información con el resto de enrutadores, y estos no intercambiarán información entre sí. Generalmente, tras un cambio de topología el enrutador designado es aquel que ya estaba designado antiguamente o aquel con identificador de mayor prioridad [7].

1.1.2 Tipos de Servicio

OSPF dispone de cinco tipos de servicio, los mismos que se utilizan en IPv4. El tipo de servicio se define en el campo ToS (Type of Service) del paquete, y determina el significado del coste de los enlace. A continuación una breve descripción de cada tipo de servicio:

1. Normal (ToS 0): Es la métrica que se emplea por defecto. Asignada por el administrador para satisfacer necesidades generales, y que es comprendida por todos los enrutadores.
2. Minimizar coste monetario (ToS 2): Métrica empleada si se puede asignar coste monetario al uso de la red.
3. Maximizar fiabilidad (ToS 4): Métrica basada en la historia reciente de fallos en la red o en tasas de paquetes erróneos.
4. Maximizar caudal (ToS 8): Esta métrica debe configurarse previamente basándose en la capacidad de cada enlace. Una magnitud muy utilizada es la duración de un bit en nanosegundos.
5. Minimizar retardo (ToS 16): Medida del retardo para un salto particular, basada en el retardo de propagación y en el retardo en los buffers.

Para proporcionar estos cinco tipos de servicio, OSPF mantiene cinco grafos de topología distintos y sus correspondientes tablas de encaminamiento. Los datagramas IP suelen incorporar un campo ToS. Según el valor de este campo, cada enrutador consulta la tabla de encaminamiento apropiada para encaminar el datagrama. Si el datagrama no incluye el campo ToS entonces se usa la tabla correspondiente a la métrica por defecto (ToS 0).

1.2.3 Formato de los paquetes

OSPF es un protocolo que se ejecuta sobre IP, es decir, sus paquetes son transmitidos encapsulados dentro de paquetes IP. Los paquetes OSPF tienen la misma cabecera de longitud fija, lo que favorece su codificación compacta y rápido procesamiento [7]. Esta cabecera se muestra en la Figura 1.7. El significado de cada campo es el siguiente:

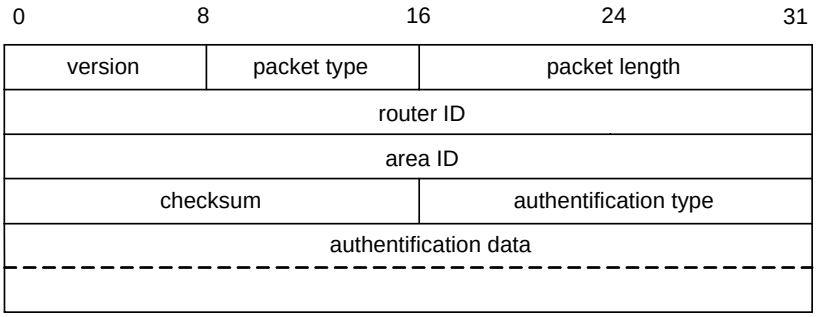

Figura 1.7: Cabecera común de los paquetes OSPF

- *Version*: Versión del protocolo
- *Packet type*: Tipo de paquete
  1 = hello
  2 = DD, database description
  3 = link state request (solicitud de información)
  4 = link state update (actualización de información)
  5 = link state acknowledment (reconocimiento de actualización)
- *Packet length*: Número de octetos del paquete.
- *Router ID*: Dirección IP del enrutador emisor.

- *Area ID*: Identificador del área a la que pertenece el paquete.
- *Checksum*: Código de error.
- *Authentification type*:
  0 = sin autentificación
  1 = con clave simple
  2 - 255 = actualmente indefinido.
- *Authentification data*: Clave de 64 bits.

A continuación se describe cada uno de los cinco tipos de paquetes OSPF. En primer lugar, los paquetes *hello* permiten detectar cambios en el estado de los vecinos o de los enlaces que unen a un nodo con sus vecinos. Siempre son transmitidos entre vecinos inmediatos y nunca recorren más de un enlace. La figura 1.8 muestra el formato de estos paquetes donde se ha obviado la cabecera. El significado de cada campo es el siguiente:

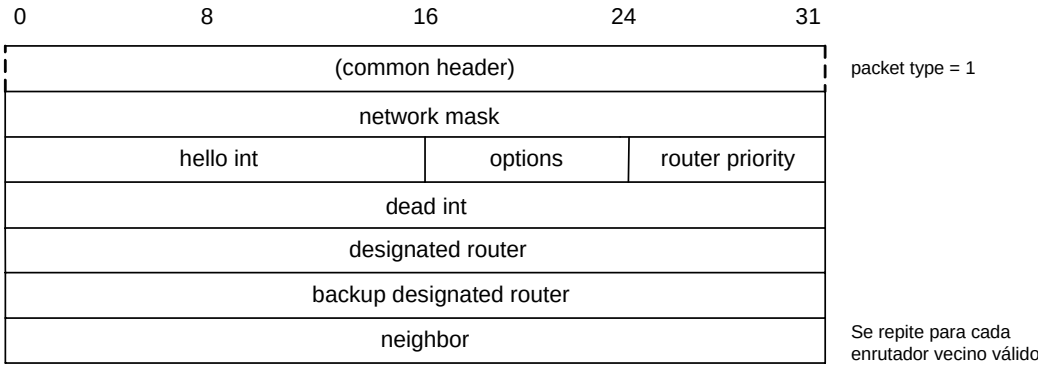

Figura 1.8: Paquete *hello* de OSPF

- *Network mask*: La máscara configurada para este enlace en el enrutador emisor. Si el receptor no comparte este valor, entonces rechaza el paquete y no acepta el emisor como vecino.
- *Hello int*: Intervalo entre emisión de paquetes *hello.* Este campo también debe coincidir con la información del receptor.
- *Options*: Ciertas opciones como el soporte de múltiples métricas.

- *Router priority*: Prioridad aplicada en la elección de enrutadores designados (principales y de reserva).
- *Dead int*: Intervalo de tiempo en que un enrutador considera a otra desactivado si no recibe paquetes *hello*.
- *Designated router*: Identificador del enrutador que el emisor considera enrutador designado, o cero si no considera ninguno.
- *Backup designated router*: Identificador del enrutador que el emisor considera enrutador designado de reserva, o cero si no considera ninguno.
- *Neighbors*: Lista de identificadores de vecinos activos, es decir, aquellos de los que ha recibido paquetes *hello* dentro del intervalo delimitado en el campo *dead int*.

Cuando se activa un enlace entre dos enrutadores, estos deben sincronizar la información topológica que poseen. Para ello, los dos nodos aceptan una relación maestro/esclavo. El maestro comunica su información topológica al esclavo mediante paquetes de descripción de la base de datos (DD), utilizando tantos como sea necesario. Por su parte, el enrutador esclavo confirma cada paquete DD enviando paquetes DD al maestro con el mismo número de secuencia, pero conteniendo la propia información topológica. El maestro no envía un nuevo DD en tanto el anterior no haya sido confirmado. Cuando un nodo ha terminado de transmitir su información topológica continúa emitiendo paquetes vacíos hasta que termine el otro. La figura 1.9 muestra el formato de estos paquetes. El significado de cada campo es el siguiente:

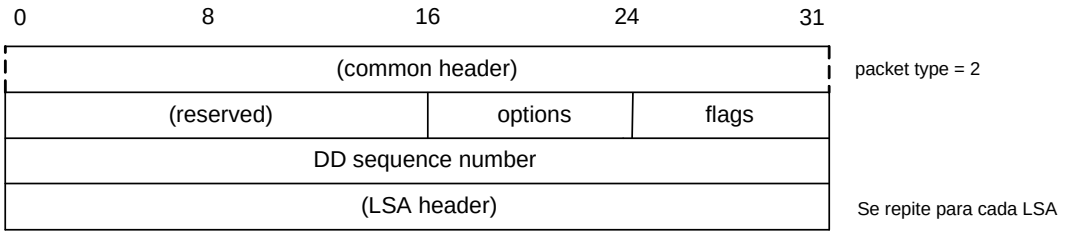

Figura 1.9: Paquete *database description*

- Options: Similar al campo *options* del paquete *hello.*

- *Flags:* bits cuyo estado activo indica
  MS (master/slave): el emisor es el nodo maestro.
  M (more): no es el último paquete DD.
  I (init): es el primer paquete DD.
- *DD packet sequence number*: Número orden en la secuencia de paquetes de descripción de topología.
- *LSA header*: es la parte común a diferentes tipos de LSA (link state advertisiment). Puede repetirse varias veces dentro del paquete. Como otros paquetes también incorporan LSA.

En cualquier momento, un enrutador puede solicitar información topológica a otro enrutador vecino. Para ello utiliza un mensaje *link state request*. La figura 1.10 muestra el formato de estos paquetes. Los campos *LS type, link state ID y adevertising router* son en realidad un fragmento de la cabecera de un LSA.

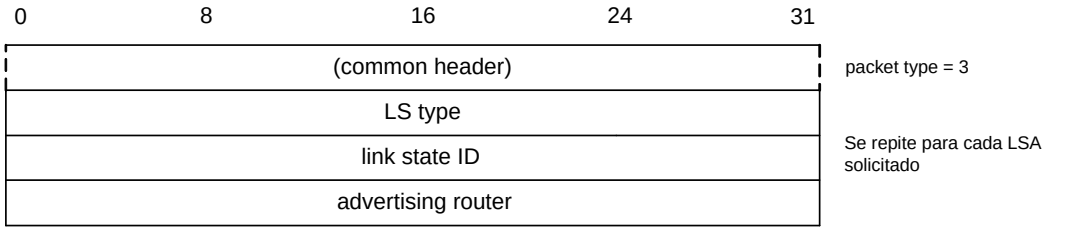

Figura 1.10: Paquete *link state request*

Los paquetes link state update contienen uno o varios LSAs. La figura 1.11 muestra el formato de estos paquetes.

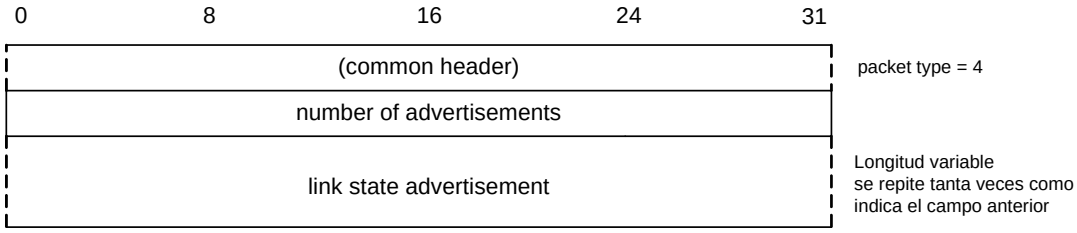

Figura 1.11: Paquete *link state update*

Los paquetes *link state acknowlegment* son paquetes de reconocimiento que proporciona su confiabilidad a OSPF. Cada uno puede reconocer varios LSAs. La figura 1.12 muestra el formato de estos paquetes.

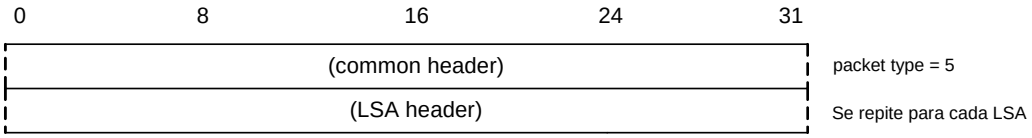

Figura 1.12: Paquete *link state acknowlegment*

1.2.4 Información contenida en un LSA

Existen cinco tipos de LSAs. Todos ellos tienen una cabecera común. Primero se describe esta cabecera y después se comenta la información exclusiva de cada tipo. La cabecera tiene una longitud fija de 20 bytes, cuyo formato se muestra en la figura 1.13. El contenido de cada campo es el siguiente:

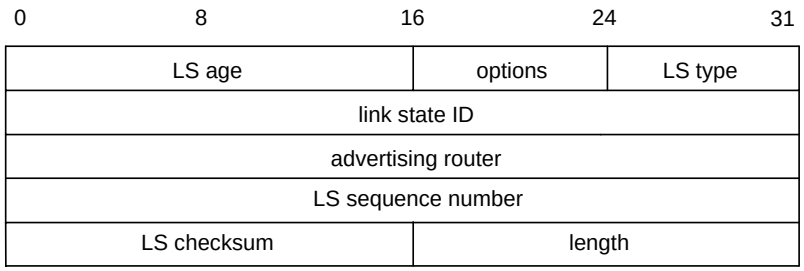

Figura 1.13: Cabecera de un LSA

- *LS age*: Edad estimada de la información.
- *LS type:* Los valores posibles son los siguientes:
  1 = enlaces del enrutador.
  2 = enlaces de la red.
  3 = resumen de enlaces (subredes IP alcanzables)
  4 = resumen de enlaces (enrutadores alcanzables de sistemas vecinos)
  5 = resumen de enlaces (subredes IP alcanzables de sistemas vecinos)
- *Link state ID*: Su significado depende del valor del campo anterior:
  Type = 1, el ID del enrutador que generó la información.

Type = 2, la dirección IP del enrutador designado de la LAN.

Type = 3, la dirección IP del enlace que conecta la subred.

Type = 4, el ID del enrutador borde.

Type = 5, la dirección IP del enlace que conecta la subred.

- *Advertising router:* ID del enrutador que generó la información.
- *LS sequence number:* Número de secuencia del LSA.
- *LS checksum:* Código de redundancia.
- *Length:* Tamaño em bytes.

1.3 El Protocolo BGP

El protocolo BGP (Border Gateway Protocol) es el protocolo de encaminamiento interdominio más utilizado en Internet. Este protocolo se diseño para permitir la cooperación en el intercambio de información de encaminamiento entre enrutadores de distintos sistemas autónomos. En terminología BGP los enrutadores se denominan gateways y realizan tres procesos funcionales: adquisición de vecinos, detección de vecinos alcanzables y detección de redes alcanzables [7].

El término *adquisición de vecinos* implica que dos dispositivos de encaminamiento que comparten la misma subred física, pero pertenecen a distintos sistemas autónomos, deciden intercambiar regularmente información de encaminamiento. Se requiere un procedimiento formal para la adquisición ya que uno de los dos dispositivos puede decidir no participar. En este procedimiento un dispositivo hace una oferta a otro (mediante un mensaje *open*), el cual puede aceptarla (mediante un mensaje *keepalive*) o rechazarla.

Una vez establecida la relación de vecindad, se utiliza el procedimiento de *detección de vecino alcanzable* para mantenerla. Cada miembro necesita estar seguro de que su pareja existe y está todavía comprometida con la relación. Para este propósito, periódicamente ambos dispositivos de encaminamiento se envían mensajes *keepalive*.

El último procedimiento es la *detección de redes alcanzables*. Cada pasarela mantiene una base de datos con las subredes que puede alcanzar y la ruta completa para hacerlo. Siempre que se modifica esta base de datos, la pasarela lo notifica a todos los demás dispositivos de encaminamiento que implementan BGP, por medio de paquetes *update*. De esta forma, el resto de pasarelas puede actualizar su propia información [7].

1.3.1 Formato de los paquetes

A diferencia de OSPF, BGP es un protocolo situado sobre el nivel de transporte, es decir, los paquetes BGP son transmitidos encapsulados dentro de paquetes TCP. Esto permite asumir que el intercambio de información se realiza de forma confiable. Los cuatro tipos de paquetes BGP tienen la cabecera mostrada en la figura 1.14. El contenido de cada campo es el siguiente:

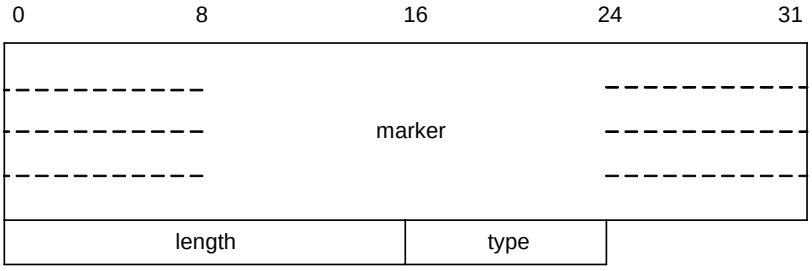

Figura 1.14: Cabecera de un mensaje BGP

- *Marker:* El emisor puede insertar un valor de hasta 16 bytes en este campo. Este valor sería usado como parte de un mecanismo de autentificación que permita al destinatario verificar la identidad del emisor.
- *Length:* Longitud en bytes del paquete, incluyendo la cabecera.
- *Type:* Tipo de paquete. Existen cuatro posibilidades:
  1 = open
  2 = update
  3 = notification
  4 = keepalive

Para adquirir un vecino, un dispositivo de encaminamiento establece primero una conexión TCP. Para ello se utiliza un paquete *open* mostrado en la figura 1.15. Este mensaje identifica al AS al que pertenece el emisor y suministra la dirección IP del dispositivo de encaminamiento. La descripción de cada campo es la siguiente:

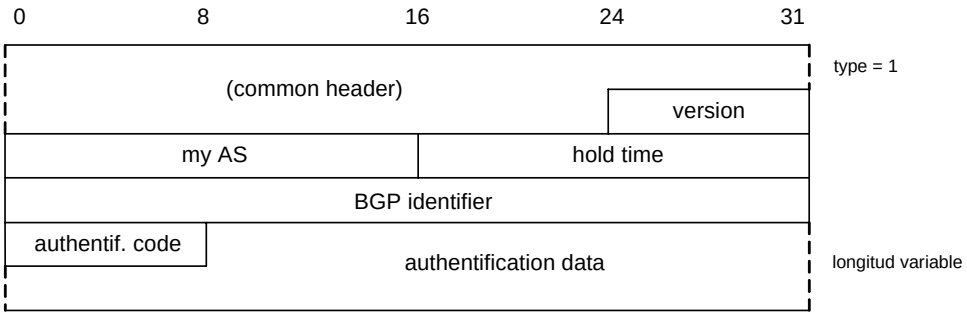

Figura 1.15: Formato de paquete *open*

- *Version:* Versión del protocolo, actualmente la 4.
- *My autonomous system:* Indica el número de AS del emisor.
- *Hold time:* Tiempo que tiene que esperar el receptor antes de asumir que el emisor a caído. El emisor debe continuar emitiendo paquetes antes de que este tiempo se agote.
- *BGP identifier:* Dirección IP del emisor. BGP considera como identificador de cada enrutador su propia dirección IP.
- *Authentification code:* Define el sistema de autentificación empleado. En la actualidad este campo se asigna a cero.
- *Authentification data:* Datos destinados a la autentificación del paquete. La longitud y el contenido de este campo dependen del campo anterior.

Un mensaje *update* facilita dos tipos de información:

1. Información sobre una ruta particular a través del conjunto de redes. Dicha ruta se incorpora a la base de datos de cada dispositivo de encaminamiento que la recibe.

2. Una lista de rutas que fueron previamente anunciadas por este dispositivo de encaminamiento, y que ahora han sido eliminadas.

Estos dos tipos de información pueden ser proporcionadas simultáneamente en un único paquete. El formato del paquete *update* se muestra en la figura 1.16. El contenido de cada campo se describe a continuación:

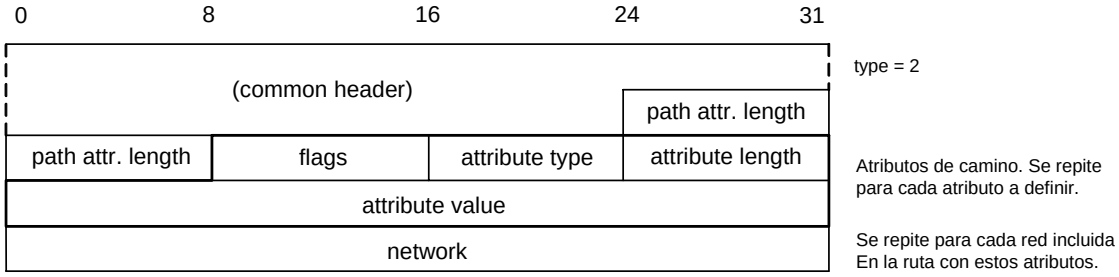

Figura 1.16: Formato de paquete *update*

- *Path attributes length:* Longitud de rutas no factibles. Número de atributos de la ruta.
- *Flags:* Diversos bits que indican la opcionalidad, transitividad y parcialidad del atributo.
- *Attribute type:* Existen cinco tipos de atributos:

  1 = *origin*; al atributo ocupa 1 byte e indica si la información fue generada por un protocolo de encaminamiento interior (como OSPF) o por un protocolo de encaminamiento exterior (en particular, BGP).

  2 = *AS path*; el atributo es de longitud variable y enumera una lista de AS que atraviesa la ruta.

  3 = *next hop*; el atributo ocupa 4 bytes y proporciona la dirección IP del dispositivo de encaminamiento frontera que se debe usar para alcanzar los destinos indicados en el campo *network*.

  4 = *unreachable*; el atributo no ocupa lugar adicional.

  5 = *inter-AS metric*; el atributo ocupa 2 bytes.

El tercer tipo de paquete es el paquete *notification*.

Un paquete de notificación es enviado por el enrutador R1 al enrutador R2 para explicar porque deniega la conexión a R2. Su formato se muestra en la figura 1.17. El contenido de cada campo es el siguiente:

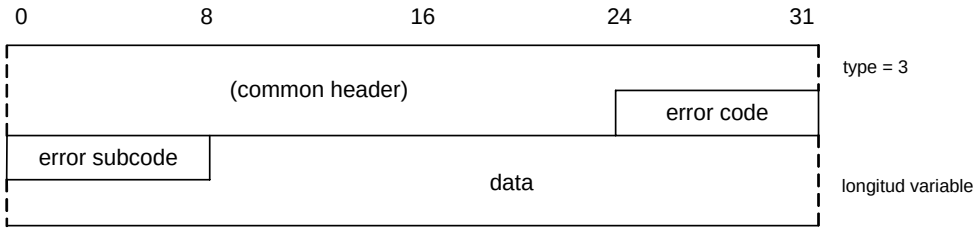

Figura 1.17: Formato de paquete *notification*

- *Error code:* Para cada código de error existen diversos subcódigos que no detallaremos:
  1 = cabecera corrupta. El tipo de paquete es inaceptable, bien por errores de sintaxis o por cuestiones de autentificación.
  2 = paquete *open* corrupto.
  3 = paquete *update* corrupto.
  4 = tiempo de hola down expirado.
  5 = error en la máquina d estados finitos (errores de procedimiento).
  6 = cese (cierre voluntario de una conexión).
- Data: Contiene el comando ofensivo.

El cuarto y último tipo de paquete es el paquete *keepalive*. Este paquete no tiene otra información aparte de la cabecera mostrada en la figura 1.13. Este paquete se envía para inicializar el temporizador *hold town* del receptor antes de que expire, y el emisor no tiene información de interés que comunicar.

1.4 Calidad de Servicio en Redes IP

Se entiende por calidad de servicio (QoS) de la red, la garantía que esta proporciona a una transmisión de datos, la cual requiere unos niveles mínimos de ancho de banda y una respuesta temporal acotada para resultar satisfactoria [8].

1.4.1 Parámetros

A continuación se detalla un conjunto acotado de parámetros de calidad de servicio:

1.4.1.1 Ancho de banda

Es la media del número de bits por segundo que pueden ser transmitidos correctamente a través de la red. El caudal de medida suele encontrarse desde kbps o Mbps.

1.4.1.2 Retardo punto a punto

Es el tiempo medio acumulado durante el trayecto de un paquete para atravesar la red de un punto a otro. Para medir con exactitud el retardo, se deben tener en cuenta los puntos donde éste se produce:

- Retardo de propagación. Es el retardo que se obtiene del tiempo que tarda la luz en recorrer el medio de transmisión por la que se transmite.
- Retardo de conmutación. Se produce por el tiempo consumido en el procesado realizado para cambiar el enlace por el que un paquete ha entrado al router.
- Retardo de clasificación (scheduling). El retardo de scheduling o queueing se debe a la acción de clasificar el tráfico en las diferentes colas de los equipos de red. Desde el momento en el que un paquete llega a una cola, se decide cual es su clase correspondiente, se añade a esa cola y luego, se vuelve a transmitir a la salida de la cola se sucede un retardo en la transmisión.
- Retardo de serialización: El retardo de serialización aparece cuando un paquete es adaptado a un medio por el cual se va a transmitir. La velocidad de ese mismo medio y el tamaño del paquete son determinantes.

1.4.1.3 Jitter

Variación del retardo punto a punto de los paquetes causada por la clasificación y los retardos de acceso en el nodo fuente, y por el retardo de los

nodos de tránsito y el buffer del nodo de recepción. Las variaciones que suceden durante estos procesos, por no tener comportamientos fijos, son los causantes de la aparición del jitter.

1.4.1.4 Pérdida de Paquetes

La pérdida de paquetes es medida como un porcentaje de los paquetes transmitidos. Son los paquetes que siendo enviados nunca llegan a su destino.

Los motivos que provocan una pérdida de paquetes son múltiples siendo la congestión el primer causante de ello. Concretamente, el límite de capacidad de los buffers de los dispositivos de red es el punto donde se registra el problema.

1.4.2 Modelo de QoS IntServ

El modelo de servicios diferenciados o IntServ (INTegrated SERVices) realiza una reserva previa de recursos antes de establecer la comunicación. El protocolo que lleva a cabo la reserva de recursos y la señalización de establecimiento de rutas es el RSVP (Resource Reservation Protocol) [8].

Para el modelo IntServ existen tres tipos de calidad de servicio:

- Garantizado. Con ancho de banda reservado, retardo acotado y sin pérdida de datos.
- Carga controlada. Condiciones de transmisión mínimas similares a best-effort con poca carga de red.
- Best-effort. Similar a las condiciones de acceso a la Internet actuales con variación de respuesta en función de la carga de la red.

1.4.3 Modelo de QoS DiffServ

El modelo de servicios diferenciados o DiffServ es propuesto por la IETF para habilitar una cierta clasificación del tráfico IP en un número limitado de clases de servicio. Si bien los DiffServ no establecen una ruta extremo a extremo para conocer el estado de la red, los dispositivos de red con clases de servicio

configuradas pueden llegar a obtener un resultado preferente para tráfico prioritario con respecto a los demás cuando la red está congestionada [8].

Los servicios diferenciados son propuestos para resolver problemas que aparecen en los servicios integrados y en RSVP, siendo el modelo *DiffServ* más escalable, flexible y sencillo.

1.5 Los Peligros en nuestras Redes

Año tras año, el número de virus y gusanos que se cuelan en sistemas va en aumento, e incluso los ataques han ido modificando su disfraz. Por eso desde hace poco podemos hablar de spyware y de troyanos, además de los ya conocidos virus y gusanos [9].

Por ello son muchas las empresas que han sacado al mercado productos de defensa: antivirus, antisyware, antitroyanos, etc. Todos dedicados, junto con otros sistemas de defensa, a preservar la seguridad de los usuarios de la red y a reducir el número de vulnerabilidades.

1.5.1 Servicios para la seguridad

La falta de seguridad de las comunicaciones, propicia la obtención de contraseñas en texto en claro, direcciones de redes, puertos, etc. Con toda esta información, los atacantes-intrusos pueden conseguir entrar en la red, enviar mensajes en nombre de otros y muchas otras formas de atacar.

Existen muchas maneras de conseguir información de otras personas, aunque también existen sistemas para evitar que se produzcan esos robos de información. Para preservar la seguridad de las comunicaciones y de las redes privadas, existen una serie de servicios a tener en cuenta:

- Confidencialidad: Es la protección de la información transmitida, de tal manera que sólo el emisor y el receptor deseado entiendan el contenido del mensaje. Por ello, la información es encriptada (transformada-

disfrazada) para que el mensaje interceptado por una tercera persona no pueda ser desencriptado y por lo tanto, entendido. Otro aspecto de la confidencialidad es la protección del tráfico de los posibles análisis. Esto requiere que para un atacante no pueda ser posible la observación de las direcciones de origen y destino, frecuencia, longitud, puertos y otras características de tráfico, que se podrían utilizar de algún modo.

- Autenticación: La autenticación no es más que la confirmación de que el emisor es quien dice ser. También es la manera de asegurar que el mensaje no ha sido interceptado y reenviado a su destino original. Este proceso se puede llevar a cabo a través del uso de claves, firmas digitales, PINs; según el protocolo de autenticación utilizado.
- Integridad del mensaje: Tal y como ocurría con la confidencialidad, la integridad de mensaje, asegura que la información del o de los mensajes recibidos no han sido duplicados, insertados, modificados, reordenados o repetidos.
- No repudio: Es el proceso por el cual, los usuarios no puedan negar las responsabilidades de las acciones que ellos llevan a cabo. De esta manera se asegura quién ha enviado el mensaje, y también el emisor puede certificar si el receptor que ha recibido el mensaje es su receptor original.
- Control de acceso: Es la habilidad de limitar y controlar el acceso a una aplicación o a un dispositivo-ordenador. Para ello, en primer lugar se autentica o identifica al usuario. Si ha tenido éxito, se procede a su autorización para poder utilizar los servicios de la aplicación o del dispositivo.
- Disponibilidad: La disponibilidad se refiere a que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo. La cual viene provocada a que algunos ataques provocan la reducción (total o parcial) de la disponibilidad de acceso a un dispositivo o una aplicación.

Estos son lo puntos para clasificar la seguridad. A partir de aquí se puede observar que existen distintas maneras de intentar asegurar la información o el

acceso legal. El uso de palabras clave, a través de claves públicas y privadas, es también de uso habitual para poder autenticar y asegurar las comunicaciones.

1.5.2 Firewalls

La aplicación más utilizada en los últimos años es la archiconocida firewall (cortafuegos). Esta es una combinación de hardware y software que utilizan las empresas y los usuarios para aislar la red privada del exterior, como si fuera una gran barrera (como se muestra en la figura 1.18).

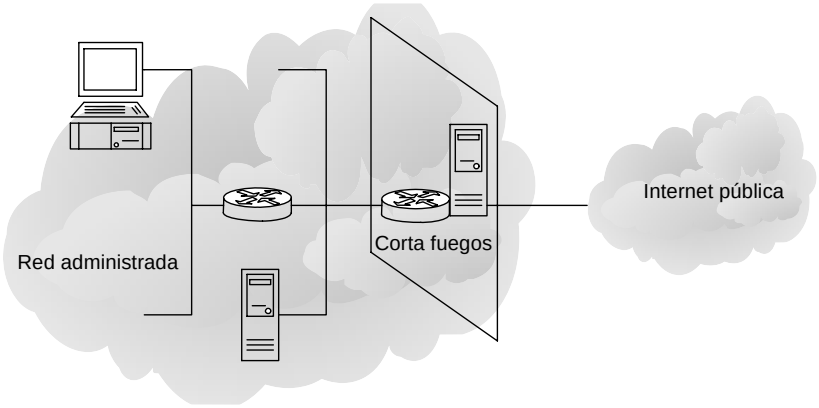

Figura 1.18: Red administrativa con cortafuegos

Un firewall es un mero control de acceso del tráfico entrante/saliente de la red del usuario. En este control, se revisan los datagramas o paquetes que por él pasan y según las reglas que haya impuesto el administrador de la red, actuará en consecuencia: eliminando, reenviado o preguntando al administrador.

1.5.3 Amenazas y contramedidas

Todo elemento de red, ordenador o dispositivo con sistema operativo, es susceptible de padecer intrusiones, virus u otros elementos indeseables.

En la década de las comunicaciones incluso los móviles comienzan a ser parte de la carnaza para los “phreackers” (“hackers” de los sistemas telefónicos).

En esta sección, únicamente daremos un vistazo a las amenazas más comunes y genéricas en el mundo de las redes, y que por lo tanto, son más probables en ambientes de MPLS (Multi-Protocol Label Switching) y ATM.

1.5.3.1 Planear

Cualquier atacante que se precie, utiliza la técnica del espionaje para averiguar información sobre su objetivo. A través de las informaciones que recopila al respecto, puede conseguir planear un ataque mejor.

A nivel de red, en algunos tipos de ataques, se deben conocer las direcciones IP de las máquinas y los puertos abiertos, los sistemas operativos que se utilizan y servicios que ofertan. Por lo tanto, podemos llamar planear a la recopilación de información sobre una red o un sistema.

Esta recopilación se puede llevar a cabo a través de intentos de envíos ping (si contesta afirmativamente quiere decir que la IP existe). En el caso de querer averiguar los puertos abiertos, se puede hacer un “escaneado de puertos”.

Programas como el Nmap tienen este objetivo. Su funcionamiento es muy simple, y sólo consiste en ir preguntando secuencialmente a los números de puerto en una máquina y esperar la respuesta. Con esta técnica se puede averiguar tanto los servicios que presta la máquina como las puertas abiertas que deja.

Muchos de los firewalls actuales tienen la capacidad de poder descubrir este tipo de ataques, y acto seguido avisar al administrador de las peticiones que se hacen desde el exterior.

1.5.3.2 Husmear paquetes

Un husmeador de paquetes es un programa que se ejecuta en un dispositivo asociado a la red. Como se muestra en la figura 1.19, con él los administradores pueden conocer todos los movimientos de la red, con el fin de gestionar y

monitorizar la red. Por otro lado, para los hackers es una gran manera de obtener información. El llamado eavesdropping puede facilitar información privada de los usuarios de la red.

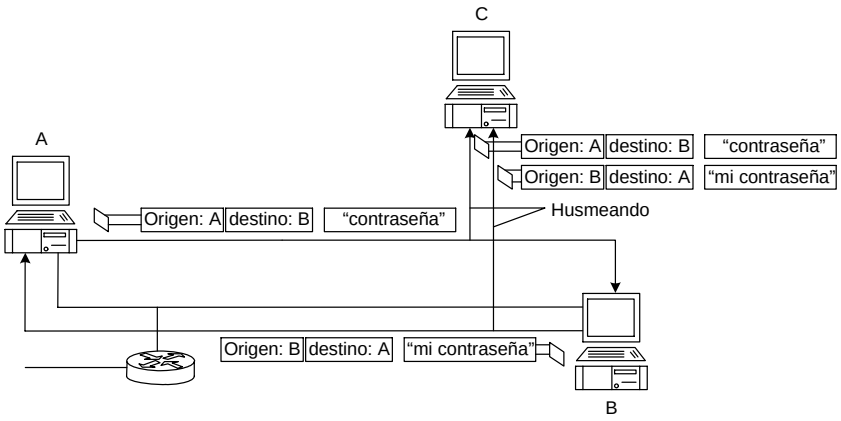

Figura 1.19: Ejemplo de eavesdropping

Con la lectura ilegal de los payloads, se puede obtener tanto información de la red como de direcciones de red, el tipo de aplicaciones-servicios que se ejecutan, pero sobretodo identificadores y contraseñas.

1.5.3.3 Denegación de Servicio

La denegación de servicio o DoS (Denial of Service) tiene por objetivo inutilizar a un elemento de red, un host o una red completa. Este tipo de ataques, consisten en incrementar mucho la carga de trabajo de la infraestructura atacada de modo que no pueda realizar las tareas que tiene encomendadas.

Otro ataque parecido puede ser, enviar fragmentos IP pero nunca los suficientes como para poder completar el datagrama. De tal manera que el servidor va acumulando los fragmentos IP sin poder llegar a procesarlos y llena su memoria.

También existe otro tipo de ataque a terceros, llamado smurf. Este ataque consiste en hacer que un gran número de host inocentes respondan a los

paquetes ICMP de solicitud de eco (ping), con una dirección IP origen falsa. Esto produce que un gran número de paquetes ICMP de respuesta inundaran al host cuya dirección ha sido robada.

1.5.3.4 Spoofing

Es utilizado en los ataques de denegación de servicio. El spoofing o falsificación es hacer creer al agredido que la web, la IP, el e-mail o cualquier tipo de tráfico de red, es real cuando en realidad una tercera persona es la que lo está generando.

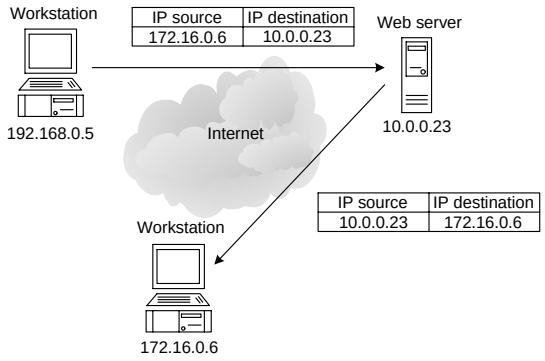

Figura 1.20: Ejemplo de IP spoofing

Se trata del ataque de spooging IP, y es muy sencillo de ejecutar porque cualquier administrador puede cambiar la IP (192.168.0.5) de su interfaz por otra (172.16.0.6), para, por ejemplo, intentar entrar en una restringida a un conjunto de IPs, o como en el caso de la figura, hacer recibir al agredido una información que no había pedido.

Cada vez más, se están buscando maneras para evitar este tipo de ataques y la denegación de servicios que normalmente viene asociada. Estas contramedidas pasan por autenticar que los datos recibidos son verdaderos-originales (como por ejemplo para los e-mails), como también denegando la entrada a cualquier tipo de tráfico broadcast.

1.5.3.5 Secuestro

Como la misma palabra indica, este tipo de ataques consiste en secuestrar una conexión entre dos puntos finales, de tal manera que el atacante pueda hacerse pasar por uno de los dos puntos finales sin que el otro se de cuenta.

El atacante, en algunas ocasiones, actúa como una pasarela de aplicación, enviando información falsa a los usuarios reales de la conexión sin que ellos puedan notarlo.

1.5.4 Los peligros

Los peligros más comunes en infraestructuras ATM y MPLS son:

1.5.4.1 En plano de usuario:

- Observación no autorizada de tráfico de usuarios
- Modificación de tráfico de usuario
- Inserción de tráfico no auténtico
- Suplantación de usuario o conexión
- DoS del plano de usuario
- Falsificación de VPNs

1.5.4.2 En plano de control

- DoS del plano de control
- Ataques a infraestructuras
- Desconfiguración de dispositivos
- Suplantación de servidores para la difusión de información falsa
- Ataques a protocolos de control
- Observación no autorizada de tráfico de control

CAPÍTULO II

REDES PRIVADAS VIRTUALES (VPN)

2.1 Generalidades

Es comúnmente aceptado el hecho que las tecnologías de información en Internet han cambiado la forma como las compañías se mantienen comunicadas con sus clientes, socios de negocios, empleados y proveedores.

La tecnología en nuestros días avanza muy rápidamente y con ello la inseguridad en las redes, por ello surge la tecnología en software y hardware que nos proporcionan ayuda en cuanto a velocidad y seguridad de la información.

2.1.1 Redes Privadas Virtuales (VPN)

Una VPN (Virtual Private Network) es una conexión que tiene la apariencia y muchas de las ventajas de un enlace dedicado pero trabaja sobre una red pública. Para este propósito usa una técnica llamada entunelamiento (tunneling), los paquetes de datos son enrutados por la red pública, tal como Internet o alguna otra red comercial, en un túnel privado que simula una conexión punto a punto.

Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura. También hace universales para su transporte los diferentes protocolos LAN, de allí la característica de multiprotocolo que hace sumamente universal la tecnología de las redes virtuales privadas [10].

La figura 2.1 muestra los distintos escenarios que se pueden manejar con la tecnología de Redes Privadas Virtuales (Dial-Up, Intranet VPN y Extranet VPN).

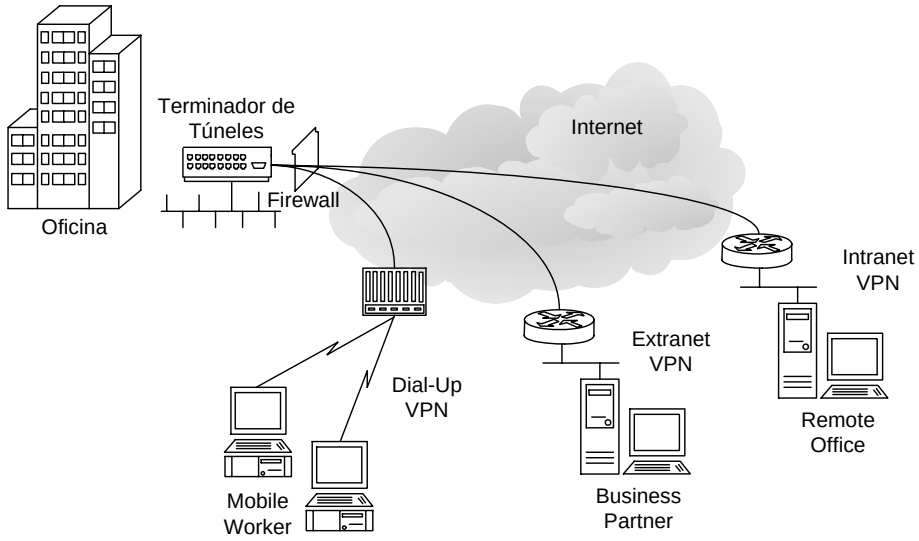

Figura 2.1: Distintas maneras de crear una VPN

Los componentes básicos de un túnel, y que se muestran en la figura 2.2 son:

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

El inicio y la terminación del túnel pueden ser hechos por una amplia variedad de equipos o software.

Un túnel puede ser empezado, por ejemplo, por un usuario remoto con un computador portátil equipado con un modem análogo y un software de conexión telefónica para hacer una VPN, también puede haber un enrutador de una extranet en una oficina remota o en una LAN pequeña.

Un túnel puede ser terminado por otro enrutador habilitado para tal fin, por un switch con esta característica o por un software que haga tal fin.

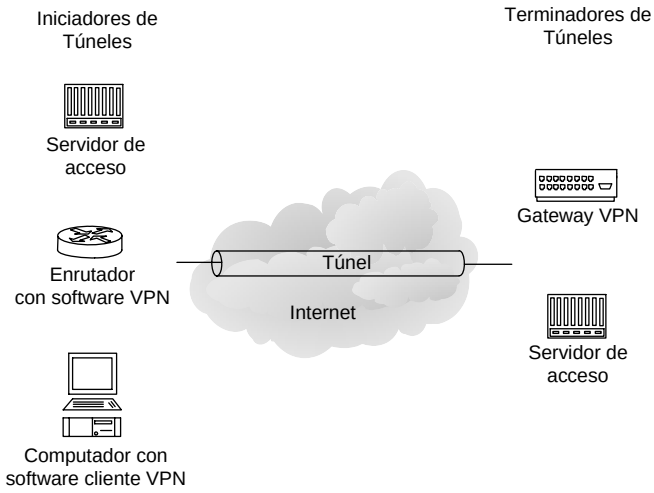

Figura 2.2: Elementos básicos de un túnel VPN

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

En muchos casos las características que le permiten a los dispositivos ser iniciadores o terminadores del túnel se pueden adicionar con una simple actualización del sistema operativo o de sus tarjetas. Una buena solución VPN requiere la combinación de tres componentes tecnológicos críticos: seguridad, control de tráfico y manejo empresarial.

- Seguridad: Dentro de este punto se destacan: el control de acceso para garantizar la seguridad de las conexiones de la red, el cifrado para proteger la privacidad de los datos y la autenticación para poder verificar acertadamente tanto la identidad de los usuarios como la integridad misma de la información.
- Control de tráfico: el segundo componente crítico en la implementación de una efectiva VPN es el control de tráfico que garantice solidez, calidad del servicio y un desempeño veloz. Las comunicaciones en Internet pueden

llegar a ser excesivamente lentas, lo que las convertirían en soluciones inadecuadas en aplicaciones de negocios donde la rapidez es casi un imperativo. Aquí es donde entra a jugar parámetros como la prioridad de los datos y la garantización de ancho de banda.

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

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

2.2 Tipos de Redes Privadas Virtuales

Con la introducción de nuevas tecnologías en las redes de los SP (Service Provider) y nuevos requerimientos de los clientes, las implementaciones de VPN se han convertido más y más complejas y para su solución los servicios de VPN modernos recorren una gran variedad de tecnologías y topologías.

A continuación, exponemos una clasificación según tipos de IP VPN dados en la RFC 2764, una división en categorías según alcance de las VPN para las organizaciones [11].

2.2.1 Según RFC 2764 (“A Framework for IP Based Virtual Private Networks”)

Son definidos cuatro tipos de IP VPN en la RFC 2764:

2.2.2.1 Virtual Leased Lines (VLL)

Brindan enlaces punto a punto orientados a conexión entre los sitios de los clientes. El cliente percibe cada VLL como un enlace (físico) privado dedicado, aunque en realidad está realizado por un túnel IP a través del backbone de la red.

El protocolo de túnel IP utilizado debe ser capaz de transportar cualquier protocolo entre los sitios conectados por las VLL.

2.2.2.2 Virtual Private LAN Segments (VPLS)

Brinda una imitación de LAN entre sitios VPLS, como con las VLLs, un VPLS requiere del uso de túneles IP que sean transparentes a los protocolos transportados por las LAN simuladas. Las LAN pueden ser simuladas usando un engranaje de túneles entre los sitios de los clientes o por el mapeado de cada VPLS a una dirección IP multicast separada.

2.2.2.3 Virtual Private Routed Networks (VPRN)

Simulan redes dedicadas de enrutadores IP entre los sitios de los clientes, aunque una VPRN transporte tráfico IP, esta debe ser tratada como un dominio de enrutamiento separado desde la subyacente red del SP, como la VPRN es probablemente usada por varios clientes asignando direcciones IP. Cada cliente se ve el mismo como el operador de la red y por lo tanto puede asignar las direcciones IP de la manera que desee.

2.2.2.4 Virtual Private Dial Networks (VPDN)

Les permite a los clientes que el SP le aprovisione y gestione los accesos conmutados a su red. En lugar de cada cliente configurar sus propios servidores de acceso y usando secciones PPP (Point-to-Point Protocol) entre un local central y los usuarios remotos, el SP brinda uno o muchos servidores de acceso compartidos.

Usando túneles desde el servidor de acceso del SP hasta un punto de acceso dentro de la red del cliente se transportan secciones PPP para cada VPDN conocido como concentrador de acceso.

2.2.2 Según el alcance de la VPN para la organización

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

La tecnología implica: técnicas de entunelamiento, autenticación, control de acceso, y seguridad de los datos; y los escenarios que se pueden construir son: Intranet VPN (LAN-to-LAN VPN), Acceso Remoto VPN y Extranet VPN [10].

2.2.2.1 Intranet VPN (LAN-to-LAN)

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

Tradicionalmente, para conectar dos o más oficinas remotas de una misma compañía se han necesitado contratar enlaces dedicados Clear Channels o Circuitos Virtuales Permanentes (PVCs) Frame Relay.

Las empresas adoptan diferentes topologías de red WAN (Wide Area Network) para interconectar todos sus sitios remotos, entre estas se encuentran: Enlaces punto-a-punto, de estrella, de malla parcial y de malla completa. Las figuras 2.3, 2.4, 2.5 y 2.6 detallan cada una de las topologías anteriormente mencionadas.

En general, cuando se necesita concentrar tráfico en al menos un nodo, es preferible usar tecnologías como Frame Relay pues solo se necesita un último kilómetro por el cual viajan todos los PVCs contratados con el proveedor de servicio. La mayoría de escenarios de enlaces WAN corporativos tienen más de dos nodos interconectados, por tanto habrá al menos un nodo donde existan al menos dos PVCs compartiendo un último kilómetro, esto sería por ejemplo, en la topología de estrella.

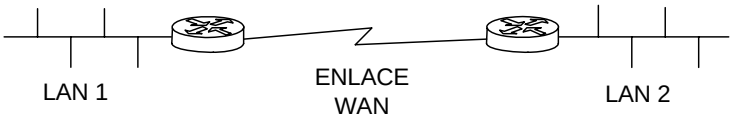

Figura 2.3: Enlace Punto-a-punto

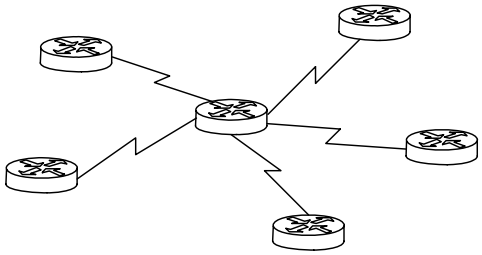

Figura 2.4: Topología en Estrella

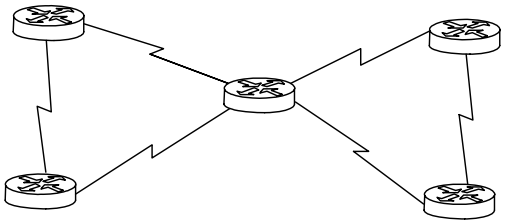

Figura 2.5: Topología de Malla Parcial

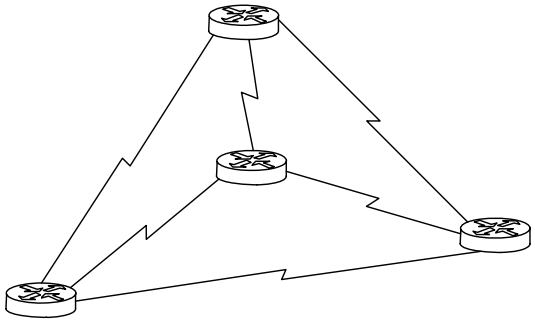

Figura 2.6: Topología de Malla Completa

La ventaja que han sustentado los tradicionales enlaces dedicados es la disponibilidad, sin embargo, estos enlaces también son susceptibles de caídas, y su montaje, en cuanto a hardware se refiere, es tan complejo que es prácticamente imposible cambiar a otro proveedor mientras el enlace se reestablece. Con un escenario LAN-to-LAN VPN, cuando un enlace a Internet de la ISP (Internet Service Provider) que le presta el servicio a la empresa que tiene montada la VPN se cae, la conmutación a otro proveedor es prácticamente transparente para la empresa, ya que el enrutador de frontera de la ISP (que sirve

de gateway de toda la red) se encarga de seleccionar otro enlace que se encuentra arriba.

La figura 2.7 ilustra la conexión de tres oficinas de una misma compañía usando una arquitectura LAN-to-LAN VPN. Nótese que los túneles VPN que aparecen señalados no son enlaces físicos sino lógicos que viajan por Internet. El único equipo que tiene que adquirir la compañía para cada oficina a conectar es un gateway VPN que tiene, por lo general, un puerto LAN (Ethernet o Fast Ethernet) para conectarse a la LAN Corporativa, y un puerto LAN o WAN para conectarse hacia la ISP. Solo se necesita un último kilómetro por oficina, por ahí viajan todos los túneles VPN que se necesiten.

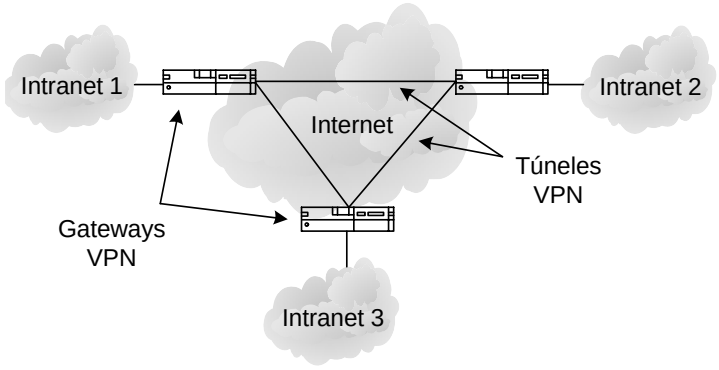

Figura 2.7: Esquema de una solución Intranet VPN (LAN-to-LAN VPN)

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

2.2.2.2 Acceso Remoto VPN

Fue la primera aplicación que se le dio a la emergente tecnología de las VPNs. Consiste en usar cualquier RAS (Remote Access Server) que preste

servicio de conexión a Internet como punto de acceso a una red corporativa también conectada a Internet por medio de un gateway VPN.

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

Con el acceso remoto VPN un trabajador que se haya desplazado a otro país, por ejemplo, y que quiere acceder a la base de datos de su compañía, o al correo interno, o a cualquier otro recurso de su red corporativa, solo tiene que conectarse a Internet con una simple llamada local a la ISP de la ciudad en la que se encuentre, y ejecutar su cliente de marcación VPN. A partir de la versión Windows98, Microsoft incluyó un cliente de marcación VPN que funciona con el protocolo de entunelamiento PPTP (Point-to-Point Tunneling Protocol). Todos los gateways VPN vienen con software VPN clientes para ser instalados en los distintos sistemas operativos presentes en el mercado.

La figura 2.8 muestra la creación de un túnel conmutado VPN usando un cliente PPTP instalado en el computador del trabajador remoto. Nótese que se realizan dos conexiones, una PPP a la ISP, y una PPTP al gateway VPN de la compañía que se encuentra conectado a Internet. La conexión PPP puede ser análoga o digital RDSI (Integrated Services Data Network).

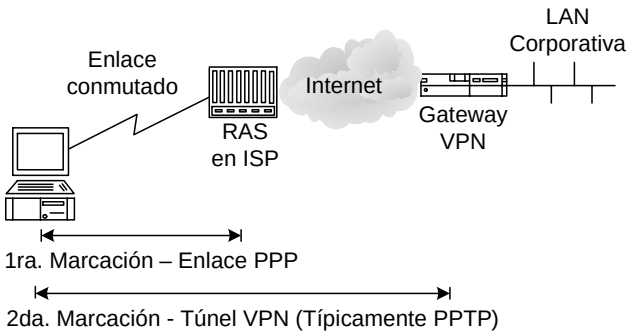

Figura 2.8: Escenario de Acceso remoto VPN

Otra de las grandes ventajas del acceso remoto VPN sobre el tradicional acceso remoto es poder usar tecnologías de acceso de banda ancha como xDSL (Digital Subscriber Line) y cable módem. Para una empresa seria costoso e inconveniente tener un concentrador xDSL en sus instalaciones para permitirle a sus trabajadores teleconmutados el acceso a su red. Mientras que las VPNs usan la infraestructura existente de los proveedores del mercado para accesar a gran velocidad a la red corporativa.

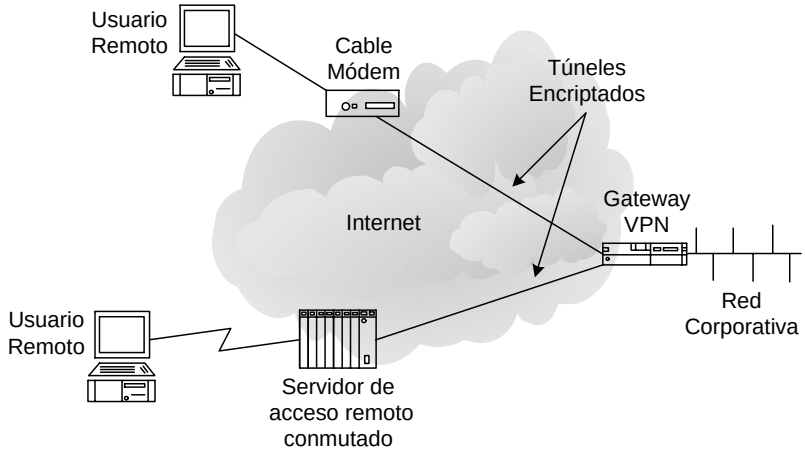

Figura 2.9: Dos montajes típicos de un acceso remoto VPN

La figura 2.9 ilustra dos tipos de accesos remotos VPN, uno de banda ancha, donde el usuario remoto que crea el túnel tiene una conexión cable módem (también aplica xDSL) hacia la ISP; y otro acceso por medio de un módem análogo común, en este caso el usuario remoto podría estar en otra ciudad o incluso en otro país.

2.2.2.3 Extranet VPN

Las empresas necesitan intercambiar información y realizar transacciones no solamente entre sitios de su misma organización sino también con otras compañías. Hoy en día todas las empresas están haciendo presencia en la Internet y esto hace casi imperativo la comunicación con las otras empresas por este medio.

Ciertamente con una arquitectura de Extranet VPNs cada empresa tiene que controlar muy meticulosamente el acceso a los recursos de su red corporativa y a los datos que van a intercambiar con sus socios de negocios. Implementar una topología Extranet VPN implica incrementar la complejidad de los sistemas de control de acceso y de autenticación.

Adicionalmente la tendencia de los mercados hacen que un cambio en la topología se pueda realizar fácilmente, para esto una Extranet VPN debe poder adicionar y eliminar dinámicamente acceso seguro a otras compañías. Tal reconfiguración dinámica es difícil cuando se cuenta con circuitos cerrados dedicados.

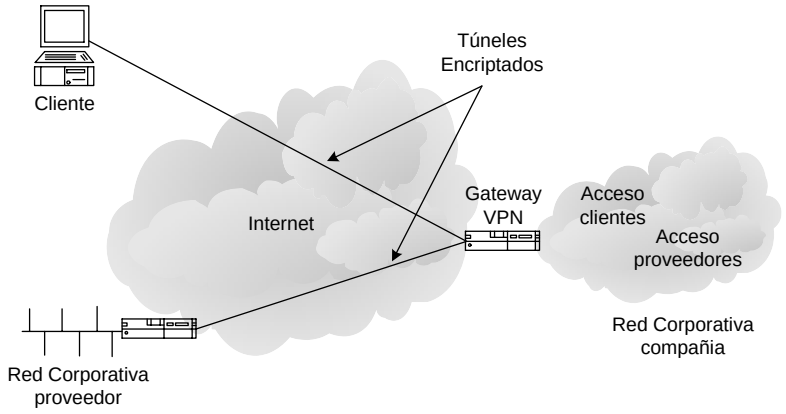

Figura 2.10: Arquitectura Extranet VPN, clasificando el acceso según privilegios de los clientes VPNs remotos

La presencia de una compañía en Internet y el uso de la arquitectura de Extranet VPN, hace posible crear conexiones dinámicas seguras a otras redes sin necesidad de cambiar la infraestructura física. Ejemplos de conexiones dinámicas seguras y que son conocidos como Extranet VPNs se muestran en la figura 2.10

Al igual que en una arquitectura LAN to LAN VPN es necesario un gateway VPN que se instala en la frontera de la red corporativa. Los túneles son creados a través de Internet entre este gateway y el gateway VPN situado en la red de la otra empresa.

De otro modo un cliente VPN en un computador independiente podría accesar a la red corporativa como un cliente usando cualquier acceso remoto.

En la actualidad la mayoría de los gateways VPN pueden establecer múltiples túneles seguros a múltiples empresas. Sin embargo, es importante que una empresa no sea capaz de obtener acceso a la información de otra compañía que está accediendo por medio de Extranet VPNs.

Un nivel más de seguridad puede ser adicionado ubicando recursos exclusivos a cada una de las compañías que va a acceder a la red de interés en diferentes servidores.

2.3 CLASIFICACION DE LAS VPN

De los posibles modelos de VPN dos han ganado un amplio uso:

- El modelo superpuesto (*overlay*), donde el SP simula líneas dedicadas para el cliente.
- El modelo par a par (*peer to peer*) donde el SP y el usuario intercambian información de enrutamiento de Nivel 3, con la cual el proveedor transporta los datos entre los sitios del usuario por un trayecto óptimo en lo cual el usuario no interviene [11].

2.3.1 VPN Overlay

Es aquella VPN en donde el SP emula una línea virtual entre los sitios remotos del cliente [12]. Este modelo puede incluir tanto túneles GRE (Generic Routing Encapsulation) como IPSec (IP Security).

El modelo superpuesto (overlay) se puede comprender de una forma mejor porque en el existe una clara separación entre las responsabilidades del cliente y del SP. El SP brinda al cliente una configuración que simula líneas dedicadas llamadas circuitos virtuales (VC, Virtual Circuit), los que pueden estar disponibles

constantemente (PVC) o establecidos bajo demanda (SVC, Switched Virtual Circuit) [11].

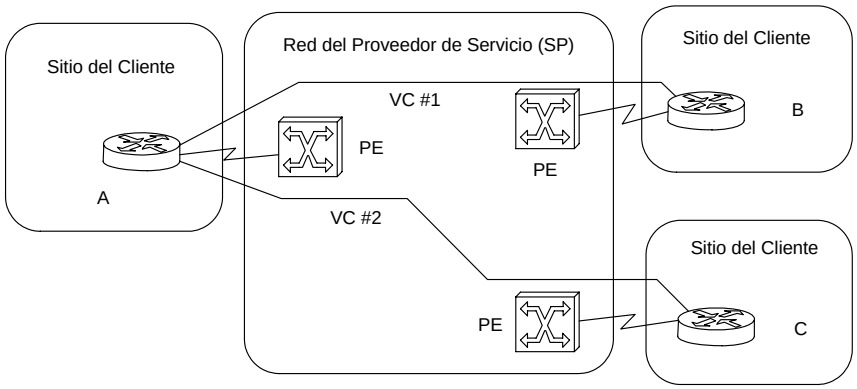

Figura 2.11: Ejemplo de topología de red VPN superpuesta

Como observamos en la Figura 2.11 el cliente establece comunicación entre sus enrutadores sobre los VCs suministrados por el SP. La información de los protocolos de enrutamiento siempre es intercambiada entre los dispositivos del cliente por lo que el SP desconoce la topología interna de la red del cliente.

2.3.2 VPN Peer-to-Peer

En este modelo el SP y su cliente intercambian información de enrutamiento en cada interconexión que poseen entre los routers PE (Provider Edge) y CE (Customer Edge).

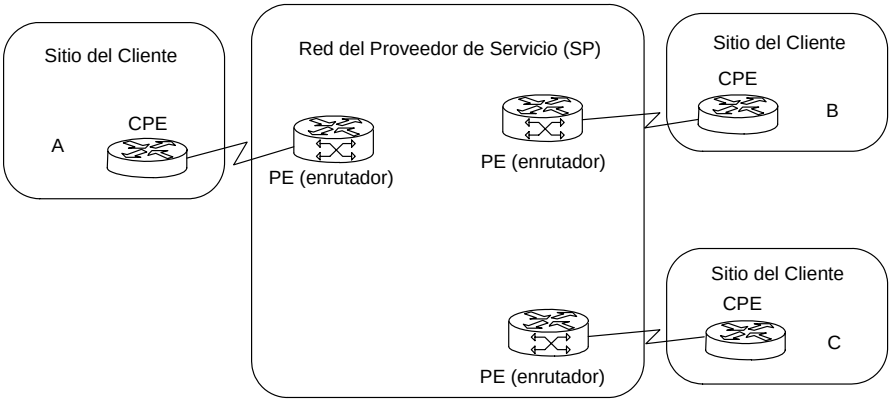

Figura 2.12: Ejemplo de VPN par a par

El SP es el responsable de redistribuir y suministrar la información de enrutamiento óptima de los otros CE de la misma VPN.

Como el equipamiento del SP puede ser compartido entre una o más VPNs, es éste quien debe aislar el tráfico de los distintos clientes. En el modelo par a par el PE es un enrutador que intercambia directamente información de Nivel 3 con el CPE [12]. La figura 2.12 muestra un ejemplo de VPN par a par.

2.4 Modelos de Entunelamiento

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

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

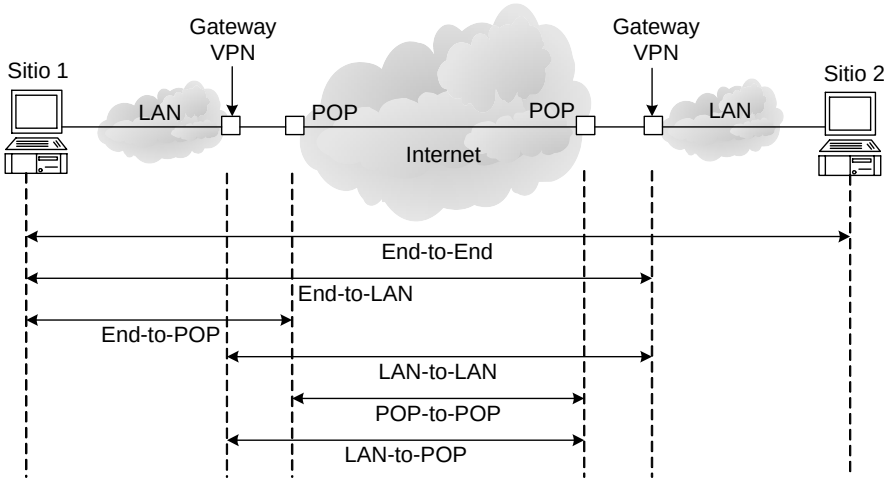

Figura 2.13: Modelos de Entunelamiento VPN

Dado que un túnel VPN se compone de dos terminadores, se pueden obtener seis tipos de modelos de seguridad derivados de la posible combinación de las diferentes localizaciones: End-to-End, End-to-LAN, End-to-POP, LAN-to-LAN, LAN-to-POP y POP-to-POP [10], en la figura 2.13 se notan cada uno de ellos.

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

En el modelo End-to-LAN, el túnel comienza en un host y termina en el perímetro de una LAN en la cual reside el host destino. Un dispositivo VPN localizado en el perímetro de la red es el responsable de la negociación y obtención de los servicios de seguridad de los host remotos. De esta manera, la seguridad de un gran número de dispositivos en una red corporativa puede ser manejada en un único punto, facilitando así la escalabilidad del mismo. Dado que la red corporativa es considerada un sitio seguro, comúnmente no hay necesidad de encriptar la información que transita dentro de ella. La mayoría de implementaciones de acceso remoto VPN trabajan con este modelo.

El modelo de entunelamiento End-to-POP es aquel en el cual un host remoto termina el túnel en un POP de la ISP. Un dispositivo VPN o un equipo con funciones de terminador VPN y que se encuentra en la red de la ISP es el responsable por la negociación y concesión de los servicios de seguridad. La entrega de los datos desde el POP hasta el host destino es por lo general asegurada con infraestructura física, la cual separa el tráfico del resto de la red

pública. Por lo general en este caso el ISP administra los permisos y controla el acceso según las directivas de los administradores de red de las empresas clientes. La arquitectura de acceso remoto VPN también usa este modelo.

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

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

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

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

2.5 Requisitos de una VPN

Aunque es posible dotar a una VPN de servicios de valor añadido, el servicio más básico ofrecido por una red privada virtual consiste en [13]:

- El tráfico de cada VPN está totalmente aislado del resto del tráfico que circula por la red.
- Como consecuencia directa, cada VPN puede emplear direccionamiento privado. De este modo, una empresa que quiere conectar varias sedes mediante una VPN no necesita cambiar su plan de direccionamiento ni pedir direcciones públicas.
- El intercambio de información entre sedes de una VPN debe ser seguro. La empresa puede confiar la seguridad al operador que le ofrece el servicio o puede emplear sus propios mecanismos de seguridad.
- El operador debe cumplir unos requisitos de calidad de servicio para el tráfico que circula por la VPN. Estos requisitos se refieren tanto a la disponibilidad como ancho de banda, latencia, etc.

2.6 Tecnologías empleadas en las VPN

Básicamente, y desde el punto de vista del modelo OSI, se puede crear una VPN usando tecnologías de capa 2 (enlace de datos) y de capa 3 (red). Dentro de la primera categoría están PPTP y L2TP, y en la segunda se encuentra IPSec.

2.6.1 PPTP (Point-to-Point Tunneling Protocol)

Es quizá el protocolo más sencillo de entunelamiento de paquetes. Es usado, en general, por pequeñas empresas para realizar sus VPNs LAN-to-LAN, y en topologías de acceso remoto, para trabajadores teleconmutados (teleworkers), tales como vendedores externos o trabajadores que se mantienen en constante movimiento por fuera de sus oficinas [10].

El protocolo más comúnmente usado para acceso conmutado a Internet es el protocolo punto-a-punto (PPP). PPTP se soporta sobre toda la funcionalidad que PPP le brinda a un acceso conmutado para construir sus túneles a través de Internet. PPTP encapsula paquetes PPP usando una versión modificada del Protocolo de Encapsulamiento Ruteado Genérico (GRE, Generic Routing Encapsulation). Dado lo anterior, PPTP no solo es capaz de encapsular paquetes IP, sino IPX y NETBEUI, los protocolos de red local más usados. La figura 2.14 muestra una conexión PPP entre un host y un RAS. Como se puede ver, es una

conexión sencilla punto a punto donde lo primero que se realiza es una autenticación sencilla previa al envío y recibo de tramas PPP de datos

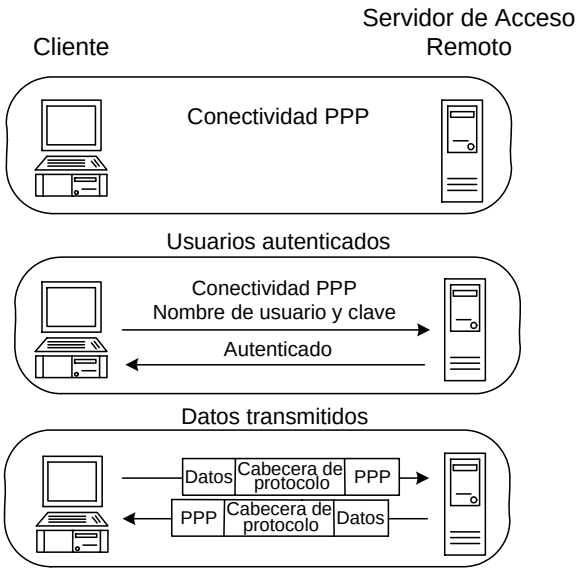

Figura 2.14: Conexión PPP típica entre un host y un RAS

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

2.6.1.1 Relación entre PPP y PPTP.

PPP es el protocolo más comúnmente usado para acceso a Internet, prácticamente el único, además es usado en algunos enlaces seriales punto a punto WAN. PPP trabaja en la capa 2 del modelo OSI, la capa de enlace de datos, e incluye métodos para encapsular varios tipos de datagramas para ser transferidos sobre enlaces seriales.

PPP tiene dos juegos de protocolos: el Protocolo de Control de Enlace (LCP) que se encarga de las labores de establecimiento, configuración y prueba de la conexión y una serie de Protocolos de Control de Red (NCPs) para el establecimiento y configuración de los diferentes protocolos de capa 3 [10].

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

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

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

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

Luego que el enlace PPP es creado, el protocolo PPTP define dos diferentes tipos de paquetes: paquetes de control y paquetes de datos, cada uno de los cuales es asignado a diferentes canales lógicos. PPTP separa los canales de control y de datos usando un flujo de control que corre sobre TCP y un flujo de

datos que está encapsulado con cabeceras IP usando GRE. La conexión TCP es creada entre el cliente y el servidor PPTP. Esta conexión es usada para intercambiar mensajes de control.

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

Después de que el túnel PPTP se ha establecido, los datos del usuario son transmitidos entre el cliente y el servidor PPTP. Estos datos son transmitidos en datagramas IP contenidos dentro de los paquetes PPP. Los datagramas IP son creados usando una versión modificada del protocolo GRE (Generic Routing Encapsulation); esta modificación consiste en incluir un identificador de los host que puede ser usado para controlar los privilegios de acceso y la capacidad de reconocimiento, la cual es usada para monitorear la rata de transferencia a la cual los paquetes están transmitiéndose en el túnel.

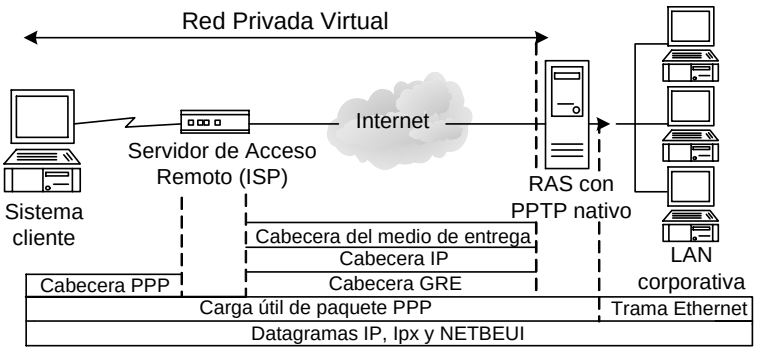

Figura 2.15 Estructura de un túnel PPTP

La cabecera GRE es usada para encapsular el paquete PPP dentro del datagrama IP. La información útil del paquete (Payload) es esencialmente el paquete PPP original enviado por el cliente. Dado que PPTP opera con un

protocolo de capa 2, debe incluir una cabecera que depende del medio en el cual el túnel está transmitiendo, esta puede ser Ethernet, Frame Relay o PPP. La figura 2.15 muestra la estructura en los diferentes sitios de un túnel de un paquete IP usando encapsulacion PPTP desde el sistema cliente hasta la LAN corporativa.

2.6.1.2 Túneles

PPTP permite a los usuarios y a las ISPs crear varios tipos de túneles, basados en la capacidad del computador del usuario final y en el soporte de la ISP para implementar PPTP. De esta manera, el computador del usuario final determina el lugar de terminación del túnel, bien sea en su computador, si está corriendo un cliente PPTP, o en el servidor de acceso remoto de la ISP, si su computador solo soporta PPP y no PPTP.

En este segundo caso el servidor de acceso de la ISP debe soportar PPTP, a diferencia del primer caso, donde la ISP no se involucra en ningún proceso de entunelamiento de datos.

Dado lo anterior, los túneles se pueden dividir en dos clases, voluntarios y permanentes.

Los túneles voluntarios son creados por requerimiento de un usuario y para un uso específico. Los túneles permanentes son creados automáticamente sin la acción de un usuario y no le permite escoger ningún tipo de privilegio.

En los túneles voluntarios, la configuración del mismo depende del usuario final, cuando se usan túneles de este tipo, el usuario puede simultáneamente acceder a Internet y abrir un túnel seguro hacia el servidor PPTP. En este caso el cliente PPTP reside en el computador del usuario. Los túneles voluntarios proveen más privacidad e integridad de los datos que un túnel permanente. La figura 2.16 muestra un escenario de túneles voluntarios creados desde dos clientes distintos a un mismo servidor PPTP a través de Internet.

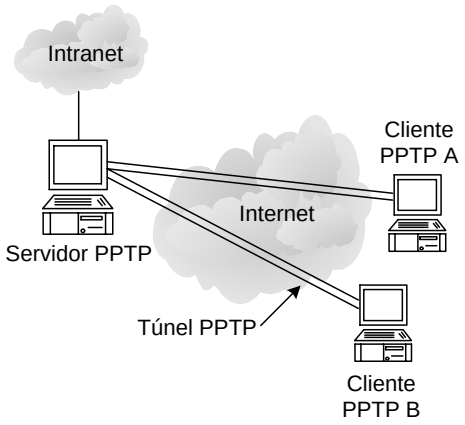

Figura 2.16: Túneles Voluntarios

Los túneles permanentes son creados sin el consentimiento del usuario, por lo tanto, son transparentes para el mismo. El cliente PPTP reside en el servidor de acceso remoto de la ISP al que se conectan los usuarios finales. Todo el tráfico originado desde el computador del usuario final es reenviado por el RAS sobre el túnel PPTP.

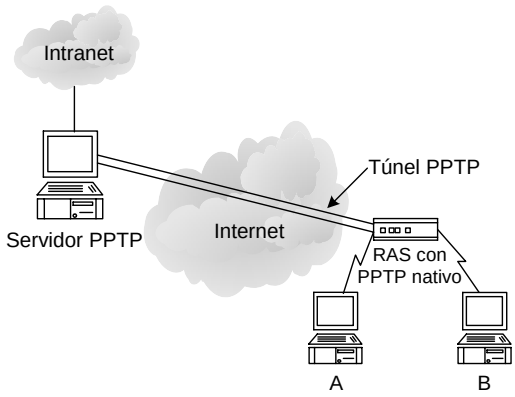

Figura 2.17: Túneles Permanentes

En este caso la conexión del usuario se limita solo a la utilización del túnel PPTP, no hay acceso a la red pública (Internet) sobre la cual se establece el túnel. Un túnel permanente PPTP permite que múltiples conexiones sean transportadas sobre el mismo túnel. La figura 2.17 muestra un túnel permanente

entre un RAS con capacidad para encapsular sesiones PPP usando PPTP y por medio del cual van multiplexadas dos sesiones de clientes A y B.

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

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

Los túneles permanentes se dividen en estáticos y dinámicos. Los túneles estáticos son aquellos que requieren equipos dedicados y su configuración es manual. En este tipo de túneles el usuario final tiene a su disposición varios RAS, los cuales tienen establecidos diferentes túneles a diferentes servidores PPTP. Por ejemplo, si un usuario necesita hacer una VPN a su oficina regional ubicada en la ciudad A tiene que marcar un número X, pero si ese mismo usuario quiere hacer una VPN con su oficina en una ciudad B, tiene que marcar un número Y. Los túneles permanentes dinámicos usan el nombre del usuario para determinar el túnel asociado con él, es decir que se encargan de aprovechar mejor los recursos y el usuario puede marcar al mismo número para establecer túneles a diferentes sitios.

2.6.1.3 Entunelamiento LAN-to-LAN

Originalmente PPTP fue desarrollado pensando en brindar soluciones de acceso remoto VPN, es decir, proveer acceso conmutado seguro a redes locales corporativas vía Internet.

La implementación de Microsoft para entunelamiento LAN-to-LAN exige la presencia de dos servidores PPTP que tienen la función de hacer de gateways seguros de las dos redes locales. Sin embargo, la gran desventaja de usar PPTP en topologías LAN-to-LAN es la inseguridad inherente a la arquitectura del protocolo. En efecto, la autenticación y el cifrado son controlados por protocolos que ofrecen un nivel muy bajo de confiabilidad. La figura 2.18 muestra una topología de red LAN-to-LAN entre una pareja de servidores PPTP usando un túnel PPTP sobre Internet, para los usuarios tanto de la LAN corporativa A como de la B el túnel es transparente, y a nivel lógico se trabaja como en una única red local [10].

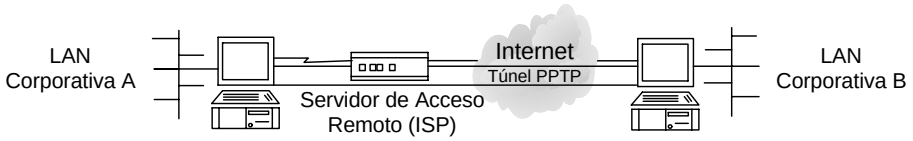

Figura 2.18: Topología LAN-to-LAN usando un túnel PPTP

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

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

2.6.2 L2TP (Layer 2 Tunneling Protocol)

Dado que L2TP es un protocolo de capa 2, ofrece a los usuarios la misma flexibilidad de PPTP de soportar otros protocolos aparte de IP, tales como IPX y NETBEUI. Puesto que L2TP usa PPTP en enlaces conmutados, incluye mecanismos de autenticación nativos de PPP como PAP y CHAP.

2.6.2.1 Componentes Básicos de un Túnel L2TP

2.6.2.1.1 Concentrador de acceso L2TP (LAC)

Un LAC es un nodo que se encuentra en un punto extremo de un túnel L2TP. El LAC se encuentra entre un LNS y un sistema remoto y reenvía los paquetes a y desde cada uno. Los paquetes enviados desde el LAC hasta el LNS van tunelizados. En algunas ocasiones el sistema remoto actúa como un LAC, esto se presenta cuando se cuenta con un software cliente LAC [10].

2.6.2.1.2 Servidor de Red L2TP (LNS)

Un LNS es un nodo que se encuentra en un punto extremo de un túnel L2TP y que interactúa con el LAC, o punto final opuesto. El LNS es el punto lógico de terminación de una sesión PPP que está siendo tunelizada desde un sistema remoto por el LAC.

2.6.2.1.3 Túnel

Un Túnel existe entre una pareja LAC-LNS. El túnel consiste de una conexión de control y de ninguna o más sesiones L2TP. El túnel transporta datagramas PPP encapsulados y mensajes de control entre el LAC y el LNS.

2.6.2.2 Topología de L2TP

La figura 2.19 describe un escenario típico L2TP. El objetivo es tunelizar tramas PPTP entre un sistema remoto o un cliente LAC y un LNS localizado en la LAN corporativa.

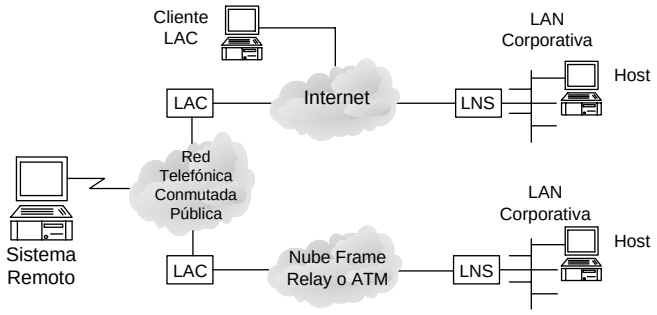

Figura 2.19: Distintos escenarios de túneles L2TP

El sistema remoto inicia una conexión PPP a través de la red de telefonía pública conmutada a un LAC. El LAC luego tuneliza la conexión PPP a través de Internet o una nube Frame Relay o ATM a un LNS por donde accesa a la LAN remota corporativa. La dirección del sistema remoto es dada desde la LAN corporativa por medio de una negociación PPP NCP. La autenticación, autorización y accounting puede ser provista por el dominio de la red corporativa remota como si el usuario estuviera conectado a un servidor de acceso de la red directamente.

Un cliente LAC (un host que corre L2TP nativo) puede también crear un túnel hasta la LAN corporativa sin usar un LAC externo. En este caso, el host tiene un software cliente LAC y previamente ha estado conectado a la red pública, tal como Internet. Una conexión PPP “virtual” es luego creada y el software cliente LAC hace un túnel hasta el cliente LNS. Como en el caso anterior, el direccionamiento, la autenticación, la autorización y el acounting pueden ser provistos por el dominio de la LAN corporativa remota.

2.6.2.3 Estructura del Protocolo L2TP

L2TP utiliza dos tipos de mensajes, los mensajes de control y los mensajes de datos. Los mensajes de control son usados en el establecimiento, mantenimiento y finalización de túneles y llamadas. Los mensajes de datos son usados para encapsular tramas PPP que está siendo transportadas sobre el túnel. Los mensajes de control utilizan un canal de control confiable con el cual L2TP garantiza la entrega. Los mensajes de datos no son retransmitidos cuando ocurren pérdidas de paquetes.

La figura 2.20 muestra la relación de las tramas PPP y los mensajes de control con los canales de datos y control L2TP respectivamente. Las tramas PPP son transportadas sobre un canal de datos no confiable y son encapsuladas primero por una cabecera L2TP y luego por una cabecera de transporte de paquetes que pueden ser UDP, Frame Relay o ATM. Los mensajes de control son enviados sobre un canal de control L2TP confiable, el cual transmite paquetes en banda sobre el mismo transporte de paquetes.

Para esto se requiere que números de secuencia estén presentes en todos los mensajes de control. Los mensajes de datos pueden usar esos números de secuencia para reordenar paquetes y detectar pérdidas de los mismos.

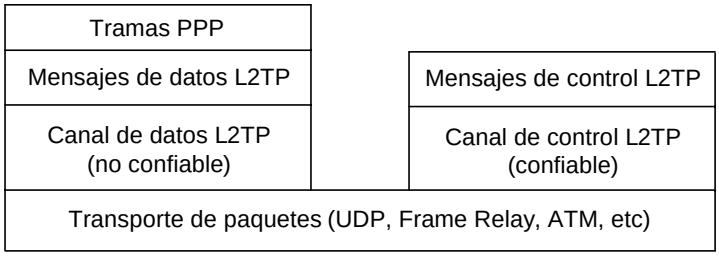

Figura 2.20: Estructura del protocolo L2TP

2.6.2.3.1 Formato de una Cabecera L2TP

Los paquetes L2TP para el canal de control y el canal de datos comparten un formato de cabecera común. La figura 2.21 muestra el formato de una cabecera L2TP.

T	L	x	x	S	c	O	P	x	x	x	x	Ver	Length (Opc)
Tunnel ID													Session ID
Ns (Opc)													Nr (Opc)
Offset Size (Opc)													Offset padding (Opc)

Figura 2.21: Formato de una cabecera L2TP

El bit T (type), indica el tipo de mensaje, es 0 para un mensaje de datos y 1 para un mensaje de control.

Si el bit L (length) es 1, el campo Longitud está presente. Este bit debe estar puesto en 1 para los mensajes de control.

Los bits x son reservados para futuras extensiones. Todos los bits reservados deben ser puestos en 0 para los mensajes salientes y deben ser ignorados por el receptor.

Si el bit S (sequence) de Secuencia (S) esta puesto en 0, el Ns y Nr están presentes. El bit S debe estar puesto en 1 para los mensajes de control.

Si el bit O (Offset) es 1, el campo de tamaño Offset está presente. El bit O debe ser puesto en 0 para los mensajes de control.

Si el bit P (Priority) es 1, los mensajes de datos deben recibir un trato preferencial en las colas locales y en la transmisión. Los requerimientos echo LCP usados como keepalive para el enlace deben generalmente ser enviados con este bit puesto en 1 dado que un intervalo de tiempo grande originado por una conexión local puede originar una demora en los mensajes keepalive ocasionando una pérdida innecesaria del enlace. Esta característica es solamente usada por los mensajes de datos. El bit P debe ser puesto en 0 para todos los mensajes de control.

El campo Ver debe ser 2 e indicar la versión de la cabecera L2TP de los mensajes de datos. Los paquetes recibidos con un campo Ver desconocido deben ser descartados.

El campo Length indica la longitud total del mensaje en octetos.

El campo Tunnel ID sirve como identificador para el control de conexión. Los túneles L2TP son nombrados por identificadores que tienen significado local únicamente. Es decir, el mismo túnel.

El campo Session ID indica el identificador para una sesión dentro del túnel. Al igual que los identificadores de túnel, las sesiones L2TP son nombradas por identificadores que tienen únicamente significado local.

El campo Ns indica el número de secuencia para los mensaje de datos y de control.

El campo Nr indica el número de secuencia esperado en el siguiente mensaje de control a ser recibido. En los mensajes de datos el campo Nr es reservado, y si es presente debe ser ignorado.

Si el campo Offset Size está presente, especifica el número de octetos después de la cabecera L2TP, a partir de los cuales la carga útil de datos es esperada a que inicie o a que se encuentre.

2.6.2.4 Operación del Protocolo

Para tunelizar una sesión PPP con L2TP se necesita llevar a cabo dos pasos, el primero, el establecimiento de una conexión de control para el túnel y el segundo, el establecimiento de una sesión respondiendo al requerimiento de una llamada entrante o saliente.

El túnel y su correspondiente conexión de control deben ser establecidos antes que una llamada entrante o saliente sea iniciada. Una sesión L2TP debe ser establecida antes que L2TP pueda empezar a tunelizar tramas PPP. Múltiples sesiones pueden existir a través de un túnel único y múltiples túneles pueden existir entre el mismo LAC y LNS [10].

La figura 2.22 ilustra la relación que puede existir entre un LAC y un LNS, claramente se notan los puntos terminales de un enlace PPP de una sesión L2TP, de una conexión de control L2TP y del túnel en sí.

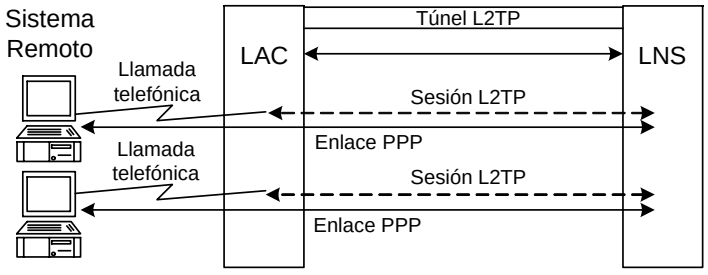

Figura 2.22: Entunelamiento de tramas PPP usando L2TP

2.6.3 IPSec (IP Security)

En IPv4 no se desarrollaron mecanismos de seguridad inherentes al protocolo, por tanto, protocolos y procedimientos adicionales a IPv4 fueron necesarios para brindar servicios de seguridad a los datos.

IPSec es un conjunto de protocolos diseñados para proveer una seguridad basada en criptografía robusta para IPv4 e IPv6, de hecho IPSec está incluido en IPv6. Entre los servicios de seguridad definidos en IPSec se encuentran, control de acceso, integridad de datos, autenticación del origen de los datos, protección antirepetición y confidencialidad en los datos. Entre las ventajas de IPSec están la modularidad del protocolo, ya que no depende de un algoritmo criptográfico específico.

2.6.3.1 Componentes de IPSec

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

2.6.3.1.1 Protocolos de Seguridad

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

AH es un protocolo que añade una nueva cabecera justo después de la cabecera IP original. AH provee autenticación del origen de los datos e integridad de los mismos, también provee integridad parcial para prevenir ataques de

repetición. Este protocolo es apropiado cuando se requiere autenticación en vez de confidencialidad [10].

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

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

2.6.3.1.2 Asociaciones de Seguridad (SAs)

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

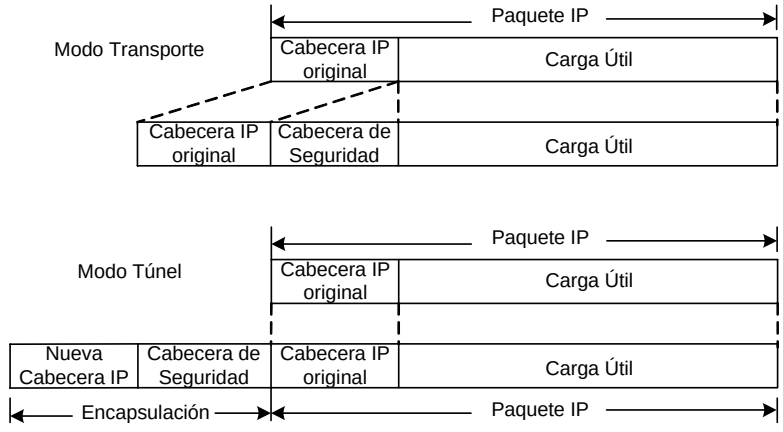

Figura 2.23: Estructura del paquete IP en modo de Transporte y Túnel

La figura 2.23 muestra los dos modos en los cuales un protocolo de seguridad puede operar: transporte y túnel; la diferencia radica en la manera

como cada uno de ellos altera el paquete IP original. El modo de transporte es diseñado para proteger los protocolos de capas superiores tales como TCP y UDP. En modo túnel, el paquete IP original se convierte en la carga útil de un nuevo paquete IP. Esto le permite al paquete IP inicial, “ocultar” su cabecera IP para que sea encriptada, considerando que el paquete IP externo sirve de guía a los datos a través de la red.

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

2.6.3.1.3 Bases de Datos de Seguridad

IPSec trabaja con dos bases de datos de seguridad, en una se encuentran las políticas de seguridad y en la otra las asociaciones de seguridad, SPD (Security Policy Database) y SAD (Security Association Database) respectivamente. El administrador de políticas define un conjunto de servicios de seguridad para ser aplicados al tráfico IP tanto entrante como saliente. Esas políticas son guardadas en las SPDs y son usadas por las SAs cuando éstas se crean. Todas las SAs son registradas en la SAD.

2.6.3.1.4 Authentication Header (AH)

El protocolo de cabecera de autenticación AH es usado para propósitos de autenticación de la carga útil IP a nivel de paquete por paquete, esto es autenticación de la integridad de los datos y de la fuente de los mismos.

Como el término autenticación indica, el protocolo AH se asegura que los datos entregados dentro del paquete IP son auténticos, es decir, que han arribado a su destino sin ninguna modificación. AH también provee de un mecanismo de protección opcional antirepetición de paquetes IP. Sin embargo,

AH no protege la confidencialidad de los datos, es decir, no recurre a ningún tipo de cifrado de los mismos.

El protocolo AH define como un paquete IP sin protección es convertido en uno nuevo que contiene información adicional y que brinda autenticación. El elemento fundamental usado por AH es una cabecera de autenticación como se muestra en la figura 2.24. El nuevo paquete IP es formado insertando la cabecera de autenticación, bien sea, después de la nueva cabecera IP o después de la cabecera IP original modificada según sea el modo en el cual trabaje la SA.

Cuando la cabecera de autenticación es insertada, la cabecera IP que la precede deberá indicar que la próxima cabecera que se encuentra es la cabecera de autenticación y no la carga útil del paquete original. Cuando la cabecera de autenticación es insertada, la cabecera IP que la precede deberá indicar que la próxima cabecera que se encuentra es la cabecera de autenticación y no la carga útil del paquete original.

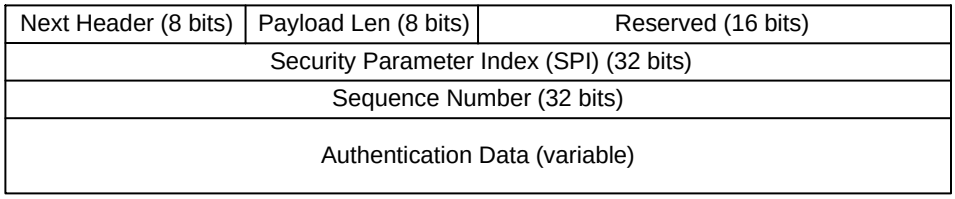

Figura 2.24: Formato de la cabecera de autenticación

La cabecera de autenticación contiene seis campos:

- Next Header: El campo Next Header es un campo de ocho bits que identifica el tipo de protocolo de la carga útil del paquete IP original.
- Payload Len: El campo Payload Len es un campo de ocho bits que especifica la longitud de la cabecera de autenticación.
- Reserved: El campo Reserved se encuentra reservado para uso futuro, actualmente debe ser puesto en 0.

- Security Parameter Index: El campo Security Parameter Index es un número arbitrario de 32 bits. Este valor es usado junto con la dirección IP de destino y el tipo de protocolo IPSec (en este caso, AH) únicamente para identificar la SA para este paquete IP. El valor SPI es escogido por el sistema destino cuando la SA es establecida.
- Sequence Number: El campo Sequence Number es un campo de 32 bits que mantiene un incremento monotónico de la secuencia de paquetes IPSec. Comienza en 0 cuando la SA es establecida y se incrementa por cada paquete IP saliente que usa esta SA. Este campo se usa como un mecanismo de protección antirepetición.
- Authentication Data: El campo Authentication Data es un campo de longitud variable que contiene el valor de chequeo de integridad ICV (Integrity Check Value) para este paquete IP. El ICV es calculado con el algoritmo seleccionado por la SA y es usado por el recepto para verificar la integridad del paquete IP entrante.

2.6.3.1.5 Encapsulating Security Payload (ESP)

El protocolo ESP IPSec provee autenticación, confidencialidad de los datos por medio de cifrado y una protección opcional antirepetición para los paquetes IP.

La autenticación y el cifrado son también opcionales, pero al menos una de ellas debe ser empleada; de lo contrario, este protocolo carecería de fundamento. La confidencialidad es lograda por medio de técnicas de cifrado. Los algoritmos de cifrado empleados a los paquetes IP son definidos por la SA sobre la cual los paquetes son enviados.

Al igual que con AH varios campos adicionales son insertados en el paquete IP para que presten los servicios mencionados anteriormente. Muchos de esos campos tienen el mismo significado que en AH, pero la diferencia es que éstos se encuentran a lo largo del paquete IP, algunos en la cabecera ESP, otros en el trailer ESP y otro esta en el segmento de autenticación ESP. La figura 2.25 muestra la conformación de un paquete IP después que se ha procesado con el

protocolo IPSec ESP, se observan la ubicación de los campos dentro de cada uno de los segmentos del nuevo paquete.

La cabecera ESP se encuentra después de la nueva cabecera IP o después de la cabecera IP original modificada, esto dependiendo del modo. El trailer ESP se encuentra al final del paquete IP original y el segmento de autenticación ESP se encuentra después de el trailer. Si la autenticación no es aplicada, el segmento de autenticación ESP no es añadido. Si el cifrado es aplicado, cada una de las partes desde el final de la cabecera ESP hasta el final de el trailer ESP son encriptadas.

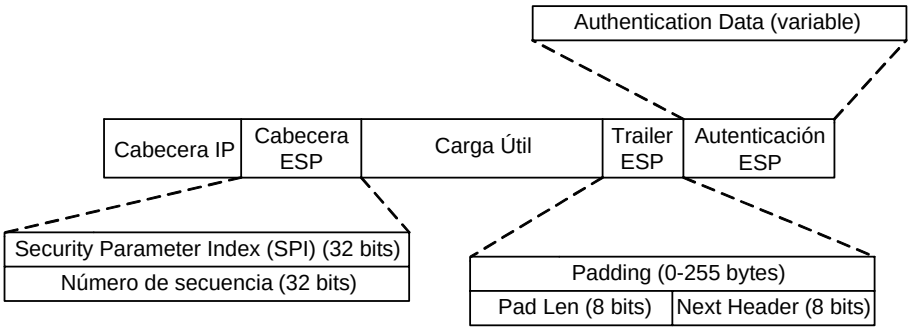

Figura 2.25: Nuevo paquete IP procesado con ESP

Al igual que en el protocolo AH, los campos SPI, Sequence Number, Next Header y Authentication Data, se encuentran definidos a lo largo del nuevo paquete IP. También se encuentran otros dos campos, el campo Padding es usado para rellenar los datos a ser encriptados y completar un límite de 4 bytes, por tanto este campo es de longitud variable. El campo Pad Len especifica la longitud del relleno para poder luego ser eliminado después de que los datos son desencriptados.

Existe un problema cuando la longitud del nuevo paquete IP, debido a la adición de una cabecera ESP y de unos campos de relleno y de autenticación, resulta ser mas grande que el tamaño máximo definido para el paquete. Cuando esto pasa, los paquetes IP son fragmentados por el dispositivo emisor. Debido a

que el procesamiento ESP debe ser aplicado únicamente a paquetes IP enteros y no fragmentados, si un paquete IP entrante ha llegado fragmentado, el gateway de seguridad que lo recibe debe reensamblar los fragmentos para formar de nuevo el paquete IP antes de que sean procesados por ESP.

2.6.3.1.6 Internet Key Exchange (IKE)

Los protocolos ESP y AH no explican cómo las asociaciones de seguridad son negociadas, simplemente se refiere a cómo lo servicios de seguridad son aplicados a cada paquete IP de acuerdo con lo que le indica la SA. Las SAs pueden ser configuradas manualmente por el administrador del sistema o pueden ser negociadas dinámicamente por medio de un protocolo de manejo de llaves tal como IKE.

Este último tipo de negociación es muy importante debido a que en una comunicación de datos es imposible saber cuando una nueva SA se tiene que establecer y más cuando los datos a asegurar provienen del exterior del sistema.

La otra razón importante para usar negociación dinámicas de SAs, es que por motivos de seguridad las SAs no pueden tener un tiempo de vida muy largo, dado que se expone a que algún atacante rompa los códigos de seguridad.

Para eliminar este riesgo, las SAs se renegocian periódicamente regenerando así todo el material asociado a las llaves mismas [10].

2.7 Ventajas de una VPN

- La principal ventaja de usar una VPN es que permite disfrutar de una conexión a red con todas las características de la red privada a la que se quiere acceder.
- El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de un ordenador en esa red privada, pudiendo acceder a la información publicada

para esa red privada: bases de datos, documentos internos, etc. a través de un acceso público [14].

- Todas las conexiones de acceso a Internet desde el ordenador cliente VPN se realizaran usando los recursos y conexiones que tenga la red privada.
- Reducción de costes en los sistemas de comunicación de una empresa.

CAPÍTULO III

MULTI-PROTOCOL LABEL SWITCHING (MPLS)

3.1 GENERALIDADES

Multi - Protocol Label Switching (MPLS) es una tecnología que modifica el reenvío tradicional de paquetes que analiza la dirección IP de destino contenida en la cabecera de la capa de red de cada paquete y por medio de la cual un paquete viaja desde la fuente hasta su destino final. En el análisis tradicional para el reenvío de un paquete IP cada proceso de estos es realizado en cada punto de la red. Los protocolos de enrutamiento dinámicos o estáticos construyen una base de datos necesaria, la cual se analiza para tomar una decisión hacia donde va el paquete IP según dirección de destino, dicha tabla se conoce como tabla de enrutamiento.

El reenvío tradicional de paquetes que realiza la capa de red, confía en la información que le proveen los protocolos de enrutamiento tales como OSPF (Open Shortest Path First) o BGP (Border Gateway Protocol) o las rutas estáticas configuradas en cada router, para tomar la decisión de reenvío entre los mismos. Es decir, la decisión de reenvío está basada única y exclusivamente en la dirección IP de destino. Todos los paquetes para el mismo destino siguen el mismo camino a través de la red si no existen otros caminos de igual costo. Si un router tiene dos caminos de igual costo hacia un mismo destino, los paquetes podrían tomar uno solo o ambos, trayendo como consecuencia una degradación en la velocidad debido al proceso de balanceo de cargas [10].

Los routers son dispositivos que trabajan a nivel de la capa de red, ellos se encargan de recolectar y distribuir la información de enrutamiento y de la conmutación a nivel 3 basada en el contenido de la cabecera de la capa de red de cada paquete.

Los routers se pueden conectar directamente por medio de enlaces punto a punto o redes de área local. También pueden ser conectados a través de switches LAN o WAN. Esos switches LAN o WAN de Capa 2 no tienen la capacidad de mantener la información de enrutamiento de Capa 3 o de seleccionar el camino que debería de tomar un paquete partiendo del análisis de su dirección de destino Capa 3. Es decir, los switches de Capa 2 no se pueden involucrar en el proceso de reenvío de paquetes a nivel de Capa 3.

En el caso de una red WAN el diseñador de la red tiene entonces que establecer trayectos a nivel 2 manualmente a través de toda la red WAN. Por esos trayectos o paths es por donde los enrutadores que están conectados físicamente a la Capa 2, reenvían sus paquetes a nivel de la Capa 3.

El establecimiento de un path en una red WAN de Capa 2 se realiza por medio de un enlace punto-a-punto, que en la mayoría de redes WAN es llamado un circuito virtual y que se establece únicamente por medio de una configuración manual. Cualquier dispositivo de enrutamiento que se encuentre conectado en los límites de una red de Capa 2 y que quiera reenviar sus paquetes a nivel de Capa 3 a otro dispositivo de enrutamiento, necesita establecer una conexión directa a través de la red.

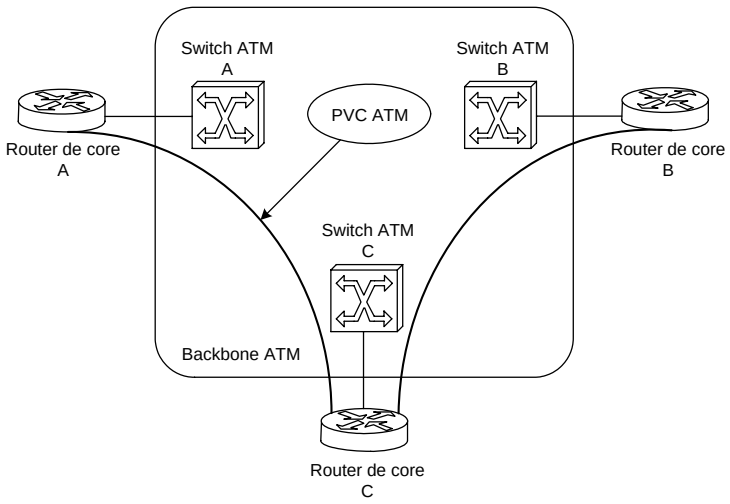

Figura 3.1: Red IP basada en un backbone ATM

La figura 3.1 muestra una red WAN ATM y tres routers que se encuentran conectados a cada switch ATM. Asumiendo que existen caminos o paths entre A y C y entre C y B, todos los paquetes enviados desde A hasta B, deben ser enviados hacia el router de C, donde ellos son analizados y enviados a través de su conexión ATM existente hasta B. Este paso extra introduce un retardo en la red y una carga innecesaria de la CPU en el router de C, al igual que el alcance existente entre el switch ATM de C y el router del mismo.

Si se quisiera implementar de mejor manera el reenvió de paquetes en la red mostrada en la figura 3.1, debería existir un circuito virtual ATM entre cada uno de los enrutadores que la componen, esto es, un VC entre A y B, un VC entre A y C y un VC entre C y B. Esto se torna fácil cuando la red es pequeña como la que se está tratando, en la cual hay tres nodos, pero en redes más grandes que se componen de decenas o cientos de enrutadores conectados a la misma red WAN.

3.1.1 Multi - Protocol Label Switching (MPLS)

MPLS quiere decir Conmutación Multi-protocolo por Etiquetas (Multi - Protocol Label Switching). Es una tecnología relativamente nueva que se desarrolló para solucionar la mayoría de los problemas que existen en la técnica actual de reenvío de paquetes. La IETF cuenta con un grupo de trabajo MPLS que ha unido esfuerzos para estandarizar esta tecnología. El objetivo primario de MPLS, es estandarizar una tecnología base que integre el intercambio de etiquetas durante el reenvío con el sistema de enrutamiento actual de redes. Se espera que esta nueva tecnología mejore la relación precio/desempeño del enrutamiento que se realiza en la capa de red, que mejore la escalabilidad de la misma capa, y que provea una gran flexibilidad en la entrega de (nuevos) servicios de enrutamiento.

3.2 Arquitectura MPLS

La arquitectura MPLS describe cómo se realiza la conmutación de etiquetas, la cual combina los beneficios del reenvío de paquetes a nivel de Capa 2 con los beneficios del enrutamiento a nivel 3. Similar a como se hace en las redes Capa

2, MPLS asigna etiquetas a los paquetes para que sean transportados a través de redes basadas en paquetes o en celdas. Este mecanismo de reenvío a través de dichas redes es conocido como intercambio de etiquetas (label swapping), lo cual permite que con una etiqueta pequeña y de longitud fija que se añade al paquete original se pueda enrutar dicho paquete a lo largo de un camino determinado que se crea con la información que cada switch en la red tiene y sobre la que existe en cada etiqueta. Esta es la forma como se puede crear una VPN usando MPLS [10].

En el reenvío de paquetes usando MPLS se puede apreciar una diferencia drástica con el reenvío original de paquetes, dado que en este último entorno, cada paquete es analizado en cada uno de los saltos de la red, donde se chequea la cabecera Capa 3, y con base en la información de la misma se toma una decisión conforme a la tabla de enrutamiento de cada dispositivo de Capa 3. En MPLS los conmutadores pueden realizar el reenvío, pero éstos no tienen la necesidad de analizar las cabeceras del nivel de red.

La arquitectura MPLS se divide en dos componentes: el componente de reenvío (también llamado data plane) y el componente de control (también llamado control plane).

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

El componente de control es el responsable de crear y mantener toda la información de reenvío de etiquetas (también llamada Vínculos) entre un grupo de switches de etiquetas interconectados. De nuevo, haciendo la analogía con el esquema tradicional de enrutamiento, el componente de control es el protocolo de enrutamiento. La figura 3.2 muestra en un esquema la arquitectura de un nodo

MPLS realizando el enrutamiento de un paquete IP. Se detalla la relación entre cada uno de los bloques dentro del mismo nodo y también con nodos adyacentes.

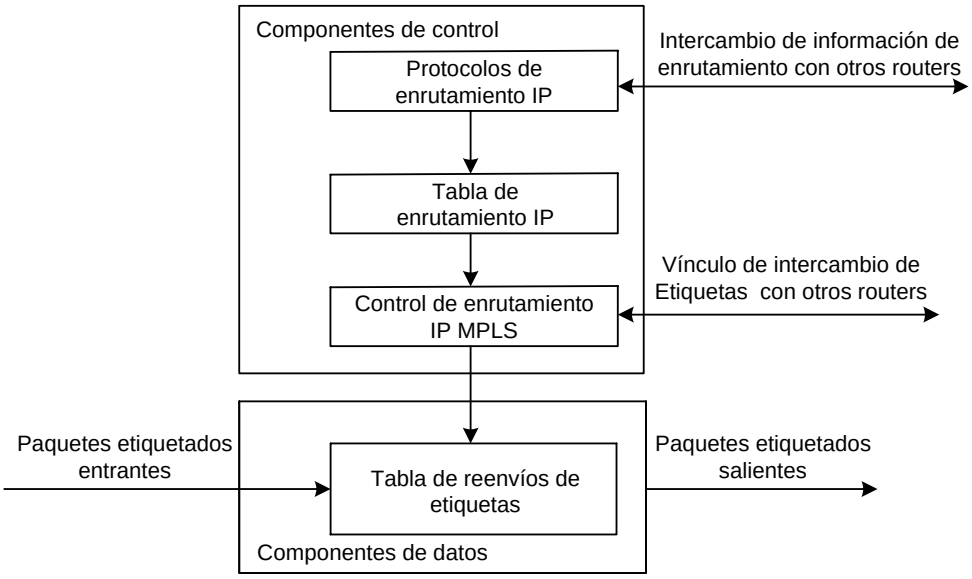

Figura 3.2: Arquitectura de un nodo MPLS

Como se observa en la Figura 3.2, cada nodo MPLS también es router IP en el componente de control, ya que ejecuta uno o varios protocolos de enrutamiento (o depende de rutas estáticas) para intercambiar información de enrutamiento con otros nodos MPLS en la red.

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

En un nodo MPLS, la tabla de enrutamiento es usada para determinar el intercambio de vínculos de etiquetas, dicho intercambio es realizado por el Protocolo de Distribución de Etiquetas o LDP (Label Distribution Protocol).

El componente de control usa las etiquetas intercambiadas con los nodos MPLS adyacentes para construir la Tabla de Reenvío de Etiquetas o LFT (Label

Forwarding Table), la cual usa el componente de datos para reenviar los paquetes etiquetados a través de la red MPLS.

3.3 Componentes de una Red MPLS

Se le llaman Enrutadores de Conmutación por Etiquetas o LSR (Label Switch Router) a cualquier dispositivo que esté involucrado en el proceso de distribución de etiquetas y que pueda reenviar paquetes. La función básica del proceso de distribución de etiquetas es poder permitirle a cada LSR que distribuya sus vínculos de etiquetas a otros LSRs dentro de la red MPLS [10].

El LSR es un router que realiza o la imposición o la remoción de las etiquetas en los límites de la red MPLS. La labor de imposición consiste en añadir al paquete original una etiqueta o un conjunto de etiquetas en el punto de ingreso a la red (en el sentido fuente-destino). La función de extracción es lo contrario, y consiste en quitar la ultima etiqueta del paquete en el punto de egreso antes de ser reenviada al siguiente host externo a la red MPLS.

Los LSR usan la tabla de reenvío IP tradicional para etiquetar paquetes IP o para remover las etiquetas de los mismos antes de ser enviados a un nodo no MPLS.

3.4 FEC (Forwarding Equivalence Classes) Y Etiquetas [Label]

La imposición de etiquetas en MPLS es la acción de añadir una etiqueta a un paquete cuando éste entra a un dominio MPLS. Esta función se realiza siempre en los límites de la red MPLS y es ejecutada por un Edge - LSR.

En el reenvío tradicional de paquetes IP, cada salto en la red realiza una consulta en la tabla de reenvío IP, y con base en la dirección destino que se encuentra en la cabecera de red, selecciona el siguiente salto y reenvía el paquete hacia éste. Esta iteración se repite en cada salto de la red hasta que el paquete llega a su destino final [10].

Escoger el siguiente salto para el paquete IP es la combinación de dos funciones. La primera función clasifica todos los paquetes que llegan en determinado momento al router en varios grupos de prefijos IP destino; es decir, agrupa todos los paquetes que pertenecen a una misma subred y que por lo tanto tienen que ser reenviados al mismo destino. La segunda función asocia a cada grupo de paquetes creado en el primer paso a una dirección IP que es su siguiente salto.

Dentro de la arquitectura MPLS, el resultado de la primera función, es decir, los grupos de paquetes con el mismo destino, es llamado un FEC (Forwarding Equivalence Classes). Cada paquete dentro un FEC es reenviado de la misma manera, por lo tanto atraviesan la red usando el mismo path.

A diferencia del reenvío tradicional de paquetes, el proceso de asignar a un paquete un FEC es realizado solo una vez y no por cada salto, con lo cual se reduce el procesamiento de cada router dentro de la red. El FEC a el cual el paquete es asignado, es luego codificado como un identificador de tamaño fijo llamado etiqueta.

Cuando el paquete etiquetado llega al siguiente salto dentro del dominio MPLS, el LSR que lo recibe, analiza su etiqueta y lo reenvía al siguiente salto dependiendo de la información que aparece en LFT. Es muy importante anotar, que este análisis se realiza primero que el de Capa 3, por tanto el proceso de toma de decisión a nivel 3 no se realiza.

3.5 Protocolos y distribución de Etiquetas

Un protocolo de distribución de etiquetas es un conjunto de procedimientos por los cuales un enrutador LSR informa a otro de la relación etiqueta/FEC que ha hecho. Dos enrutadores LSR, que usan un protocolo de distribución de etiquetas para intercambiar la información de la etiqueta/FEC se les conoce como "puertos de distribución de etiquetas" respecto a la información que intercambian. Si dos enrutadores LSR son puertos de distribución de etiquetas, se habla de que hay

una "distribución de etiquetas adyacente" entre ellos. El protocolo de distribución de etiquetas también abarca las negociaciones en el que dos puertos de distribución de etiquetas necesitan comunicarse con el fin de aprender de las posibilidades MPLS del otro.

Dependiendo de como se establezcan los LSP (Label Switched Path) que es la ruta sobre una red MPLS establecida sobre un protocolo de señalización, se pueden presentar diversas opciones. Si se utiliza la aproximación salto a salto (hop by hop) para el establecimiento de los LSP la IETF ha recomendado (no obligatorio) el uso del protocolo LDP para la asignación de etiquetas, en este caso también se pueden utilizar los protocolos RSVP y CR-LDP (Constraint-Based Routing Label Distribution Protocol) [15].

3.5.1 LDP (Label Distribution Protocol)

Es la opción recomendada aunque no obligatoria del IETF para el intercambio de mensajes entre LSR's. Se realiza mediante el envío de PDU's (Protocol Data Unit) de LDP. Este envío se basa en la utilización se sesiones LDP que se establecen sobre conexiones TCP. Es importante destacar que cada LDP PDU puede transportar más de un mensaje LDP, sin que estos mensajes tengan que tener relación entre ellos. El protocolo LDP utiliza el esquema de codificación de mensajes conocido como TLV (Tipo, Longitud, Valor), cada mensaje LDP tiene la siguiente estructura:

- U: campo de un bit que indica el comportamiento en caso de recibir un mensaje desconocido. U=0 hay que responder con un mensaje de notificación al LSR origen, U=1 se ignora el mensaje y se continua procesando el PDU.
- F: campo de un bit. Este campo sólo se utiliza cuando el bit U esta en 1. Si se recibe un mensaje desconocido que debe reenviarse y el bit F está en cero, este mensaje no es reenviado al siguiente LSR, en caso contrario si se hace.
- Tipo: campo de 14 bits que define el tipo de mensaje y, por lo tanto indica cómo debe ser interpretado el campo valor.

- Longitud: campo de 2 octetos que especifica la longitud del campo valor.
- Valor: campo de longitud variable que contienen la información del mensaje. La interpretación de la cadena de octetos de este campo depende del contenido del campo tipo.

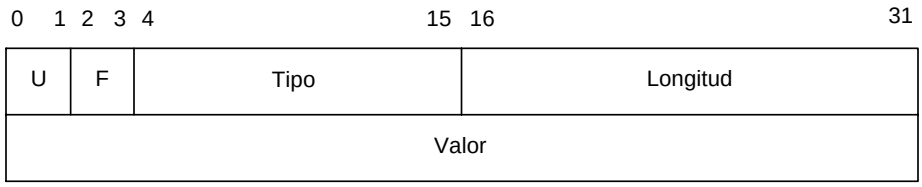

Figura 3.3: Formato de un mensaje LDP

3.5.2 RSVP (Resource Reservation Protocol)

Para poder utilizar este protocolo en el entorno MPLS se le han agregado nuevas capacidades, estas se refieren a los objetos formatos de los paquetes y procedimientos necesarios para establecer los túneles LSP. Para el establecimiento de los túneles LSP el protocolo de señalización utiliza el modelo *downstream on demand*. Esto significa que la petición de asociación entre el FEC y una etiqueta para crear un túnel LSP es iniciada por el LSR de entrada, para lograr este objetivo hay que agregar un objeto (LABEL_REQUEST) al mensaje del path de RSVP antes mencionado [15].

Un *mensaje path* es aquel que lleva un objeto de etiqueta, que indica la etiqueta que el LSR quisiera que fuera usada sobre el segmento de los LSP que une a los LSR.

Un requisito adicional para este protocolo RSVP es que el dominio MPLS debe soportar el encaminamiento explicito (*explicit routing*) para facilitar la gestión de tráfico. Para lograr esto se añade el objeto (EXPLICIT_ROUTE) en los mensajes del path. Este nuevo objeto encapsula el conjunto de nodos ordenados que constituyen la ruta explícita que deben seguir los datos. Como la asignación de etiquetas se realiza desde el destino hacia el origen, en sentido contrario al flujo de datos, es necesario incrementar el mensaje *resv* con un objeto adicional

(LABEL) capaz de transportar la nueva información requerida para este uso del protocolo.

El funcionamiento de este protocolo para el establecimiento de túneles LSP se describe a continuación.

- Cuando un LER (Label Edge Router), que son los routers situados en la frontera de la red, entran al dominio MPLS necesitan establecer un LSP hasta un determinado LER de salida, iniciando un procedimiento para establecerlo, mediante un mensaje *path*. La ruta que debe seguir el LSP puede ser una ruta explícita determinada por el gestor de la red (esta ruta puede no coincidir con la calculada por los algoritmos de encaminamiento de la capa red).
- Cuando los LSR intermedios reciben el mensaje de *path* lo procesan de acuerdo con las especificaciones del protocolo y una vez reconocido que no son el extremo del FEC, transmiten el mensaje hacia el siguiente nodo de la ruta.
- Cuando el mensaje de path finalmente alcanza el LSE destino, éste procede a reservar los recursos internos, selecciona la etiqueta a utilizar para este túnel LSP y procede a propagarla hacia el anterior LSR mediante un mensaje de reserva (*resv*).
- Cuando los LSR's intermedios reciben la asignación de la etiqueta con el mensaje de resv proceden a reservar los recursos internos necesarios y determinar la etiqueta a utilizar para el flujo. Una vez calculada la propagan para el LSR anterior de nuevo con ayuda del mensaje *resv*. Este proceso se repite hasta alcanzar el LSR origen donde también se realiza el proceso de reservar recursos internos, pero en este caso no es necesario asignar etiqueta y propagarla ya que se ha alcanzado el origen del FEC.

3.5.3 CR - LDP (Constraint - Based Routing Label Distribution Protocol)

Es un encaminamiento basado en restricciones (Constraint-based routing). Esta extensión del LDP se basa en el calculo de trayectos que están sujetos a ciertas restricciones: ancho de banda, los requisitos de calidad de servicios QoS,

demora (delay), variación de demora o jitter, o cualquier otro requisito asociado al trayecto que defina el operador de la red. Esta es una de las herramientas más útiles para controlar el dimensionado del tráfico y la QoS en la red que pueden ofrecer a sus clientes y/o usuarios [15].

Debido a ello, el capítulo MPLS de la IETF ha elaborado las extensiones necesarias para que el protocolo LDP pueda soportar este tipo de encaminamiento esta extensión es conocida como CR-LDP (Constraint-Based Routing Label Distribution Protocol) y se ha definido expresamente para soportar el establecimiento y mantenimiento de LSP encaminados en forma explícita y las modificaciones de los LSP, pero no incluyen los algoritmos necesarios para calcular trayectos según los criterios definidos por el operador de la red. Las principales limitaciones son las siguientes:

- Solo se soportan LSP's punto a punto.
- Solo se soportan LSP's unidireccionales.
- Sólo se soporta una única etiqueta por LSP.

3.6 Descripción Funcional de MPLS

La operación del MPLS se basa en las componentes funcionales de envío y control, aludidas anteriormente, y que actúan ligadas íntimamente entre sí.

3.6.1 Funcionamiento del envío de paquetes en MPLS

La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son simplex por naturaleza (se establecen para un sentido del tráfico en cada punto dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Label-Switching Router) a otro, a través del dominio MPLS. Un LSR no es sino un router especializado en el envío de paquetes etiquetados por MPLS [16].

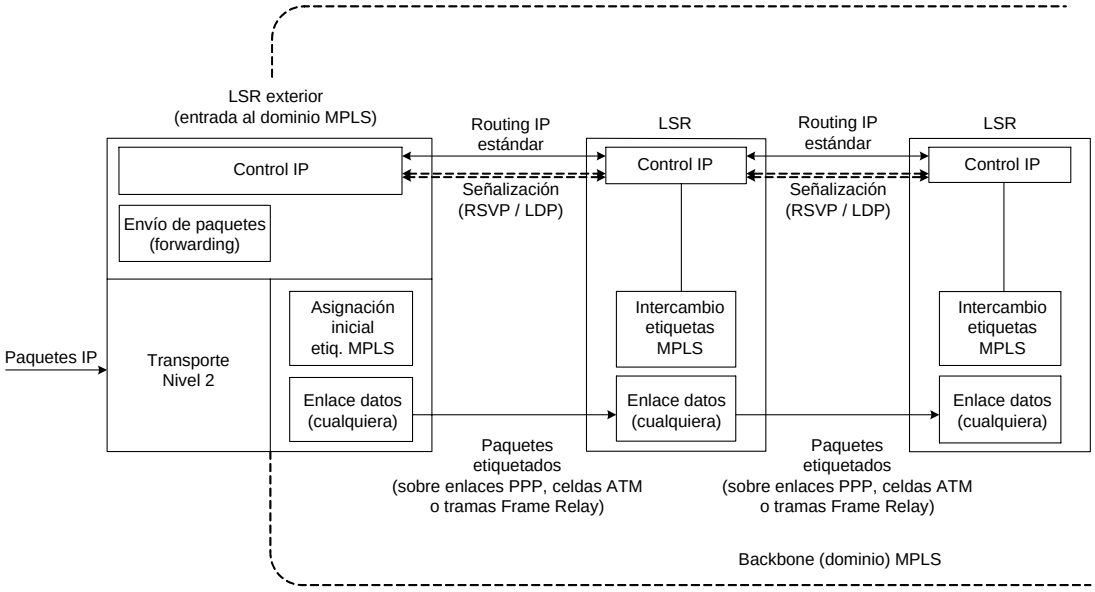

Figura 3.4: Esquema funcional del MPLS

En la figura 3.4 se puede ver la funcionalidad del MPLS. Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de control (*routing*) y de envío (*forwarding*). Del mismo modo, el envío se implementa mediante el intercambio de etiquetas en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por el ATM Forum; en lugar de ello, en MPLS o bien se utiliza el protocolo RSVP o bien un nuevo estándar de señalización LDP. Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera.

Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM, esto lo resuelve el procedimiento de intercambio de etiquetas MPLS.

El papel de ATM queda restringido al mero transporte de datos a base de celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto.

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un router que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control.

Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por ese interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola). En la figura 3.5 se ilustra un ejemplo del funcionamiento de un LRS del núcleo MPLS. A un paquete que llega al LSR por el interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

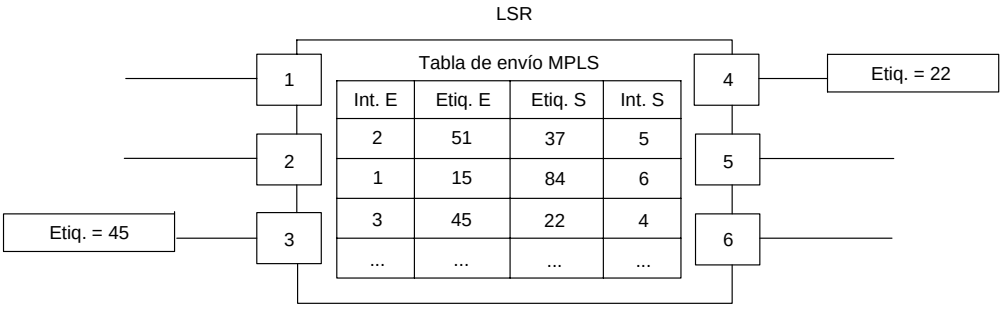

Figura 3.5: Detalle de la tabla de envío de un LSR

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura 3.6 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo)

y envía el paquete al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por *routing* convencional [16].

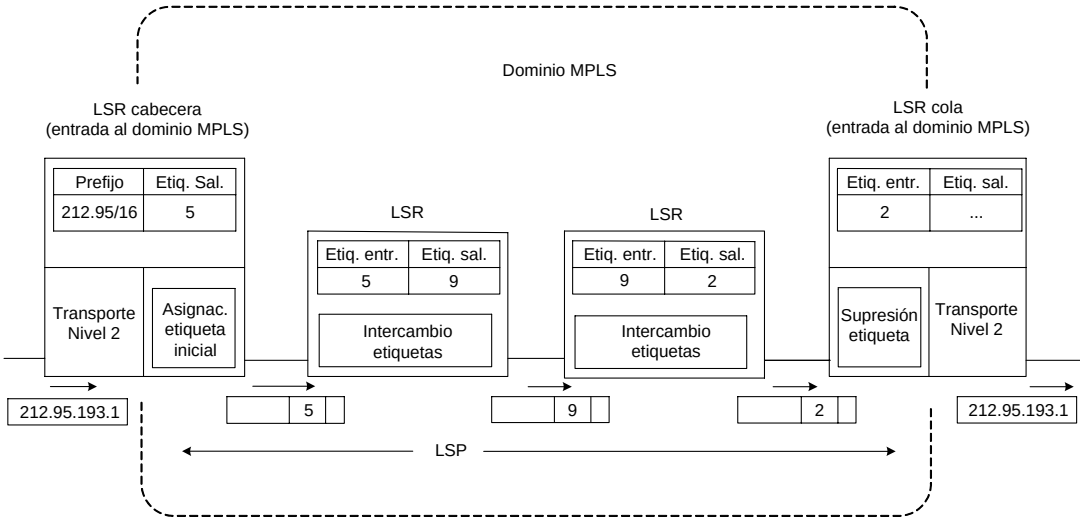

Figura 3.6: Ejemplo de envío de un paquete por un LSP

Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no mira sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3. Según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas, se utilizan esos campos nativo para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas, entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

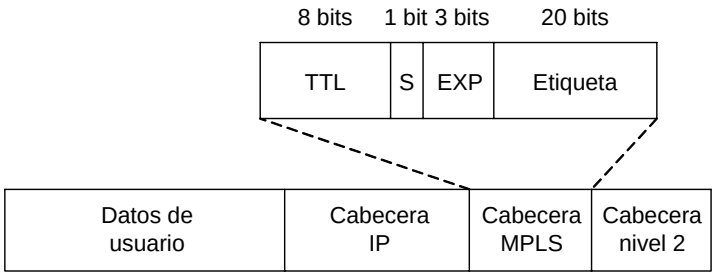

Figura 3.7: Estructura de la cabecera genérica MPLS

En la figura 3.7 se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS), 1 bit de stack para poder apilar etiquetas de forma jerárquica (S) y 8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

3.6.2 Control de la Información en MPLS.

Hasta ahora se ha visto el mecanismo básico de envío de paquetes a través de los LSPs mediante el procedimiento de intercambio de etiquetas según las tablas de los LSRs. Pero queda por ver dos aspectos fundamentales:

- Cómo se generan las tablas de envío que establecen los LSPs.
- Cómo se distribuye la información sobre las etiquetas a los LSRs.

El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de encaminamiento. MPLS necesita esta información de *routing* para establecer los caminos virtuales LSPs. Lo más lógico es utilizar la propia información de encaminamiento que manejan

los protocolos internos IGP (Internet Gateway Protocol) para construir las tablas de encaminamiento. Esto es lo que hace MPLS precisamente para cada ruta IP en la red se crea un camino de etiquetas a base de concatenar las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

El segundo aspecto se refiere a la información de señalización. Pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo de Servicios Integrados del IETF. Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, cual es el caso del LDP.

3.6.3 Funcionamiento global MPLS.

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la figura 3.8, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS.

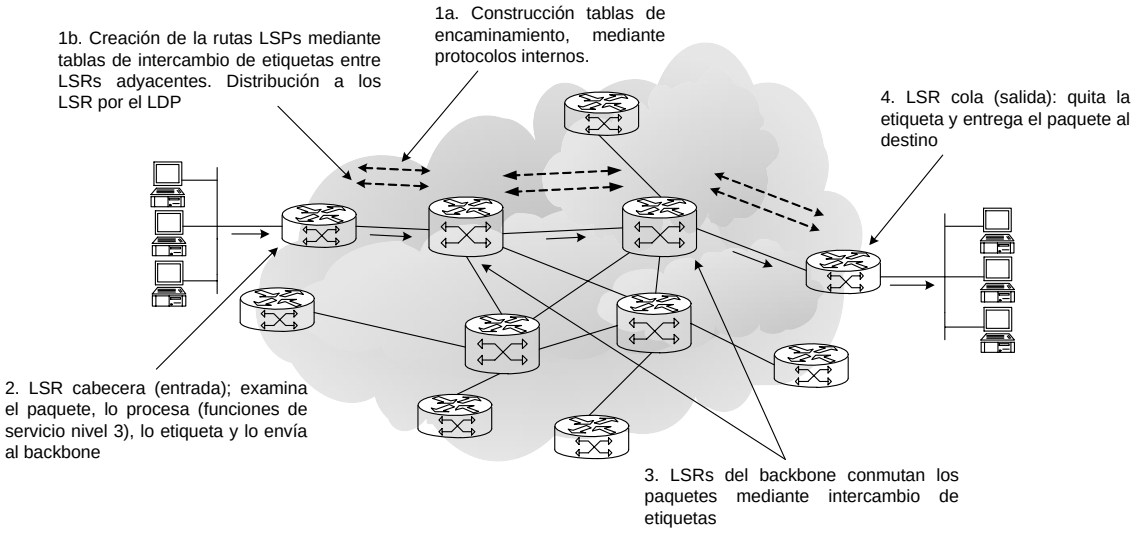

Figura 3.8: Funcionamiento de una red MPLS

Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de routers IP. Funcionalmente es como si estuvieran unidos todos en una topología mallada. Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs. La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario [16].

3.7 Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

- Ingeniería de tráfico
- Diferenciación de niveles de servicio mediante clases (CoS)
- Servicio de redes privadas virtuales (VPN)

Veamos brevemente las características de estas aplicaciones y las ventajas que MPLS supone para ello frente a otras soluciones tradicionales.

3.7.1 Ingeniería de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos). En el

esquema de la figura 3.9 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino [16].

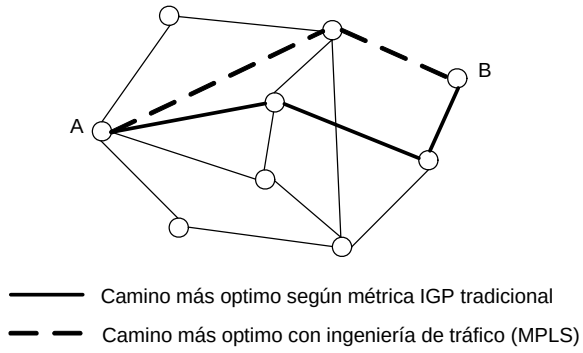

Figura 3.9: Comparación entre camino más optimo IGP con ingeniería de tráfico

El camino más optimo entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes hagan aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes *backbones*, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.
- Permite hacer encaminamiento restringido (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura

ATM por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

3.7.2 Clases de Servicio (CoS)

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades.

Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el www, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de vídeo y voz interactiva. Para ello se emplea el campo ToS (Type of Service). Esta es la técnica QoS de marcar los paquetes que se envían a la red [16].

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De es te modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

- El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.
- Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico *best-effort*, tres niveles de servicio, primera, preferente y turista, que, lógicamente, tendrán distintos precios.

3.7.3 Redes Privadas Virtuales (VPN)

Una red privada virtual (VPN) se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y privada indica que el usuario cree que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales [16].

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PCVs entre los diversos nodos que conforman la VPN. Algo similar se puede hacer con ATM, con diversas clases de garantías. Los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión. Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CPEs del cliente y restablecer todos los PVCs.

Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los NSPs (Network Service Provider), ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costes de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN. No es el objetivo de esta sección una exposición completa de IP VPNs sobre túneles; se pretende tan sólo resumir sus características para poder apreciar luego las ventajas que ofrece MPLS frente a esas soluciones. Se puede obtener más información sobre IP VPN con túneles en las referencias correspondientes a VPNs con MPLS. Los túneles IP en conexiones dedicadas se pueden establecer de dos maneras:

- En el nivel 3, mediante el protocolo IPSec del IETF.
- En el nivel 2, mediante el encapsulamiento de paquetes privados sobre una red IP pública.

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios routers de acceso del NSP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del NSP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de

usuarios, si así lo desean. A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor.

A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen unas características comunes que las hacen menos eficientes frente a la solución MPLS:

- Están basadas en conexiones punto a punto (PVCs o túneles).
- La configuración es manual.
- La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.
- Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales.
- La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, a base de túneles extremos a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En la figura 3.10 se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales y los túneles MPLS (LSPs) está en que éstos se crean dentro de la red, a base de LSPs, y no de extremo a extremo a través de la red.

En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una nube común en las que solamente pueden entrar los miembros de la misma

VPN. Las nubes que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS.

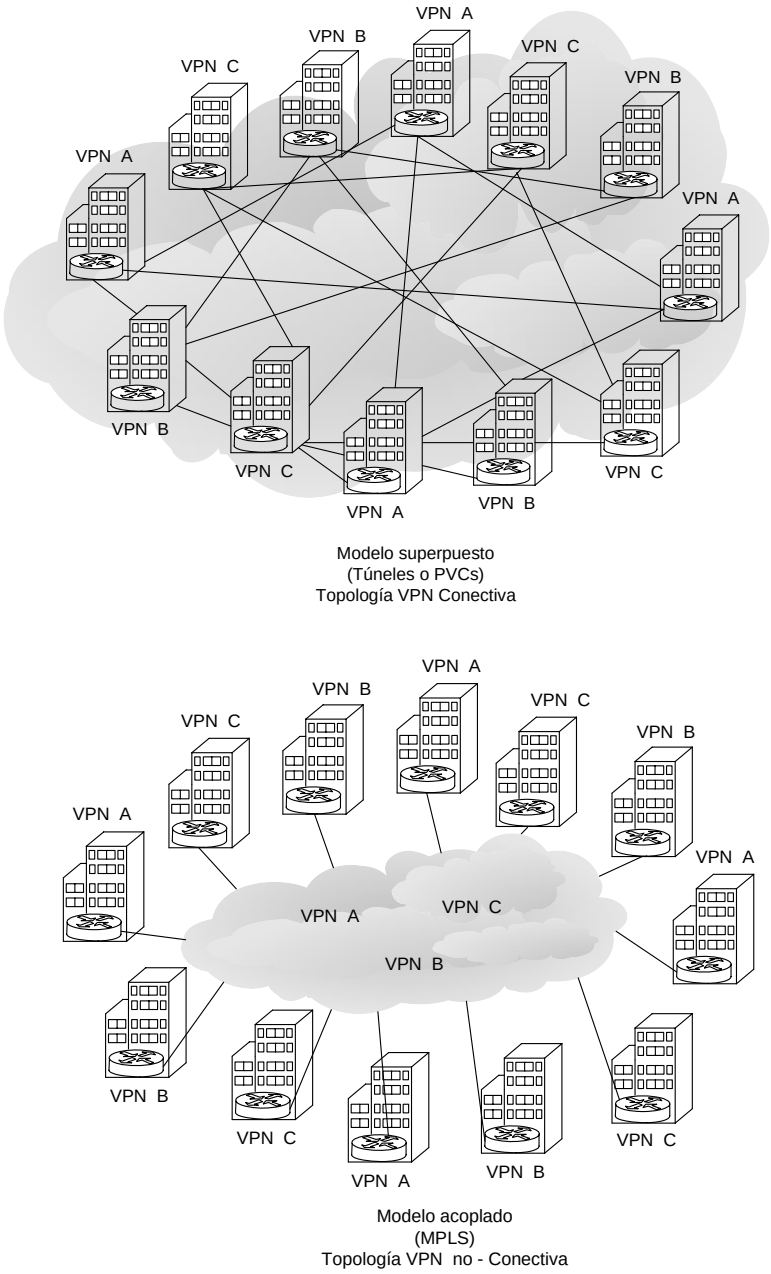

Figura 3.10: Modelo superpuesto (túneles/PVCs) vs. modelo acoplado (MPLS)

Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles

se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada rutas MPLS sino que ve una internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

CAPÍTULO IV

DISEÑO DE REDES PRIVADAS VIRTUALES UTILIZANDO TECNOLOGÍA MPLS

4.1 Planeación

El objetivo de este capítulo es diseñar una red MPLS que da servicio de red privada virtual a 1 cliente con 2 redes.

Se utilizara el protocolo LDP, que va a hacer el protocolo encargado de la distribución de etiquetas entre dispositivos, la razón radica que para el uso de la aproximación salto a salto (hop by hop) en el establecimiento de los LSP la IETF recomienda el uso del protocolo LDP para la asignación de etiquetas.

Por otro lado se harán uso de 3 ruteadores (ver figura 4.1), la función de los mismos será: router 1 asignar las etiquetas, router 2 conmutar y router 3 quitar las etiquetas.

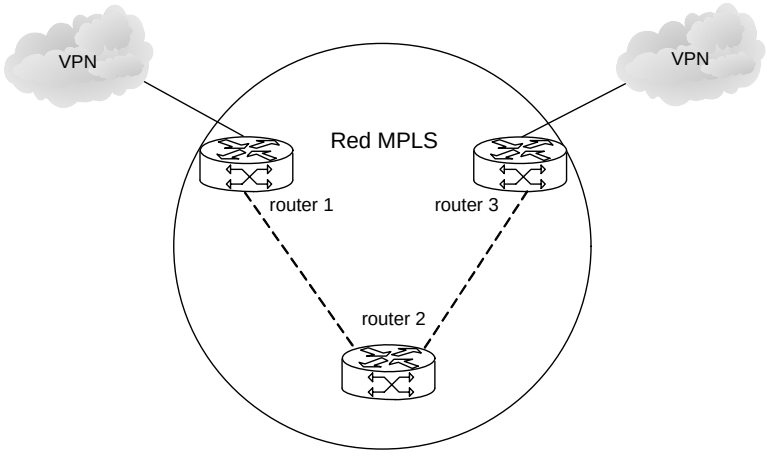

Figura 4.1: Distribución de routers en la red MPLS

El tipo de VPN será independiente del diseño, ya que se asumirá que la VPN como tal ya existe cualquiera que esta sea, de la misma que se partirá para realizar el diseño.

4.2 Requerimientos

La red está formada por 3 routers Cisco 2611, cuyas características importantes son:

- Router IP con OSPF, BGP.
- 2 puertos Fast Ethernet (10/100 Base T), 1 puerto Ethernet (10 Base T).
- MPLS con LDP para distribución de etiquetas.

4.3 Enrutamiento

4.3.1 Configuración de una Interfaz Loopback

La interfaz de loopback nos servirá para el identificador del router. Una interfaz de loopback se crea de la siguiente manera:

Comando: *cisco# configure terminal*
Utilidad: entra al modo de configuración global
Comando: *cisco(config)# interface loopback<número de la interfaz>*
Utilidad: crea una interfaz de loopback, no son interfaces físicas sino virtuales
Comando: *cisco(config-if)#ip address <dirección IP> <máscara>*
Utilidad: asigna ip y máscara a la interfaz

El motivo de configurar una interfaz de loopback es que, como veremos más adelante en la configuración de OSPF y de BGP, asociaremos esta interfaz a los procesos OSPF y BGP, asegurándonos de que no vamos a perder las sesiones OSPF o BGP por un problema físico en el interfaz ya que las interfaces de loopback son interfaces lógicas.

4.3.2 Configuración de OSPF

En la red MPLS se habrá de configurar OSPF como protocolo de routing dinámico. La configuración de OSPF en un router Cisco requiere dos pasos fundamentales:

1. Arranque del proceso OSPF mediante el comando:

   Comando: *(config)# router ospf 1*
   Utilidad: habilita el proceso de ospf

   siendo “1” el identificador del proceso ospf (puede ser cualquier valor, incluso distinto en cada router de la red; únicamente se utiliza para distinguir procesos OSPF en el caso de que existan varios arrancados simultáneamente en el mismo router).

2. Definición del área en la que se encuentra cada interfaz del router que participa en OSPF. Para ello se utiliza el comando “network”:

   Comando: *(config-router)# network address wildcard-mask area area-id*
   Utilidad: publica las redes IP

   Mediante este comando se especifica la asociación entre direcciones de interfaces e identificadores de áreas. Por ejemplo:

   (config)# router ospf 1
   (config-router)# network 131.108.20.0 0.0.0.255 area 0
   (config-router)# network 131.109.10.0 0.0.0.255 area 1

   La primera línea especifica que todos los interfaces del router cuya dirección comience por 131.108.20.0 /24 pertenecen al área 0. Así mismo,

la segunda línea declara que los interfaces cuya dirección comience por 131.109.10.0/24 pertenecen al área 1.

Un comando de gran importancia para comprobar las adyacencias OSPF es *show ip ospf neighbor* que muestra la lista de routers que mantienen una relación de “vecindad” con el router en el que se ejecuta el comando.

El comando *show ip route* permite ver la tabla de rutas del router donde se ejecuta el comando e indica si el router aprende las rutas por OSPF.

Por otro lado se puede comprobar el estado de OSPF por interfaz con el siguiente comando *show ip ospf interface*

4.3.3 Configuración de BGP

Antes de configurar la red MPLS, se debe establecer un full-mesh de sesiones BGP entre los PE, que son los puntos donde se lee la cabecera del paquete que entra y se etiqueta según su destino o si el paquete sale elimina la etiqueta que se haya añadido al paquete y así dejar preparado el escenario de red para la configuración final de MPLS en los routers. Un full-mesh es el modelo usado por todos los sitios dentro de una VPN para comunicarse directamente con cada otra VPN. La configuración de BGP requiere los siguientes pasos:

1. Configurar el proceso de routing BGP.

   Comando: *cisco# configure terminal*
   Utilidad: entra al modo de configuración global
   Comando: *cisco(config)# router bgp <número de proceso BGP>*
   Utilidad: habilita el proceso de bgp

   El número de proceso BGP que generalmente se pone es el 65000, para entorno de pruebas, ya que hay otras numeraciones que están reservadas,

lo que realmente estamos configurando con el comando router bgp<numero de proceso BGP> es el sistema autónomo en el que queremos que se hable BGP.

2. Establecer las adyacencias entre los pares BGP.

   Para cada pareja de routers (A y B) que estén enfrentados hay que configurar lo siguiente:

   - En el router A se ha de especificar el router vecino e indicarle que actualice el encaminamiento a través de la interfaz de loopback configurada anteriormente:

     Comando: *cisco(config-router)# neighbor <dir IP de la interfaz del vecino que tiene enfrentada> remote-as <número de proceso BGP>*
     Utilidad: crea un nuevo vecino
     Comando: *cisco(config-router)#neighbor<dir IP de la Interfaz del vecino que tiene enfrentada> update-source loopback<número de la interfaz>*
     Utilidad: usa la dirección del interfaz designado para establecer la sesión bgp

   - En router B se ha de especificar la dirección IP de la interfaz de loopback del router vecino que se ha indicado en el comando anterior.

     Comando: *cisco(config-router)# neighbor <dir IP de la interfaz de loopback del vecino> remote-as <número de proceso BGP>*
     Utilidad: crea un nuevo vecino

Algunos comandos de interés relacionados con BGP para verificar su funcionamiento, son los siguientes:

El comando *show ip bgp neighbor* muestra los routers que mantienen una relación de vecindad con el router en el que se ejecuta el comando, así como la información relativa a esa relación.

El comando *show ip bgp summary* muestra los routers que mantienen una relación de vecindad con el router en el que se ejecuta el comando, así como el estado que se encuentran.

El comando *clear ip bgp ** permite resetear las sesiones BGP establecidas.

4.3.4 Configuración de MPLS

Una vez establecidos los protocolos de routing se han de configurar las funcionalidades MPLS en el routers. Para ello hay que arrancar el protocolo de distribución de etiquetas en las distintas interfaces por que queremos "hablar MPLS". La configuración de MPLS requiere los siguientes pasos:

1. Configurar el CEF (Cisco Express Forwarding) en todos los routers con funcionalidad PE y P (ver figura 4.2).

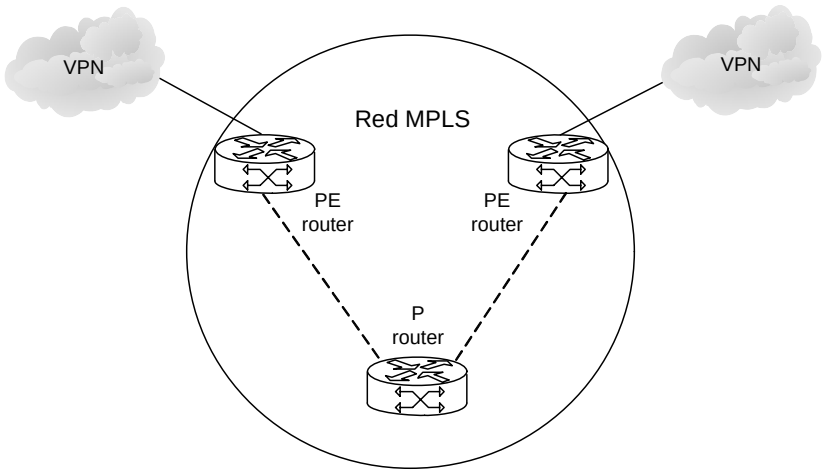

Figura 4.2: Routers PE y P

CEF es el conjunto de funcionalidades que reúnen los equipos Cisco para poder trabajar en un entrono MPLS entre otras funciones. Los comandos que hay que ejecutar para activar CEF en un router que soporte estas funcionalidades son:

Comando: *cisco# configure terminal*
Utilidad: modo de configuración global
Comando: *cisco(config)# ip cef*
Utilidad: habilita el proceso de cef

Para comprobar si se ha activado CEF correctamente se utilizará el siguiente comando: *show ip cef summary*

En caso de que no se hubiese habilitado CEF no se obtendría resultado alguno como salida del comando.

2. Activación del protocolo de distribución de etiquetas LDP. Hay que realizar la siguiente configuración en cada interfaz que vaya a hablar MPLS.

Comando: *cisco(config)# interface <nombre de la interfaz>*
Utilidad: asigna la interfaz a configurar
Comando: *cisco(config-if)# mpls ip*
Utilidad: habilita el proceso mpls
Comando: *cisco(config-if)# mpls label protocol ldp*
Utilidad: habilita el protocolo ldp

4.4 Topología de la Red VPN MPLS

La topología lógica de la red se muestra en la figura 4.3, donde todos los enlaces son Ethernet.

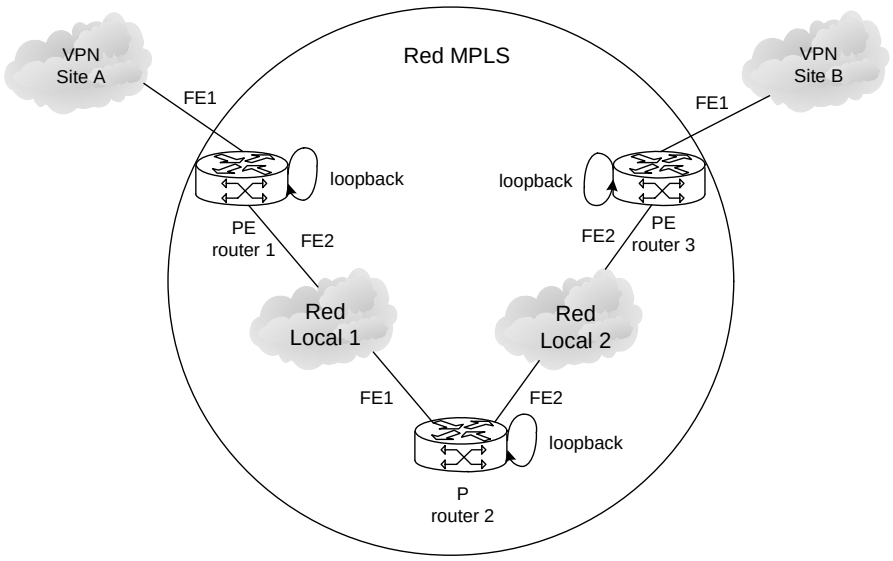

Figura 4.3: Red VPN MPLS - topología lógica

4.5 Configuración de Redes VPN sobre MPLS

4.5.1 Planeación de Direcciones IP.

A continuación se especifica las direcciones IP a ser configuradas en los respectivos routers con sus respectivas máscaras, en donde todos los enlaces son Ethernet.

VPN	IP Address	Mask
Site A	10.10.1.0	255.255.255.0
Site B	10.10.2.0	255.255.255.0

Tabla 4.1: Direcciones IP de la VPN

Red	IP Address	Mask
Local 1	10.1.10.0	255.255.255.0
Local 2	10.1.20.0	255.255.255.0

Tabla 4.2: Direcciones IP de la Red Local

Router 1	IP Address	Mask
Fast Ethernet 1	10.10.1.2	255.255.255.0
Fast Ethernet 2	10.1.10.2	255.255.255.0
Loopback	10.1.1.1	255.255.255.255

Tabla 4.3: Direcciones IP del Router 1

Router 2	IP Address	Mask
Fast Ethernet 1	10.1.10.4	255.255.255.0
Fast Ethernet 2	10.1.20.4	255.255.255.0
Loopback	10.1.1.3	255.255.255.255

Tabla 4.4: Direcciones IP del Router 2

Router 3	IP Address	Mask
Fast Ethernet 1	10.10.2.2	255.255.255.0
Fast Ethernet 2	10.1.20.2	255.255.255.0
Loopback	10.1.1.2	255.255.255.255

Tabla 4.5: Direcciones IP del Router 3

4.5.2 Configuración de equipos con funcionalidad PE

La configuración de VPN's sobre MPLS requiere los siguientes pasos en cada uno de los routers con funcionalidad PE.

1. Configuración de la VRF asociada a la VPN que vamos a configurar en los routers con funcionalidad PE. Una VRF (vpn routing and forwarding) puede ser visto como un router virtual e incluye las tablas de envío y encaminamiento de los sitios pertenecientes a una VPN. Los parámetros necesarios para crearla son:

    - Route Distinguisher (RD) que permite identificar unívocamente un prefijo de VPN. Un RD es un simple número que no hereda ningún significado, sólo se usa para diferenciar los prefijos VPNv4 entre distintas VPN.

- Route-Target (RT) que identifica las VFR en que se instalan las rutas. Un RT permite el control y manejo de prefijos VPNv4, que es el atributo que lleva asociado cada prefijo VPNv4.

  Comando: *cisco#configure terminal*
  Utilidad: entra al modo de configuración global
  Comando: *cisco(config)# ip vrf <nombre de la VRF>*
  Utilidad: crea una VPN
  Comando: *cisco(config-vrf)# rd <valor del rd>*
  Utilidad: identifica una VPN
  Comando: cisco(config-vrf)# route-target export <valor que tiene que exportar>
  Utilidad: exporta todas las rutas de la VPN
  Comando: cisco(config-vrf)# route-target import <valor que tiene que importar>
  Utilidad: importa todas las rutas de la VPN

  El siguiente comando unifica en uno solo los dos últimos, para indicar que el router donde se ejecuta debe exportar e importar el mismo route-target.

  cisco(config-vrf)# route-target both <valor que tiene que importar y exportar>

2. Configuración del forwarding en las interfaces de los routers PE que están enfrentadas a los routers CE.

   Comando: *cisco#configure terminal*
   Utilidad: entra al modo de configuración global
   Comando: *cisco(config)# interface <nombre de la interfaz>*
   Utilidad: asigna la interfaz a configurar
   Comando: *cisco(config-if)# ip vrf forwarding <nombre de la VRF>*

Utilidad: asocia esta interfaz con la VPN creada

3. Reasignación de la dirección IP a la interfaz donde acabamos de configurar el forwarding dentro de la VPN, ya que pierde el direccionamiento de dicha interfaz. Después de ejecutar este último comando se mostrará un mensaje indicando que la interfaz anterior se le ha quitado la configuración IP, por lo que habrá que volver a configurarla:

   Comando: *cisco(config-if)# ip address <dirección IP> <máscara>*
   Utilidad: asigna ip y máscara a la interfaz

4. Configuración del encaminamiento dinámico en la VRF creada: Hay que arrancar un nuevo proceso OSPF dedicado al encaminamiento dentro de la VRF.

   Comando: *cisco# configure terminal*
   Utilidad: *entra al* modo de configuración global
   Comando: *cisco(config)# router ospf <identificador del proceso> vrf <nombre VRF>*
   Utilidad: habilita el proceso de ospf para la VPN

   Definir el área en la que se encuentran las interfaces pertenecientes a la VPN.

   cisco(config-router)# network <red> <wildcard> area 0

5. Configuración de IMBGP (Multiprotocol BGP): Para que los prefijos aprendidos puedan ser transmitidos a los otros equipos PE, hay que configurar iMBGP siguiendo los siguientes pasos:

- Comprobar que los vecinos iBGP siguen activos y operativos. Utilizar el comando

  show ip bgp summary

- Nos metemos en la configuración de BGP del router.

  Comando: *cisco# configure terminal*
  Utilidad: entra al modo de configuración global
  Comando: *cisco(config)# router bgp <número de proceso BGP que esté configurado>*
  Utilidad: habilita el proceso de bgp

- Entramos a configurar iMBGP para la VPN.

  Comando: *cisco(config-router)# address-family vpnv4*
  Utilidad: crea un sub-proceso no BGP para cambio de rutas de todas las VPN's existentes en la red

- Hay que activar los vecinos existentes con la nueva funcionalidad. Según se vayan ejecutando los comandos siguientes se irán reseteando las sesiones BGP. Configurar para cada vecino IBGP mostrado con el comando *show ip bgp summary* lo siguiente:

  Comando: *cisco(config-router-af)# neighbor <dir IP del vecino iBGP> activate*
  Utilidad: activa los vecinos
  Comando: *cisco(config-router-af)#neighbor <dir IP del vecino iBGP> send-community both*
  Utilidad: envía las comunidades asociadas a los distintos prefijos

6. Configuración del envió de los prefijos aprendidos al resto de los equipos con funcionalidad PE. Una vez establecidas las sesiones iMBGP con el resto de equipos PE y verificada la conectividad local con los integrantes de la VPN, queda pendiente propagar los prefijos locales al resto de equipos PE para que éstos sepan encaminar los paquetes hacia dichos prefijos. Para ello, bastará con redistribuir OSPF en el iMBGP

   Comando: *cisco#configure terminal*
   Utilidad: entra al modo de configuración global
   Comando: *cisco(config)# router bgp <número de proceso BGP que esté configurado>*
   Utilidad: habilita el proceso de bgp
   Comando: *cisco(config-router)# address-family ipv4 vrf <nombre del VRF>*
   Utilidad: cambio de rutas de todas las VPN's existentes en la red
   Comando: *cisco(config-router-af)# redistribute ospf <identificador del proceso OSPF> vrf <nombre del VRF>*
   Utilidad: aplica las rutas de ospf en el proceso bgp para la VPN

   El identificador del proceso OSPF se corresponde con el identificador del proceso OSPF que hemos utilizado para configurar el encaminamiento dinámico en la VRF en el paso 4. Conviene resetear las sesiones iMBGP con el comando *cisco# clear ip bgp **

7. Configuración del envío de los prefijos aprendidos a los equipos con funcionalidad CE.

   Comando: *cisco# configure terminal*
   Utilidad: entra al modo de configuración global
   Comando: *cisco(config)# router ospf <identificador del proceso OSPF> vrf <nombre del VRF>*
   Utilidad: habilita el proceso de ospf para la VPN

Comando: *cisco(config-router)# redistribute bgp <número de proceso BGP que esté configurado> subnets metric 20*

Utilidad: aplica las rutas de ospf en el proceso bgp para la VPN

4.6 Esquema Final de Diseño

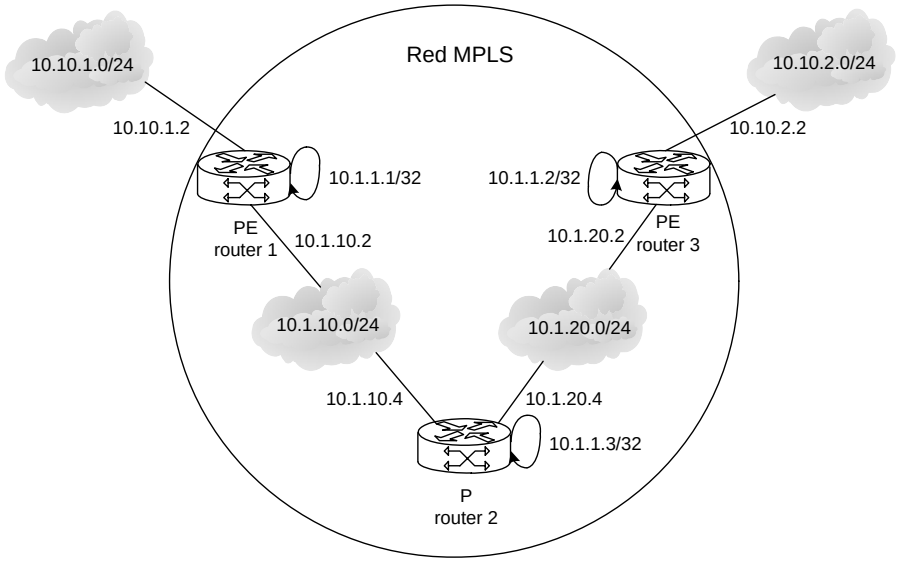

Figura 4.4: Esquema VPN MPLS final

La red MPLS tiene configurados los 3 routers con OSPF como protocolo de encaminamiento interno. De esta forma cada router conoce la topología completa de la red MPLS (ver figura 4.5). Los routers frontera PE1 y PE2 tienen configurado BGP (conexión TCP), como protocolo de encaminamiento externo. De esta forma los routers PE conocen de la existencia de las redes IP de los clientes, lo cual implica que cada router PE esté conectado a un router del cliente con BGP.

Los routers PE tiene 2 tablas de encaminamiento, la normal IP, compuesta por las rutas directas y las aprendidas por OSPF, internas a la red MPLS. La segunda tabla es de encaminamiento de las VPN, compuesta por las rutas directas y las aprendidas por BGP.

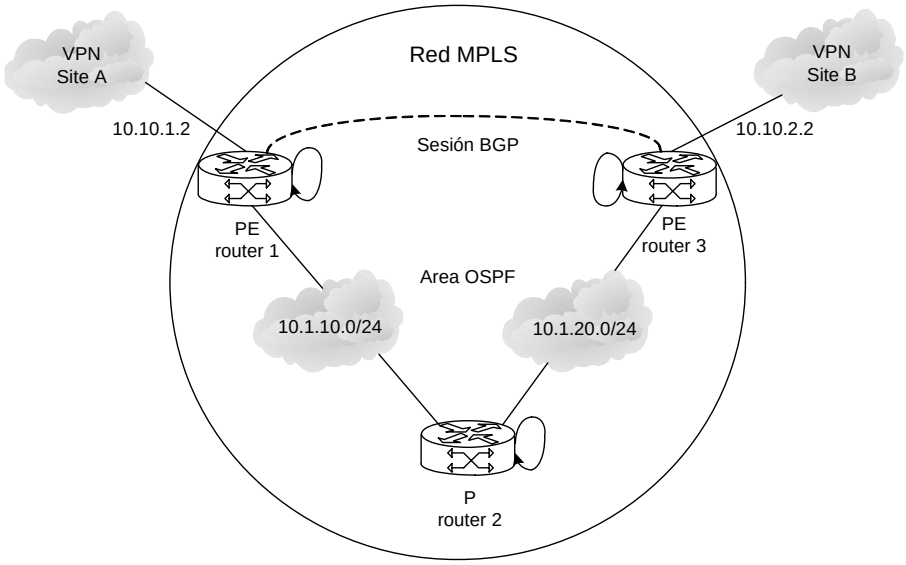

Figura 4.5: Topologia de encaminamiento

CAPÍTULO V

ANÁLISIS COMPARATIVO DE LAS VPN'S CON LA TECNOLOGÍA MPLS

5.1 Comparación entre MPLS y otras opciones para IP VPN'S

Un gran número de empresas y proveedores de servicio consideran MPLS como el servicio de IP VPN entre sedes de mayor calidad. Sin embargo, existen otros dos tipos de IP VPN: IPSec y SSL.

Las IP VPN basadas en la tecnología de Seguridad IP (IPSec) han obtenido éxito ofreciendo acceso remoto a redes de empresas encriptando el tráfico en un túnel que atraviese la Internet pública.

Las IP VPN basadas en SSL (Secure Sockets Layer) permite a los usuarios acceder a sus redes empresariales sobre la Internet pública utilizando un método de best effort, que aprovecha la tecnología de navegador, para ofrecer un nivel de seguridad estándar. Dichos navegadores operan en la capa 7, la de aplicaciones. Como tales, los tipos de aplicaciones a los que puede accederse a través de las VPN's SSL suelen limitarse a los basados en navegadores [17].

Dado que ninguna de las dos versiones es compatible con aplicaciones en tiempo real (como la voz), las redes convergentes de voz y datos requieren el uso de una IP VPN MPLS.

A pesar de que las IP VPN's IPSec han obtenido una gran popularidad, no ofrecen las características de calidad de servicio (QoS) que garantiza MPLS y por lo tanto pueden quedar sujetas a los retrasos de best effort típicas de la Internet

pública. En contraposición, las empresas que utilizan IP VPN's basadas en MPLS disponen de un medio fiable para priorizar su tráfico de aplicaciones y se encuentran en proceso de desplegar otras nuevas, añadir nuevas sedes con mayor facilidad y llevar a término sus negocios con mayores éxitos.

Las IP VNP's MPLS ofrecen una flexibilidad y estabilidad excelentes y pueden desplegarse a la escala necesaria con mayor rapidez que su equivalente de la Internet pública. Las IP VPN's IPSec utilizan túneles encriptados entre sedes, que deben establecerse antes de que la VPN pueda utilizarse, lo que no supone un problema en caso de VPN's de reducidas dimensiones, aunque en el caso de las de mayor tamaño, con requisitos más complejos de encaminamiento de tráfico entre sedes, el resultado puede consistir en un enorme número de túneles de difícil gestión. No obstante, con el MPLS los intercambios entre la sede del cliente y la red IP privada del proveedor de servicios deben establecerse una sola vez para que dicho emplazamiento pueda formar parte de la VPN. Añadir o quitar sedes en el futuro no requerirá por tanto una reconfiguración de la red.

Los proveedores de servicios han adoptado MPLS como una herramienta para gestionar sus flujos de tráfico de red IP y garantizar que la latencia, o el tiempo que trata el tráfico en recorrer la red, se reduce al mínimo, en contraposición al enfoque de best effort de la Internet pública. A su vez, esto significa que en la actualidad MPLS ofrece una calidad de servicio mucho mayor que otros mecanismos de garantía para IP VPN [17].

Cada sesión IPSec debe autentificarse por separado mientras que con MPLS, el proveedor de servicios gestiona esta funcionalidad de forma centrada. Las VPN IP IPSec resultan especialmente inadecuadas para la voz y cualquier otro tipo de tráfico sensible a retardos dado que, no sólo no es capaz de priorizar el tráfico, sino que se introduce además un retardo al encriptar los datos en origen y desencriptarlos en destino. En términos de seguridad IPSec representa una solución de acceso local adecuada, pero ya se ha reconocido que el MPLS ofrece el mismo nivel de seguridad que las soluciones basadas en frame relay o ATM .

	MPLS	IPSec
Calidad de servicio	Ofrece priorización del trafico a través de clases de servicio.	Depende de la Internet pública para el transporte; solamente puede ofrecer el best effort
Coste	Inferior al de frame relay o ATM, aunque superior al de otras IP VPN. Los recortes de costes aumentan si la red tradicional se encuentra fuertemente mallada.	Bajo, dado que utiliza la Internet pública para el transporte.
Seguridad	Comparable a la de las redes tradicionales de frame relay o ATM. La seguridad es más rigurosa que la que se obtiene con IPSec.	Seguridad exhaustiva mediante una combinación de certificados digitales de autentificación y una serie de opciones de encriptación.
Adecuación a aplicaciones	Todas las aplicaciones, incluido el software empresarial de misión crítica que requiere alta calidad y baja latencia, así como las de tiempo real, como el video y la voz IP.	Acceso remoto y móvil seguro. Aplicaciones centradas en IP, como el correo electrónico o Internet. No adecuado para tráfico en tiempo real o de alta prioridad.
Cobertura	Depende de la red MPLS del proveedor de servicios.	Muy extenso, dado que se basa en el acceso a Internet.
Escalabilidad	Altamente escalable, dado que no requiere intercambios entre sedes y cualquier despliegue normal es compatible con decenas de miles de conexiones por VPN.	Los despliegues de grandes dimensiones requieren una planificación cuidadosa que tenga en cuenta el intercambio de tráfico así como otros problemas.
Overheads de red	El encaminamiento no requiere procesamiento.	La encriptación y desencriptación requiere un overhead de procesamiento adicional.
Velocidad de despliegue	El proveedor de servicios debe desplegar un router MPLS en el extremo de la red para permitir el acceso del cliente.	Puede utilizarse la infraestructura de red IP existente.
Participación del cliente	No requiere ninguna. MPLS es tecnología de red.	Requiere software o hardware del cliente.

Tabla 5.1: Comparativa entre MPLS e IPSec

MPLS se ha ido desarrollando simultáneamente a la capacidad de ofrecer seguridad mejorada, lo que incluye la prevención de spoofing de direcciones IP, protección consiguiente contra ataques de Denegación de Servicio (DoS), autentificación de routers (para impedir la introducción de datos falsos)

IPSec se adecua mejor al modelo de red de acceso local e Internet pública, así como aquellas empresas que busquen una IP VPN económica que ofrezcan garantías de calidad de servicio (QoS) limitadas.

MPLS en cambio, se erige como la mejor solución para el modelo de red IP privada en la que una gama completa de sofisticadas garantías de calidad de servicio (QoS) otorgan a las empresas la capacidad de aprovechar al máximo su ancho de banda y gestionar de forma efectiva y predecible su tráfico de aplicaciones.

IPSec representa la herramienta ideal para proporcionar acceso remoto seguro a intranets y extranets corporativas, mientras que MPLS consiste en la solución que mejor se adapta a una calidad de servicio rigurosa sobre una red convergente de voz y datos.

5.2 Razones para migrar a MPLS VPN

En los últimos tiempos, no sólo se viene hablando de la famosa convergencia de voz, video y datos sobre una misma plataforma, sino también de la necesidad de la migración de servicios como ATM o Frame Relay a una nueva generación de IPbased VPNs (Redes Privadas Virtuales basadas en protocolo IP) como los son las MPLS VPNs (Redes Privadas Virtuales basadas en Multiprotocol Label Switching) [18].

Sin embargo, resistencia sigue siendo la primera palabra que se asocia cuando se habla de cambios, mucho más aún, cuando se trata de migraciones de servicios de comunicaciones, críticos para una empresa. A continuación, mencionaremos 10 razones claves para hacer frente a la mencionada resistencia a los cambios.

5.2.1 Flexibilidad

Cada empresa, corporación u organismo tiene desarrollada su propia estructura interna, tanto en infraestructura como en recursos humanos, generadas

en base a sus necesidades y recursos disponibles. En base a ésta estructura, muchas veces única, se montan los servicios de comunicaciones para acomodar de la mejor manera posible y al menor costo, el transporte de la información interna, así como también externa, con sus clientes y proveedores.

La topología de una MPLS VPN puede acomodarse acorde a cada necesidad, dada su naturaleza que brinda conexiones Any-to-Any (cualquiera con cualquiera) entre los distintos puntos que comprenden la VPN, contando así con el mejor camino o ruta entre cada punto. A su vez se puede obtener mayor flexibilidad realizando configuraciones híbridas con Hub-and-Spoke (estrella), por ejemplo en las conexiones con clientes.

5.2.2 Escalabilidad

Con un nuevo concepto de aprovisionamiento, llamado "Point-to-Cloud" (punto a la nube), se implementan los nuevos puntos de la VPN. Este concepto proviene del hecho de que cada vez que sea necesario subir un nuevo punto a la VPN, sólo habrá que configurar el equipamiento del Service Provider que conecte este nuevo punto. De esta forma, evitamos tareas complejas y riesgosas, como las que se producen cuando se activa un nuevo punto en una red basada en circuitos virtuales de Frame Relay o ATM, en donde es necesario re-configurar todos los puntos involucrados.

5.2.3 Accesibilidad

La arquitectura de MPLS VPN permite utilizar prácticamente todos las tecnologías de acceso para interconectar las oficinas del cliente con su Service Provider (Proveedor de Servicios). Por dicho motivo, la versatilidad que nos permite utilizar xDSL o un enlace Wireless Ethernet en las oficinas más pequeñas y hasta incluso en usuarios móviles.

5.2.4 Eficiencia

En una infraestructura 100% IP, es decir, aquellas empresas en donde todo el equipamiento involucrado y las aplicaciones utilizadas son IP-based, el uso de servicios de transporte ATM o Frame Relay someten al cliente a incurrir en un

costo adicional por el overhead que los protocolos de transporte introducen. Mediante MPLS VPN basado en un servicio IP-Based VPN este costo extra desaparece.

5.2.5 Calidad de servicio (QoS) y Clases de servicio (CoS)

Las necesidades de comunicación entre dos lugares remotos, hoy en día van mucho más allá de la simple transferencia de datos vía e-mail, web u otras aplicaciones. Siendo incluso insuficiente muchas veces, la interesante combinación de voz y datos bajo una misma plataforma.

Es por esto, que la ya mencionada Convergencia de datos con aplicaciones real-time o interactivas, voz y también video de alta calidad, necesitan de una eficiente plataforma de transporte.

Mediante la utilización de técnicas y herramientas de Calidad de Servicio (QoS), se ofrecen distintas Clases de Servicio (CoS) dentro de una MPLS VPN para cumplimentar los requerimientos de cada servicio o aplicación.

5.2.6 Administración

Las MPLS VPN son denominadas Network-Based, ésta característica proviene del hecho en que el servicio es implementado sobre la infraestructura del Service Provider; implicando, entre otras cosas, que la administración de enrutamiento es llevada a cabo por el Service Provider; quien por su naturaleza, es especialista en dicha tarea desligando así al cliente de llevarla a cabo.

5.2.7 Monitoreo

Las MPLS VPN son monitoreadas, controladas y con un constante seguimiento en forma permanente, las 24 horas los 7 días de la semana, por parte del Service Provider. Además, se extienden "Service Level Agreements" (acuerdos de nivel de servicio) para garantizar y asegurar la estabilidad y performance que el cliente necesite.

5.2.8 Fácil Migración

La simplicidad de la tecnología determina que las tareas de aprovisionamiento, administración y mantenimiento sean actividades sencillas para el Service Provider; lo cual se traslada directamente al cliente, obteniendo una migración del servicio actual sin complicaciones.

5.2.9 Seguridad

Análisis y estudios realizados por los distintos fabricantes y entidades especializadas en el área, determinaron que los niveles de seguridad entregados por una MPLS VPN son comparables con los entregados por los circuitos virtuales de Frame Relay y ATM.

Sin embargo, en escenarios donde estos niveles no son suficientes, como por ejemplo en las necesidades de entidades financieras, una MPLS VPN puede también ser combinada con la encriptación y autenticación que IPSec brinda, elevando aún más la seguridad de la VPN.

5.2.10 Bajo Costo

Siempre que se hable de reducir costos contribuirá fuertemente a inclinar la balanza. Son varios los motivos que permiten afirmar que un servicio MPLS VPN ofrece más por menos, entre ellos podemos destacar:

- Independecia de equipos de cliente (CPE): al ser un servicio Network-based, la implementación de la VPN no requiere un hardware específico ni costoso para ser instalado en las oficinas del cliente.
- Convergencia: por ser una VPN CoS-Aware (Soporte de Clases de Servicio) se puede integrar distintos servicios y aplicaciones sobre una misma plataforma. De este modo, empresas que al día de hoy mantienen distintos y costosos servicios para soportar sus necesidades de voz, datos y video; pueden unificar estos requerimientos concluyendo en un ahorro significativo y manteniendo relación con un único proveedor de servicios.

CAPÍTULO VI

LAS AMENAZAS A MPLS VPN

6.1 Las VPN's

Las VPNs son el elemento básico para la interconexión de sedes y proporcionar a los Clientes transferencia de datos privada. Pero como para todos los elementos, existen posibles amenazas de la red. Las más probables pueden llegar: desde el interior o desde un ataque DoS.

6.1.1 Posibles Intrusos

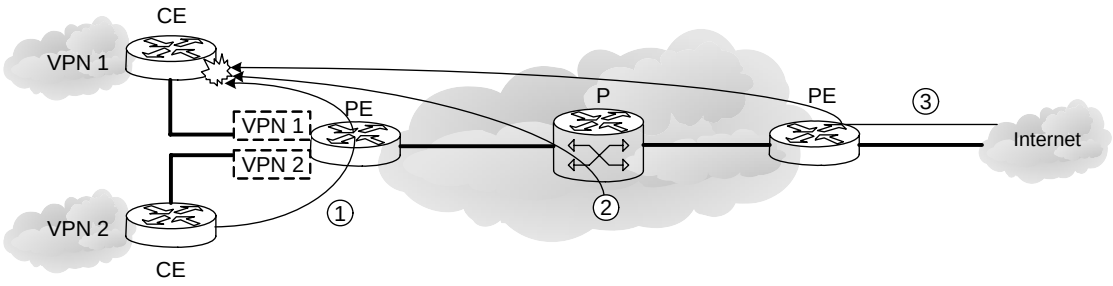

Figura 6.1: Posibles puntos de intrusión

En la figura 6.1 se muestran dos VPN's con una sola red base. Una de las VPNs dispone de una conexión a Internet. Esta, precisamente, sirve para mostrar los 3 grandes focos de posibles amenazas [9]:

- Amenazas de otras VPN's (1): Las interfaces externas de las PEs son visibles, y por ello pueden ser un centro de posibles ataques. Estos ataques, posiblemente de DoS, podrían afectar al servicio del resto de VPN's en el mismo PE. De todas maneras, la separación de VPN's ayuda

preservar la seguridad entre VPN's con lo que los posibles ataques a una VPN no deberían afectar ni al resto de VPN's ni al core.

- Amenazas del propio core (2): En caso de que se desconfiguraran las rutas, podría provocar que VPN's que no deberían estar unidas lo estuvieran. Con lo que usuarios externos podrían introducirse en la red del cliente. Este tipo de desconfiguraciones pueden ser fortuitas o provocadas.
- Amenazas de Internet (3): Es muy sencillo considerar Internet como una gran amenaza, teniendo en cuenta la gran cantidad de virus y troyanos que circulan por ella.

De todas maneras, siempre se recomienda que los clientes instalen un firewall para evitar posibles amenazas externas, y filtrar aquellas rutas que no pertenezcan a su propia VPN.

6.1.2 DoS

El ataque de negación de servicios es la amenaza más potente a la que se enfrenta cualquier elemento de red. Comparado con el caso anterior, en que una buena gestión de la entrada de paquetes (a través de un firewall, por ejemplo) puede controlar la amenaza, en DoS se deben tomar más medidas.

Los puntos por donde se puede colar este tipo de amenaza, se extiende a toda la red (tal y como muestra la figura 6.2). Tanto pueden originarse en el core (PEs y Ps), como por redes externas como Internet o extranets.

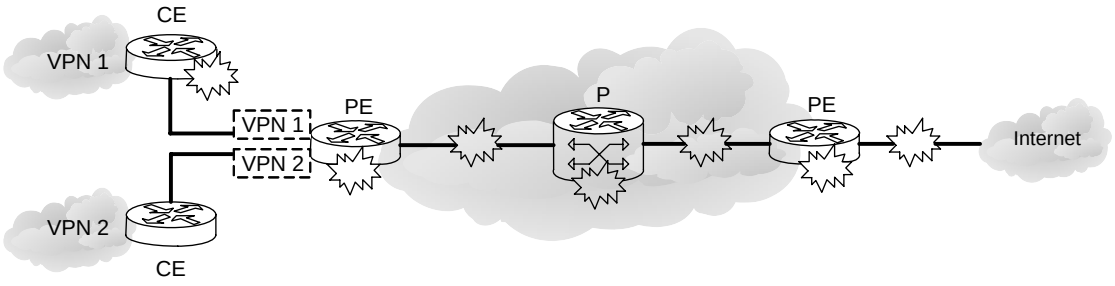

Figura 6.2: Posibles puntos de ataque de DoS

Por otro lado, y como se comentó, el ataque a una PE con DoS puede llegar afectar al resto de VPNs de la PE. De forma que sus recursos se reduzcan, unque el ataque no pasaría a las VPNs ni a sus sedes.

6.2 La Extranet

Por extranet se puede entender:

- Intranet y extranet integrados: El propósito de este tipo de conexiones es unir diversas VPNs entre sí.
- Central de servicios: En este caso la idea es que diversas VPNs tengan una sede, un punto en común.

Desde el punto de vista de seguridad, este tipo de uniones padecen el mismo tipo de amenazas que para un VPN sola. Ya que, a nivel lógico, para un PE estas VPN o sedes VPN también son una sola VPN.

De igual manera, la inclusión de un firewall ayuda a mantener al separación requerida entre las redes privadas de cada sede y las del resto de sedes añadidas.

6.3 El Core

Un backbone ATM es una fuente de posibles ataques, y como en todas las redes, MPLS VPN también tiene su repertorio. Las diferentes maneras de presentar el core: única o múltiple (Inter-AS, CsC); contienen más o menos las mismas precauciones [9].

Por otra parte, existe también una red llamada NOC (Network Operations Center) que gestiona todas las operaciones entre redes. Esta red vinculada a nivel lógico con la red, también debe ser comentada por su implicación con las redes externas como Internet y Extranets.

6.3.1 Core único

Como bien dice el encabezamiento, el core único (o core monolítico) lo forma una sola red base. Este tipo de infraestructura puede padecer las siguientes amenazas:

- Intrusiones desde el exterior: La única manera de poder protegerse de este tipo de ataques, es creando un buen control de las operaciones internas. Es evidente, observando las diferentes figuras, que el primer punto por donde se pueden producir los ataques es por una PE. De cualquier manera, ni las VPNs ni Internet no pueden acceder al core. La única comunicación que existe es entre los PEs y los CEs. Aunque estos pueden filtrar el tráfico únicamente a las interfaces y los puertos permitidos.
- DoS desde el exterior: Cualquier parte del core MPLS es potencialmente vulnerable a un ataque de este tipo desde Internet o una VPN. Sin embargo, la imposibilidad del acceso desde el exterior al core, hace que este tipo de ataque se rebaje a una inundación al PE y la VPN afectada. La única manera de asegurar el core, es haciendo que los servicios y requerimientos de QoS se cumplan (al menos los mínimos) tanto en los PEs como el en resto del core, a pesar de padecer un ataque DoS.
- Internas, como la desconfiguración: La desconfiguración de las rutas, pueden causar serios problemas entre VPNs. La asociación de VPNs que no debieran estar unidas, podría hacer que los virus, troyanos, gusanos y otras amenazas existentes en una red descuidada, pasaran también a otro Cliente. Por eso se recomienda a los clientes que sitúen firewalls en las entradas a sus redes. Por otro lado, los operadores instalan en sus redes controles que vigilan los movimientos de los equipos.

6.3.2 Inter-AS

Si en el caso anterior se trataba de una sola red core, en este pasamos a situar múltiples redes de servicios como se observa en la figura 6.3. En este tipo de uniones se siguen padeciendo las mismas amenazas que en el caso de una red única, aunque añadiendo las posibles amenazas procedentes de AS’s

(Autonomous System) vecinos. A nivel de VPN, el riesgo que pueden correr aquellas VPNs que atraviesan varios AS es mayor que si sólo atravesaran uno. Aún así, las VPN's no saben distinguir si han cruzado uno o varios AS's.

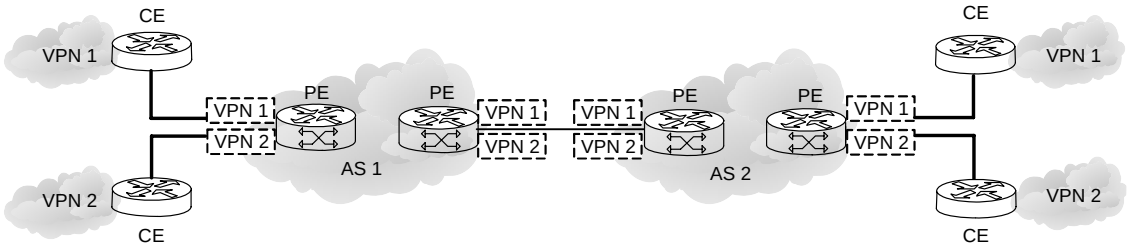

Figura 6.3: Arquitectura de Inter-AS

En el RFC 2547 (BGP/MPLS VPN's) se describen tres posibles modelos (llamados A, B y C). A nivel técnico, el modelo A es mucho más restrictivo y no hace aumentar los riesgos significativamente. En cambio, los modelos B y C, permiten más interacción entre los AS's lo cual incrementa el riesgo de intrusiones y ataques DoS entre AS's. Dependiendo del modelo, se pueden considerar las siguientes amenazas:

- Para cada VPN, cada AS puede introducir nuevas sedes conectadas a la VPN. Esto aumenta el riesgo de amenaza por ataque DoS o intrusión.
- El enrutado entre AS's supone un gran riesgo para los PEs, ya que pueden padecer ataques de ASs vecinos.
- En los modelos B y C cada AS puede enviar tráfico a través de una VPN de otra AS, sea o no compartida. Este tipo de situaciones puede ser utilizada para ataques DoS o intrusiones.

6.3.3 Carrier's Carrier (CsC)

Este modelo consigue una asociación jerárquica entre ASs. En la figura 6.4, el AS2 es un "Customer Carrier", el cual utiliza al AS1 (Provider Carrier) para transportar la información a las sedes de las VPN's del otro extremo. Para AS1, la información sobre los distintos Clientes no le importa. En este caso el AS1

solamente transporta los paquetes enviados a través de la interfaz común (CEPE).

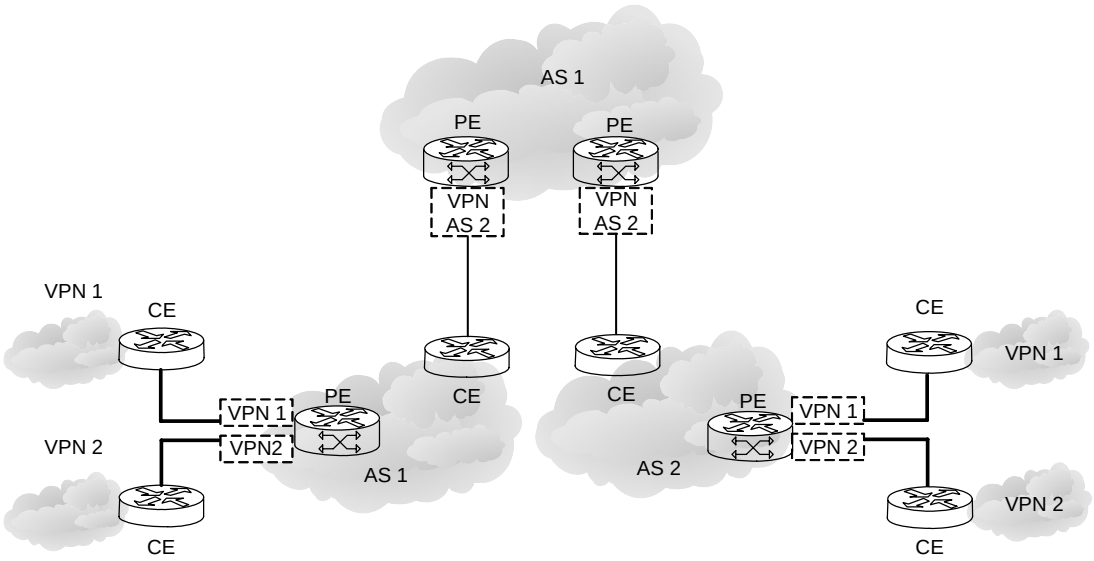

Figura 6.4: Arquitectura de CsC

Para poder hacer el transporte de los paquetes, el AS1 añade una etiqueta a la etiqueta que añade AS2 en el PE de su red. Tal y como ocurre en el caso del etiquetaje único, para el proveedor (AS1), sólo le interesa su etiqueta. De la misma manera que para el AS2, la etiqueta de AS1 no tendría ningún sentido.

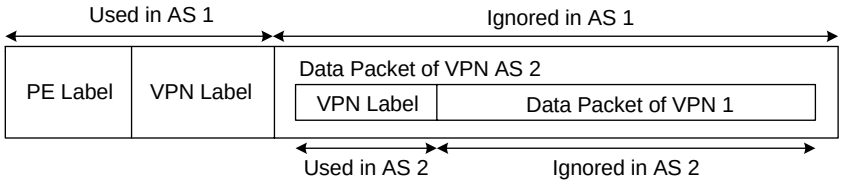

Figura 6.5: Etiquetaje en AS 1

La utilización de este tipo de etiquetaje (ver figura 6.5) provoca que no sea posible atacar la red AS1 desde AS2, ya que las direcciones permanecen ocultas como para el caso de una simple AS. Así pues, cualquier ataque contra el CsC no

supondría una amenaza. El ataque se mantendría dentro del dominio de AS2 o dentro de su VPN.

6.3.4 Network Operations Center (NOC)

Estas redes de control están lógicamente separadas de la red core. Pueden existir más de una pero permanecen independientes entre sí [9].

Sus operaciones, abarcan todas las redes externas que puede tratarse en una backbone: Internet, Intranet, y otras redes (como se ilustra en la figura 6.6). Las amenazas pueden llegar de cualquiera de las redes. Las intrusiones producidas por estas redes pueden atacar las redes de gestión o sistemas como servidores FTP (File Transfer Protocol) y TFTP (Trivial File Transfer Protocol), servidores AAA (Authentication, Authorization, and Accounting), etc.

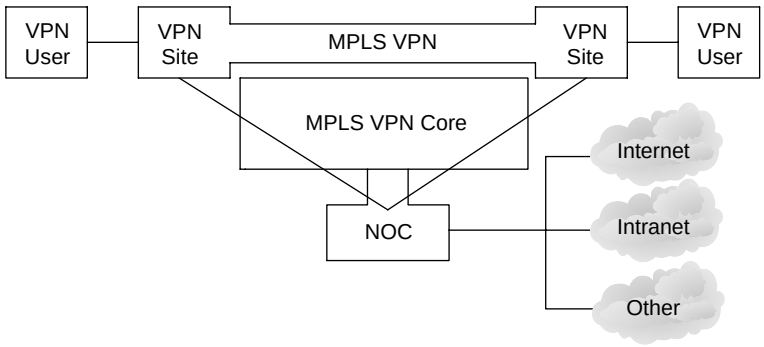

Figura 6.6: Esquema de NOC

Los posibles ataques a este tipo de redes pueden producir grandes efectos en la gestión y el mantenimiento de las redes. Por esta razón, los proveedores procuran proteger sus redes de operaciones a través de filtrajes y listas de acceso.

6.4 Internet

Internet es una red insegura para todos sus usuarios, y puede suponer un problema para los proveedores de servicios. Todos los usuarios de esta red, tal y como se recomienda a los Clientes de los proveedores de servicios, tendrían que

asegurar sus redes. Por ejemplo, la utilización de simples firewalls apaciguaría un poco todas las amenazas existentes en la red.

Aún así, los proveedores de servicios deben aplicar grandes medidas de seguridad para evitar los posibles ataques spoofing y DoS. Una manera sería la incorporación de filtrado de paquetes en los routers de entrada.

6.5 Zonas de Confianza – Zonas Inseguras

Se entiende por zonas de confianza, los puntos compartidos por dos redes o VPN's. El uso inseguro de estas zonas, puede facilitar el paso a posibles ataques de las redes vecinas [9].

A veces no se tiene en cuenta que la zona de confianza esta situada justo en una zona conectada a una red MPLS. Es evidente que este tipo de zonas, y por el compromiso mutuo que debe existir en temas de seguridad entre el proveedor y el cliente, debe protegerse. Algunas de los puntos olvidados son:

- Punto de acceso wireless sin control de acceso en una empresa con servicio MPLS VPN.
- Un ataque DoS desde Internet a un servidor web de una red VPN, donde tanto la VPN como el servicio Internet son proporcionados por el mismo core MPLS.
- Un intruso desde una VPN MPLS dentro de otra VPN, atravesando los puntos de la interconexión que se diseñan específicamente para este propósito, por ejemplo Extranets.
- Infecciones por gusanos procedentes de una sede VPNs a otra, de una extranet que las conecta entre sí. Como en muchos otros casos, las dos últimas situaciones se pueden resolver con la colocación de un firewall. Con la correcta gestión de los filtros, se puede asegurar una buena protección contra amenazas externas, y también las de la propia VPN.

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1 CONCLUSIONES

- Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha convertido en un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro.

- MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel (o conmutación IP). La idea básica de separar lo que es el envío de los datos (mediante el algoritmo de intercambio de etiquetas) de los procedimientos de encaminamiento estándar IP, ha llevado a un acercamiento de los niveles 2 y 3, con el consiguiente beneficio en cuanto a rendimiento y flexibilidad de esta arquitectura.

- El hecho de que MPLS pueda funcionar sobre cualquier tecnología de transporte, no sólo sobre infraestructuras ATM, facilita de modo significativo la migración para la próxima generación de la Internet óptica, en la que se acortará la distancia entre el nivel de red IP y la fibra.

- MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP (típicamente limitadas a encaminar por dirección de destino). Además de poder hacer ingeniería de tráfico IP, MPLS permite mantener clases de servicio y soporta con gran eficacia la creación de VPNs. Por todo ello, MPLS aparece ahora como la gran promesa y esperanza para poder mantener el ritmo actual de crecimiento de la Internet.

7.2 RECOMENDACIONES

- Se recomienda realizar un estudio al interior de la ESPE para la implementación de Redes Privadas Virtuales (VPN) utilizando tecnología MPLS (Multi-Protocol Label Switching) entre las distintas sedes y que permita el acceso al personal directivo y docente de la Universidad a la red privada de la misma. Como resultado de este estudio debería salir un cuadro comparativo donde se demuestre el ahorro mensual que tendría la Universidad con la implementación de VPN's.

- Otra recomendación es evaluar y proponer a una entidad cuya misión crítica sea la protección de su información para abandonar sus enlaces WAN tradicionales y migrar a una topología VPN. Como resultado de este trabajo debería salir una solución VPN MPLS que involucrara la implementación de un sistema de llaves públicas y los más avanzados algoritmos de encriptación y autenticación.

- Un trabajo que se propone a raíz de este, es la implementación de VPN's MPLS para la interoperabilidad de los protocolos IPv4 e IPv6. Esto es poder encapsular paquetes IPv6 dentro de paquetes IPv4 para que puedan transitar por redes nativas IPv4 y desencapsularlos al final de un gateway detrás del cual exista una red con dispositivos IPv6.

BIBLIOGRAFÍA

[1] usuarios.lycos.es/janjo/janjo1.html, Protocolos TCP/IP.

[2] tau.uab.es/~gaby/DEA/1%20Los%20protocolos%20TCPIP.pdf, Los Protocolos TCP .

[3] www.ucaribe.edu.mx/archivos/freyes/IT0103/cbxc_ip.pdf, Tutorial de Redes.

[4] trajano.us.es/~rafa/ARSS/apuntes/tema7.pdf, Redes de Datos.

[5] www.mailxmail.com/curso/ informatica/redes/capitulo13.htm, Redes IP.

[6] es.wikipedia.org/wiki/CIDR, CIDR.

[7] www.info-ab.uclm.es/sec-ab/Tecrep/diab-01-02-16.pdf, Protocolos de Encaminamiento

[8] bibliotecnica.upc.es/PFC/arxius/migrats/40628-2.pdf, Desarrollo de Plano de Gestión para una Red MPLS.

[9] bibliotecnica.upc.es/PFC/arxius/migrats/40393-2.pdf, Análisis de la Seguridad en IP/MPLS VPN: Comparación con ATM.

[10] eiee.univalle.edu.co/~telecomunicaciones/tesis/VPN/VPN-UV.pdf, Como Escoger e Implementar una VPN. Conceptos Teóricos y Prácticos.

[11] telematica.cicese.mx/revistatel/ archivos/Telem@tica_AnoIII_No22.pdf, Telematica.

[12] www.ifxnetworks.com/document/IFX_MPLSWhitePaper_sp.pdf, IFX MPLS/VPN White Paper.

[13] wap.alcatel.es/tecno/tribuna/ intmov/im_seguridadcalidad.htm, Alcatel Navigate.

[14] redcetus.com/vpn.html, Redes Privadas Virtuales.

[15] mplslab.upc.es/Publicaciones/Paper%20-%20Hesselbach%20-%20final%20-%203er%20MPLS%20Workshop.pdf, Problemas abiertos en MPLS.

[16] exa.unne.edu.ar/depar/areas/ informatica/SistemasOperativos/MPLS.pdf, MPLS “Multiprotocol Label Switching”

[17] www.idg.es/comunicaciones/conocimiento/pdfs/ip%20vpn%20white%20paperSP.pdf , Tendencias emergentes en servicios paneuropeos de IP VPN.

[18] www.ifxnetworks.com/document/10razones_mpls.pdf, Diez razones para migrar a MPLS VPN.

HOJA DE ENTREGA

Este proyecto de grado fue entregado al Departamento de Ingeniería Eléctrica y Electrónica y reposa en la Escuela Politécnica del Ejército desde:

Sangolquí, a del 2006

Elaborado por:

_____

Winston Javier Castillo Cevallos

Autoridades:

_____

Sr. Ing. M.Sc. Gonzalo Olmedo

Coordinador de Carrera de Ingeniería en Electrónica y Telecomunicaciones

_____

Sr. Abg. Jorge Carvajal

Secretario Académico del Departamento de Eléctrica y Electrónica