ESCUELA SUPERIOR POLITECNICA DEL LITORAL

FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACION

"SEGURIDAD POR MEDIO DE UNA RED PRIVADA VIRTUAL (VPN) SOBRE IP/MPLS"

PROYECTO DE TOPICO DE GRADUACION

Previa a la obtención del Titulo de:

INGENIERO EN ELECTRONICA Y TELECOMUNICACIONES

Presentada por:

IVONNE ISABEL SABANDO MENDOZA

CRISTIAN PARRALES TENELEMA

DANIEL HENRY IDROVO ACURIO

GUAYAQUIL – ECUADOR

2004

AGRADECIMIENTO

A Dios por habernos dado la sabiduría para trabajar y la fortaleza para avanzar en nuestra formación académica y personal.

A nuestros compañeros, amigos, profesores y a todas las personas por habernos dado su ayuda en el desarrollo de este trabajo.

A todos ellos un millón de gracias y que Dios los bendiga.

DEDICATORIA

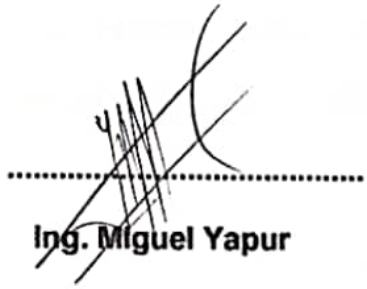
A Dios por haberme dado el maravilloso don de la vida.

A mis padres por su respaldo y apoyo incondicional.

A todos mis amigos por su ayuda.

Para todos ellos les dedico esta obra, pues les pertenece.

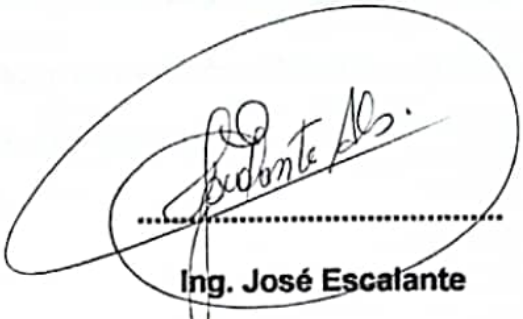
TRIBUNAL



.....

Ing. Miguel Yapur

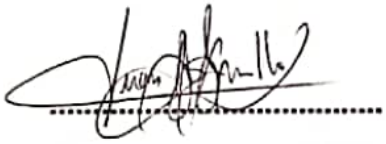
SUB-DECANO



.....

Ing. José Escalante

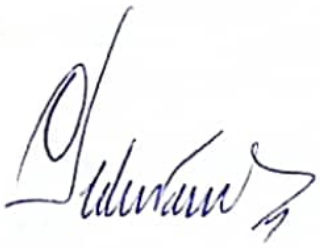
DIRECTOR DE TOPICO



.....

Ing. Juan Carlos Aviles

M. PRINCIPAL



.....

Ing. Pedro Vargas

M. PRINCIPAL

DECLARACION EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestas en este trabajo, nos corresponden exclusivamente; y el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL".

(Reglamento de Exámenes y Títulos Profesionales de la ESPOL).

Ivonne Sabando Mendoza

Cristian Parrales Tenelema

Daniel Idrovo Acurio

RESUMEN

El presente trabajo trata sobre la Seguridad por medio de VPN sobre IP/MPLS, las mismas que brindaran a los usuarios mayor seguridad en la información que transmitan dentro del Backbone de ETAPA, para lo que se diseñará uno nuevo.

Primero se tratará sobre Seguridad y protocolos de capa 2 y 3, la seguridad ha sido un elemento importante porque ha tomado relevancia en la última década en el mundo de la Computación y de las Comunicaciones, que con el crecimiento exponencial del uso de Internet se han creado intereses de muchas índoles sobre los recursos disponibles en las redes, lo que ha obligado a invertir en Mecanismos de Seguridad, para proteger la información. Para ello se utilizan protocolos que brindan seguridad en la red como son IPSec a nivel de capa 3 y los protocolos de transporte a través de sus circuitos virtuales.

Las Redes Privadas Virtuales (VPN) empezaron a evolucionar debido a los elevados costos de mantener líneas dedicadas. 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. MPLS tiene características de las dos al ser una red conmutada que usa etiquetas para enrutar paquetes.

Uno de los grandes problemas de la Internet actual es que no garantiza la calidad de servicio. La sencillez de TCP/IP hace que su eficiencia sea variable, y por lo tanto los paquetes se entregan de la mejor forma posible, estos hechos provocaron que se comenzaran a explorar soluciones que contribuyesen a superar estas limitaciones. MPLS (Multiprotocol Label Switching: conmutación de etiquetas multiprotocolo) es un estándar del IETF (Internet Engineering Task Force) que surgió para unificar las diferentes soluciones que los distintos fabricantes estaban proponiendo. Está basado en el uso de etiquetas que identifican la ruta para encaminar los paquetes, MPLS surgió de tecnologías similares existentes.

Los estándares MPLS ofrecen actualmente dos opciones para la distribución de las etiquetas usadas para encaminar los paquetes. La primera de ellas, conocida como RSVP, fue definida para reservar recursos de red para los flujos individuales con el fin de garantizar la calidad de servicio del mismo. LDP es la segunda opción disponible actualmente. Este protocolo ha sido definido expresamente por los expertos involucrados en la especificación de los estándares MPLS en el IETF.

Las aplicaciones de IP/MPLS que se pueden dar en ETAPA son muchas y una de estas aplicaciones es el comercio electrónico debido a la seguridad y calidad de servicio que la red experimenta aplicando esta tecnología, además de dar el servicio de carrier a los clientes gracias a la gran capacidad del nuevo Backbone.

Por último se muestra el diseño de la nueva red de ETAPA, además de mostrar las configuraciones de los equipos, como los routers, para que funcionen formando una VPN sobre IP/MPLS y el diseño de la VPN para los usuarios con IPSec. También se muestra el análisis financiero del proyecto para su ejecución.

INDICE GENERAL

ABREVIATURAS

ARIS	Aggregate Route-based IP Switching
ATM	Modo de Transferencia Asíncrono
B2B	Negocio a Negocio
B2C	Negocio a Consumidor
B2E	Negocio a Empleado
B2G	Negocio a Gobierno
BECN	Notificación de Congestión Explícita de Reenvío
BGP	Protocolo de Gateway Fronterizo
B-ISDN	Redes Digitales de Servicios Integrados de Banda Ancha
CBR	Constraint-Based Routing
CBS	Tamaño de Ráfagas Garantizada
CDN	Call-Disconnect-Notify
CDR	Velocidad de Datos Garantizada
CE	Router del Cliente
CHAP	Challenge Handshake Authentication Protocol
CIR	Committed Information Rate
CPE	Equipo Terminal del Cliente
CR-LDP	Enrutamiento Basado en Restricciones LDP
DCE	Equipo de Terminación de Circuito de Datos
DE	Discard Eligibility
DES	Encriptación de Datos Estandar
DLCI	Identificador de Conexión de Enlace de Datos
DNS	Servidor de Denominación de Nombre
DoI	Domain of Interpretation
DoS	Denegación de Servicio
DS	DiffServ

DTE	Equipo Terminal de Datos
DWDM	Multiplexación por División de Longitud de Onda
EBS	Tamaño de la Ráfaga en Exceso
EDI	Intercambio Electrónico de Datos
EIA	Asociación de Industrias Electrónicas
ESP/AH	Encapsulating Security Payload/Authentication Header
FANP	Flow Attribute Notification Protocol
FEC	Forwarding Equivalence Class
FECN	Notificación de Congestión Explícita de Envío
FIFO	Primero en Entrar Primero en Salir
FRAD	Ensamblador/Desensamblador Frame Relay
FRND	Dispositivo de Red Frame Relay
FTP	Protocolo de Transferencia de Archivos
GRE	Generic Routing Encapsulation
GSMP	General Switch Management Protocol
HEC	Header Error Corrección
HTTP	Protocolo de Transferencia de Hiper Texto
IANA	Internet Assigned Numbers Authority
ICCN	Incoming-Call-Connected
ICMP	Protocolo de Mensajes de Control de Internet
ICRP	Incoming-Call-Reply
ICRQ	Incoming-Call-Request
ICV	Integrity Check Value
IDEA	Algoritmo Internacional de Encriptación de Datos
IETF	Internet Engineering Task Force
IFMP	Ipsilon Flow Management Protocol
IGP	Protocolo de Gateway Interior
IKE	Interchange Key Exchange
ILM	Incoming Label Map
IP	Protocolo de Internet
IPSec	Protocolo de Seguridad de Internet
IS-IS	Intermediate System to Intermediate System
ISO	Organización Internacional de Estándares
ISP	Proveedor de Servicios de Internet
ISR	Integrated Switch Routers

L2F	Layer-2-Forwarding
LAC	Concentrador de acceso L2TP
LAN	Red de Área Local
LCP	Protocolo de Control de Enlace
LDP	Label Distribution Protocol
LNS	Servidor de Red L2TP
LSP	Camino de Conmutación de Etiquetas
LSR	Label Switching Router
MAC	Códigos de Autenticación de Mensaje
MD5	Message Digest 5
MPEs	Multiprotocol Extensions
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encriptation
MTU	Unidad Máxima de Transmisión
NAT	Network Address Translation
NCPs	Protocolos de Control de Red
NLRI	Información de Alcance del Nivel de Red
NLSP	Protocolo Network Layer Security
OCCN	Outgoing-Call-Connected
OCRP	Outgoing-Call-Reply
OCRQ	Outgoing-Call-Request
OSI	Open Systems Interconnetion
OSPF	Primera Ruta Libre más Corta
PAC	Concentrador de Acceso PPTP
PAD	Ensamblador/ Desensamblador de Paquetes
PAP	Protocolo de Autenticación de Passwords
PBS	Tamaño de Pico de la Ráfaga
PDR	Velocidad de Pico de Datos
PDU	Protocol Data Unit
PE	Límite del Proveedor
PE	Router de Contorno del Proveedor
PHB	Per-Hop Behavior
PKI	Infraestructura de Llaves Públicas
PMTU	Protocol Maximum Transfer Unit
PNS	Servidor de Red PPTP

PPP	Protocolo Punto-a-Punto
PPTP	Point-to-Point Tunneling Protocol
PS	Proveedor de Servicios
PTLS	Protocolo Transport Layer Security
PVC	Circuito virtual Permanente
QoS	Calidad de Servicio
RAS	Servicio de Acceso Remoto
RDSI	Red Digital de Servicios Integrados
RRAS	Servicio de Enrutamiento de Acceso Remoto
RSVP	Protocolo de Reserva de Recursos
RSVP-TE	Protocolo de Reserva de Recursos con túneles LSP
SA	Asociaciones de Seguridad
SAFI	Identificador de Familias de Direcciones Consecutivas
SCCCN	Start-Control-Connection-Connected
SCCRP	Start-Control-Connection-Reply
SCCRQ	Start-Control-Connection-Request
SDH	Synchronous Digital Hierarchy
SHA	Secure Hash Algorithm
SILS	Standard for Interoperable LAN Security
SLI	Set-Link-Info
SMTP	Protocolo de Transferencia de Mail Simples
SONET	Synchronous Optical Network
SP	Proveedor de Servicios
SPD	Security Policy Database
SPI	Índice de Parámetros de Seguridad
SSL	Secure Sockets Layer
StopCCN	Stop-Control-Connection-Notification
SVC	Circuito Virtual Conmutado
TCP	Protocolo de Control de Transmisión
TDM	Multiplexación por División en el Tiempo
TIR	Tasa Interna de Retorno
TLV	Tipo-Longitud-Valor
TLV ER	TLV de camino explícito
TMAR	Tasa Mínima Atractiva de Retorno
ToS	Tipo de Servicio

TTL	Tiempo de Vida
UBR	Unspecified Bit Rate
UDP	Protocolo de Datagrama de Usuario
UNI	User Network Interfases
VAN	Valor Actual Neto
VC	Circuito Virtual
VCI	Virtual Circuit Identifier
VPI	Virtual Path Identifier
VPN	Red Privada Virtual
WAN	Red de Área Amplia
WEN	WAN-Error-Notify

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCION

En el primer capitulo de este trabajo se analizará sobre los protocolos y los mecanismos de seguridad que se deben tomar en cuenta para proteger la información.

En el segundo capitulo analizaremos como poder realizar un VPN, así como las tecnologías de túneles para crear las VPN.

En el tercer capitulo analizaremos conceptos básicos, sobre la Conmutación Multinivel (Multilayer Switching), así mismo su arquitectura, los protocolos que se utilizan en esta tecnología y sus aplicaciones.

En el cuarto capitulo se explicará de las posibles aplicaciones que la nueva tecnología puede brindar a ETAPA.

En el quinto capitulo se observará el nuevo diseño del Backbone de ETAPA, así como la configuración de los equipos involucrados en ese diseño. También se mostrará el diseño de una VPN para un usuario determinado junto con su configuración. Por ultimo en este capitulo se analizará el aspecto económico y financiero del proyecto para su ejecución.

CAPITULO 1

SEGURIDAD Y PROTOCOLOS

1.1. SEGURIDAD DE REDES.

1.1.1. SEGURIDAD DE INFORMACIÓN

Los objetivos principales en Seguridad son: Prevenir la revelación, la modificación y la utilización no autorizada de datos, recursos de computadora y de red. La definición del estándar ISO define cinco elementos fundamentales que constituyen la seguridad de un sistema: La confidencialidad de los datos, la autenticación de los datos, la integridad de los datos, el control de acceso (disponibilidad) y el no repudio.

Confidencialidad implica que la información sea únicamente accesible para las entidades, sistemas o personas autorizadas. Autenticación define mecanismos para garantizar la procedencia de la información,

sea a nivel de usuario o de computadora. Integridad indica que los datos no han sido modificados o corrompidos de manera alguna desde su transmisión hasta su recepción. El control de acceso establece la forma en que el recurso está disponible cuando es requerido. El no repudio es la garantía de transmisión y recepción de información, busca proteger al emisor de que el receptor niegue haber recibido el mensaje, y proteger al receptor de que el transmisor niegue haber enviado el mensaje.

En seguridad de información, se consideran seis elementos sobre los cuales se han hecho desarrollos en busca de proporcionar ambientes protegidos:

1. ***Seguridad física*:** Un elemento de atención básica, los recursos deben ser protegidos físicamente de accesos no autorizados, accidentes, robos, etc.
2. **Segu*ridad de procedimientos*:** Elemento enfocado a las medidas de protección en los procesos y procedimientos.
3. ***Seguridad de personal*:** Elemento enfocado a la definición de privilegios, y accesos de personal involucrado con los recursos.
4. ***Seguridad de emanación de compromisos*:** Elemento enfocado a la definición de responsabilidades y compromisos en el manejo de la información.

5. ***Seguridad de sistemas operativos*:** Elemento enfocado a la protección de servicios y usuarios, accesos no autorizados al sistema operativo de una computadora.
6. ***Seguridad de comunicaciones*:** Elemento enfocado a la transmisión segura de información a través de medios de comunicación.

Prevención es la palabra clave en Seguridad, se han desarrollado algunas técnicas y herramientas de prevención a nivel de aplicaciones, siempre dependientes del sistema operativo o la aplicación que se utilice. Los protocolos de seguridad siempre buscan ofrecer servicios de seguridad en la transmisión de información, sin importar el tipo, procedencia, sistema operativo o aplicación que la genere.

1.1.1.1. VULNERABILIDADES.

El software está diseñado por humanos, quienes diseñan e implantan programas a su criterio, concepto y conocimiento del lenguaje de programación que utilizan, es común, encontrar imperfecciones en los sistemas. Son estas imperfecciones las que propician oportunidades para accesos no autorizados, las que se conocen como vulnerabilidades de los sistemas.

De acuerdo a la figura 1.1, las cuatro categorías generales de vulnerabilidades que se utilizan en la actualidad son las siguientes:

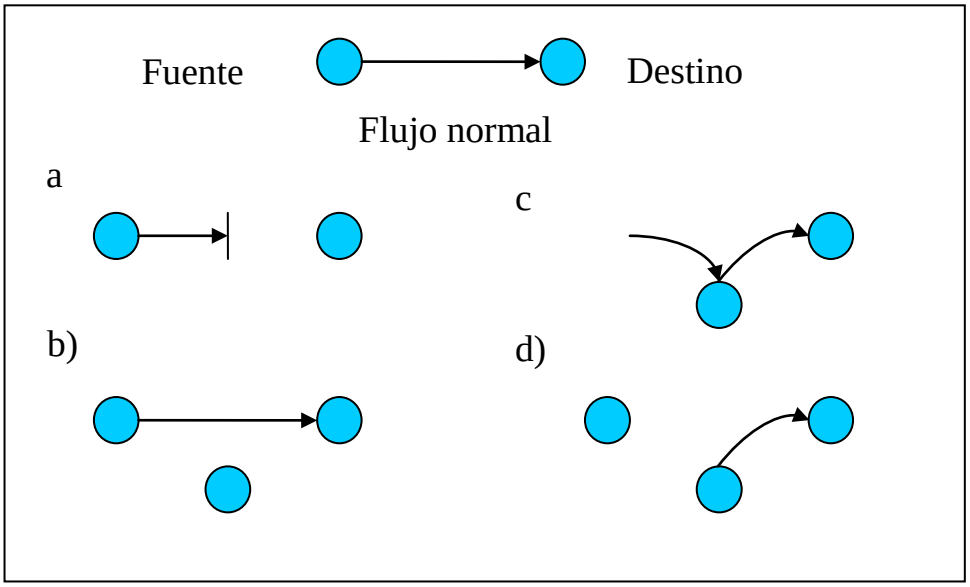


Figura 1.1 Categorías de vulnerabilidades a la seguridad. a) Interrupción, b) Intercepción, c) Modificación, d) Falsificación.

1. ***Interrupción*:** Es una amenaza contra la disponibilidad, el ataque ocasiona que un recurso del sistema deje de estar disponible. Ejemplos: DoS, destruir un elemento de hardware o cortar una línea de comunicación.
2. ***Intercepción*:** Es una amenaza contra la confidencialidad, el ataque produce la captura no autorizada de información en el medio de transmisión. Ejemplos: *Sniffers*, lectura de cabeceras, intercepción de datos.

3. ***Modificación*:** Es una amenaza contra la integridad, el ataque produce no solo el acceso no autorizado a un recurso sino también la capacidad de manipularlo. Ejemplos: Modificación del contenido de mensajes interceptados, alterar programas para modificar su funcionamiento.
4. ***Falsificación*:** Es una amenaza contra la autenticidad, el ataque produce que una entidad no autorizada inserte mensajes falsos en el sistema. Ejemplos: Sustitución de usuarios, alterar archivos, inserción de mensajes espurios en la red.

1.1.1.2. FORMAS DE ATAQUES A LA RED

Los ataques son los medios por los que se explotan las vulnerabilidades. Se identifican dos tipos de ataques: extracción (wiretapping) pasiva y extracción activa.

En la extracción pasiva el atacante escucha, sin modificar mensajes o afectar la operación de la red generalmente no puede detectarse este tipo de ataque, pero sí prevenirse mediante mecanismos como la encriptación de información.

Los objetivos del atacante son la intercepción y el análisis de tráfico en la red. Al estar escuchando el tráfico, el atacante puede identificar:

- El origen y destino de los paquetes de comunicación, así como la información de cabecera.
- Monitorear el tráfico y horarios de actividad.
- Identificar el uso de protocolos y observar la transferencia de datos entre protocolos que no utilicen encriptado, por ejemplo la versión no segura de telnet o FTP que transfieren la clave de usuario en texto simple.

En la extracción activa el atacante modifica los mensajes o irrumpe la operación de la red. El atacante tiene como objetivo modificar datos o crear tráfico falso. Este tipo de ataque, generalmente puede detectarse, pero no prevenirse. La gama de actividades identificadas sobre ataques conocidos puede clasificarse en cuatro categorías:

1. ***Modificación de mensajes***: Al interceptar mensajes, se altera su contenido o su orden para irrumpir su flujo normal.
2. ***Degradación y fraude del servicio*****:** Tiene como objetivo intervenir el funcionamiento normal de un servicio, impide el uso o la gestión de recursos en la red. Ejemplo de este ataque es el de negación de servicio (DoS, Denial of Service), donde se suprimen los servicios de SMTP, HTTP, FTP, DNS, entre otros.

3. ***Reactuación*:** Al interceptar mensajes legítimos, se capturan y repiten para producir efectos diversos, como el ingresar dinero repetidas veces en una cuenta de banco.
4. ***Suplantación de identidad*:** Este es uno de los ataques más completos y nocivos. El intruso o atacante adopta una identidad con privilegios en una red y explota esos privilegios para sus fines. Un ataque con prioridad de atención para todo administrador de red es el "spoofing" donde el intruso obtiene servicios basados en la autenticación de computadoras por su dirección IP. Es recomendable seguir una estrategia y de preferencia tener una herramienta para combatirlos.

Todos estos ataques tienen un impacto relativo a la política de seguridad de un sistema, aunque en Internet dentro de los más temidos se encuentra el DoS por su relevancia al suprimir el funcionamiento de un sistema, y el *Spoofing* al obtener privilegios de acceso de forma fraudulenta. La autenticación de IPSec ESP/AH (Encapsulating Security Payload/Authentication Header) provee protección en contra de *spoofing*, cualquier paquete fraudulento será identificado y descartado.

Para protegernos de los posibles ataques informáticos se debe implementar políticas de seguridad apoyadas por todos los medios

técnicos o de procedimientos que se aplican y desarrollan para atender vulnerabilidades y frustrar ataques específicos. Ejemplos: Reglamentos, *firewalls*, nessus, *SSH*, *tcp-wappers*, antivirus, kerberos, radius, entre muchos otros comerciales o de dominio público.

1.1.2. MECANISMOS DE SEGURIDAD.

Se han desarrollado una gran variedad de algoritmos, mecanismos y técnicas para brindar protección a los recursos informáticos, y garantizar la integridad, confidencialidad y control de acceso de información.

La confidencialidad es necesaria para mantener un secreto, pero sin autenticación, no puede saberse que la persona con la que se está compartiendo ese secreto, es quien dice ser, y sin la confianza de la integridad del mensaje recibido, no se sabe si el mensaje es el mismo al que fue enviado. Los mecanismos descritos en esta sección están enfocados a garantizar estos aspectos.

1.1.2.1. CRIPTOLOGÍA.

La Criptología es un área de estudio de las Matemáticas con gran aplicación en las Ciencias de la Computación, se divide en dos ramas: La criptografía, que involucra lo relacionado al diseño de sistemas para encriptar o cifrar información, y el criptoanálisis sobre

el proceso inverso, involucra los sistemas para desencriptar o descifrar códigos.

Los algoritmos criptográficos proveen confidencialidad de datos al convertir un mensaje (texto plano) en garabatos (cibertexto) y viceversa.

Los sistemas de criptografía se han clasificado como se muestra en la figura 1.2. Los sistemas simétricos basan su cifrado y descifrado en una sola llave, los sistemas asimétricos o de llave pública, basan su seguridad en llaves diferentes, una privada para descifrar y una pública para cifrar. Los algoritmos de bloque (Block) no poseen memoria interna, los mismos bloques utilizados para el texto plano son siempre relacionados a los bloques del cibertexto. Los sistemas de ráfaga (Stream) poseen memoria interna, los bloques del texto plano, no siempre son transformados a bloques idénticos de cibertexto. Los algoritmos criptográficos, sin importar su simetría, son conmutativos:

Texto plano = Desencriptar (Encriptar (texto plano))

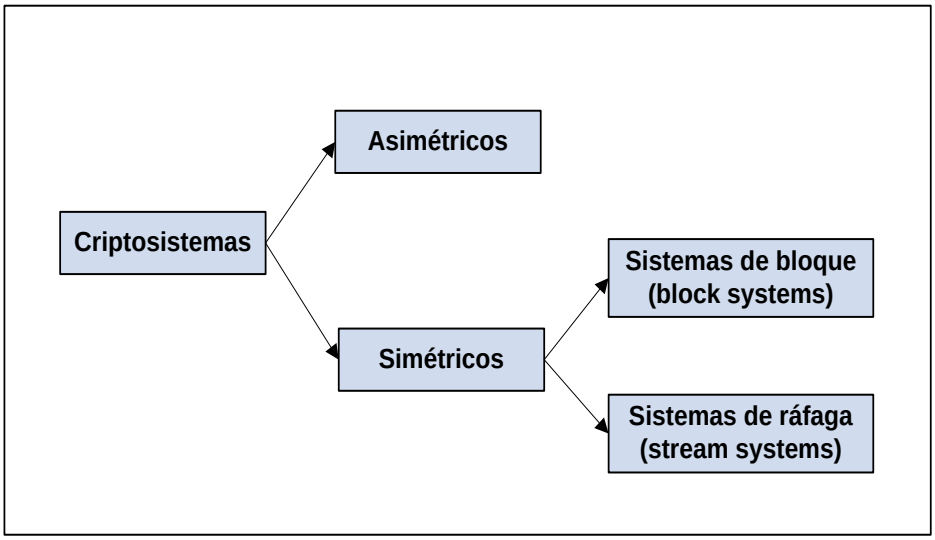


Figura 1.2. Clasificación de Criptosistemas.

Hablando de criptología, el ejemplo común involucra a quien envía el mensaje encriptado (Alicia), el que recibe el mensaje y lo descifra (Bertha), y el intruso en algún punto de la transmisión, intentando descifrar mensajes (Oscar), como se muestra en la figura 1.3.

Para caracterizar un algoritmo seguro o robusto se manejan tres categorías:

a. Incondicionalmente seguro, solo hay un algoritmo de este tipo y no es implementable, no existe manera de generar números realmente aleatorios, siempre dependen de una semilla.
b. Probablemente seguro, el problema matemático para descifrarlo es altamente complicado

c. Computacionalmente seguro, se requiere gran capacidad de cómputo para descifrarlo.

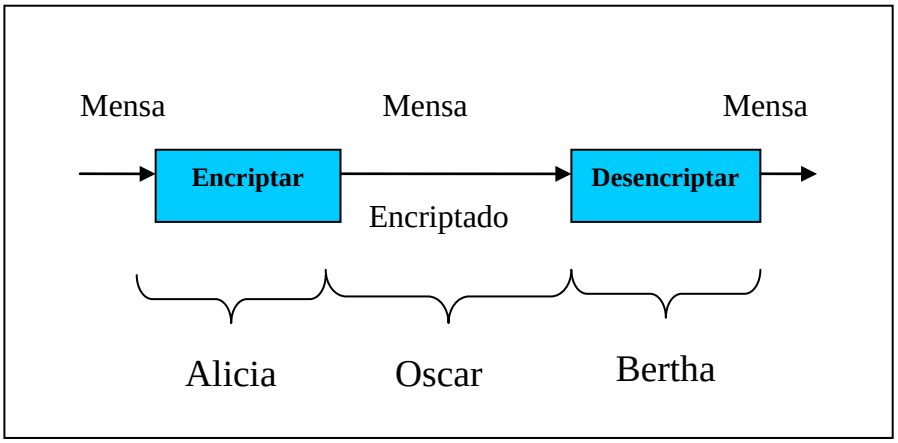


Figura 1.3. Esquema de una comunicación segura.

De los Block Ciphers el más comercial es quizá el DES (Data Encryption Standard), no es robusto pero es simple de instrumentar. Una mejor opción para sistemas más seguros es el 3DES o bien, IDEA (International Data Encryption Algorithm) más robusto aunque costoso de recursos. De los sistemas asimétricos, RSA (nombre por sus autores) es el más popular.

La selección del algoritmo de criptografía a ser utilizado en las herramientas de seguridad, se realiza en los mismos términos que otros algoritmos de computación, en base a su complejidad y robustez, acordes al nivel de seguridad deseado en el sistema.

Los algoritmos robustos son considerados de alta confidencialidad y valor, por ello, países como Estados Unidos tienen leyes muy estrictas con respecto a la exportación de la tecnología criptográfica.

1.1.2.2. INTEGRIDAD DE DATOS.

La integridad se refiere a la garantía de que la información no ha sido alterada durante su transmisión. Así como hay cibersistemas simétricos y asimétricos, también hay métodos simétricos y asimétricos para garantizar la integridad de mensajes. Los MAC (Message Authentication Codes), son códigos que utilizan funciones hash (Un algoritmo criptográfico de un solo sentido que cambia una variable de tamaño arbitrario y la convierte en una variable de tamaño fijo). El MAC se genera al aplicar la función hash a una llave privada con el mensaje, el resultado se transmite en conjunto con el mensaje, y la verificación del MAC permite aplicar la función hash a la llave secreta con el mensaje para producir un compendio temporal, y comparar este compendio con el atado al mensaje. Este proceso se llama transformación fundamental o *keyed hashing*. Es importante realizar el proceso completo, porque solo aplicar la función hash a unos datos no provee autenticación, es como una comprobación de paridad (checksum), una función *keyed hash* es un MAC.

HMAC es un método especial. Fue diseñado por Hugo Krawczyk, Ran Canetti y Mihir Bellare. Es un método mejorado de manejo de llaves con funciones Hash, y brinda protección adicional a otros algoritmos, de tal forma que SHA (Secure Hash Algorithm) se convierte en HMAC-SHA, MD5 (Message Digest 5) se convierte en HMAC-MD5. La construcción de HMAC es criptográficamente más fuerte que otras funciones hash. Por ejemplo, MD5 es susceptible a un ataque del tipo colisión, donde es posible encontrar dos entradas diferentes que produzcan el mismo compendio, HMAC-MD5 no es susceptible a este ataque.

1.1.2.3. CONTROL DE ACCESO Y AUTENTICACIÓN.

La autenticación es uno de los problemas más complicados en seguridad. Implica reconocer y garantizar que alguien (persona o computadora) es quien dice ser. La autenticación es un servicio básico de seguridad. Puede hablarse de autenticación con criptografía o sin criptografía, los grandes problemas radican en la autenticación de personas y los mecanismos de distribución de llaves y certificados.

Las firmas digitales es uno de los mecanismos más utilizados para el intercambio de mensajes en el correo electrónico. Los mecanismos de llaves digitales implican esquemas de confianza, el esquema

común es que una persona cree su llave digital, y solicite que al menos otras dos firmen su llave, de esta manera hay al menos dos testigos de que esa llave le pertenece a esa persona. La generación de llaves para computadoras, son esquemas actuales, en sistemas seguros a nivel de red, no de usuario.

En lo que se está actualmente trabajando y buscando establecer, es la Infraestructura de Llaves Públicas (Public Key Infraestructure, PKI). Una infraestructura que forma un sistema en el que participan entidades certificadoras que garantizan la identidad digital de personas, instituciones o aplicaciones. El sistema es a través del manejo de certificados, documentos digitales para autenticar personas, servidores o aplicaciones. Es un esquema complicado, donde intervienen entidades generadoras/revocadoras de certificados, solicitantes de certificados y solicitudes de legalidad de certificados. Es un esquema que exige la participación del gobierno o de entidades oficiales para validar la identidad de personas y organizaciones.

1.1.2.4. PROTOCOLOS CRIPTOGRAFÍCOS.

Dentro del contexto del modelo de interconexión OSI-ISO, la tabla 1.1 muestra la ubicación de algunos de los protocolos de criptografía más utilizados y reconocidos como estándares por la IETF. Las dos

primeras capas están sujetas a los estándares de interoperabilidad de seguridad de LAN (SILS, Standard for Interoperable LAN Security).

Los protocolos de la capa de red son objeto de estudio de este trabajo de investigación, en particular AH y ESP que son parte del conjunto de protocolos denominado IPSec.

Los protocolos de la capa de aplicación se describirán brevemente, sin profundizar, solo describiendo conceptos relevantes para el posterior entendimiento de su interoperabilidad con IPSec.

Capa	Nombre	Protocolos
7	Aplicación	X.400, MSP, PEM, S/MIME, PGP, X.500, DNSSEC, Administración de certificados y llaves
6	Presentación	
5	Sesión	SSL
4	Transporte	TLSP
3	Red	NLSP, ESP, AH
2	Enlace de datos	SILS
1	Fisica	Enlace sincrónico

Tabla 1.1. Capas y protocolos de criptografía.

Protocolo Secure Sockets Layer (SSL)

El protocolo SSL fue diseñado originalmente por Netscape Development Corporation©, la versión 3.0 fue diseñada con apoyo público y sugerencias de la industria con el siguiente objetivo: Establecer una conexión segura (con criptografía) entre cliente y servidor, proveer privacidad y confidencialidad en la comunicación de dos aplicaciones.

SSL está compuesto por dos capas. En la capa inferior, se encuentra el protocolo SSL de registro, trabaja sobre algún protocolo de transporte (TCP y UDP por ejemplo), este protocolo se utiliza para encapsulamiento, encriptamiento, autenticación, servicios de secuencia y compresión. En la capa superior se encuentran 4 protocolos: El protocolo SSL de inicio de comunicación entre dos entidades o handshake, negocia mecanismos de encriptamiento, autenticación, secuencia y compresión y establece los parámetros clave entre cliente y servidor. El protocolo Change Cipher Spec, invoca cambios síncronos de mecanismos de seguridad y parámetros clave entre cliente y servidor. El protocolo de datos de aplicación para transportar los mensajes de aplicación entre los pares de cliente y servidor, y el protocolo de Alerta, que comunica mensajes de cierre y error de conexión.

SSL provee una conexión segura con los siguientes servicios:

1. La conexión es privada, en el handshake inicial se define la llave secreta, y el algoritmo simétrico (DES, RC4, por ejemplo).
2. El cliente puede autenticarse utilizando algún algoritmo asimétrico o de llave pública (RSA, DSS, etc.). Esto es opcional, depende de si los certificados de cliente están disponibles.
3. El servidor se autentica utilizando certificados X.509.
4. La conexión es confiable. Se garantiza la integridad del mensaje utilizando funciones hash seguras MAC (SHA, MD5, etc.).
5. Se garantiza una secuencia estricta de mensajes, confía en TCP.
6. La compresión es opcional.

En la figura 1.4 se muestra el diálogo del protocolo SSL de Handshake el intercambio de mensajes del tipo “hello” entre cliente y servidor, para establecer versión, algoritmos, certificados y llaves de autenticación, antes de la transmisión de la información.

SSL ha sido ampliamente utilizado, tanto en productos comerciales como de dominio público (Open_ssl/mod_ssl para apache por ejemplo) para el protocolo HTTP. Fue sometido el internet-draft a la

IETF y propuesto como estándar en 1996, la IETF redefinió su construcción y estableció TLS 1.0 como estándar, que corresponde a la versión 3.1 de SSL.

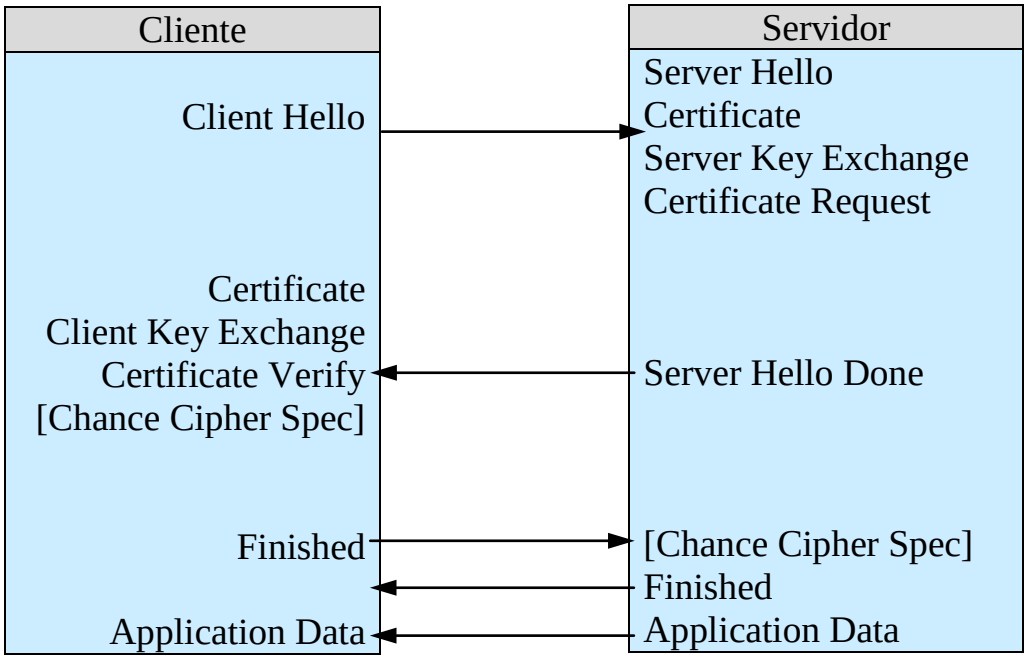


Figura 1.4. Protocolo SSL para establecer una conexión segura entre cliente y servidor.

Protocolo Transport Layer Security (TLS).

TLS es el estándar creado por la IETF como el protocolo de la capa de transporte. Surgió como respuesta a SSL de Netscape y PCT de Microsoft©, se consideró negativo para la industria el manejo de dos protocolos similares, así que se estableció TLS. Está basado en SSL, de hecho se considera una actualización, versión 3.1 de SSL y presenta las siguientes modificaciones:

- Requiere soporte para el algoritmo DSA y D-H, RSA es opcional.
- El algoritmo de generación de llaves está modificado, utiliza MD5 y SHA-1 con HMAC como función pseudo aleatoria, a diferencia del algoritmo de llaves MAC definido en SSL.
- Contiene un conjunto más completo de alertas.

TLS es la propuesta por el grupo de trabajo de la IETF, sin embargo, ha habido mayor desarrollo sobre SSL.

Protocolo Network Layer Security (NLS).

NLS es un protocolo de seguridad desarrollado en el seno de ISO-OSI, y diseñado para utilizarse en la capa superior de la capa 3 (capa de red). Se ofrece para versiones orientadas a conexión y a no conexión.

Protocolos Authentication Header AH, Encapsulating Security Payload (ESP).

Los protocolos AH y ESP son parte del conjunto de protocolos de seguridad conocidos como IPSec. IPSec es un estándar de seguridad de la capa de red. Ofrece servicios de seguridad como encriptamiento y protección de integridad para los paquetes IP. IPSec es considerado hoy en día como el mejor protocolo de

seguridad, se encuentran algunas implementaciones funcionando y diversos proyectos de experimentación y desarrollo. Dada su relación con el protocolo de siguiente generación de IP (IPv6) se considera el protocolo de seguridad para las redes de siguiente generación.

Se genera un encabezado extra entre las capas 3 y 4 (IP y TCP) para ofrecer al destino suficiente información para identificar asociaciones de seguridad. AH autentica e incluye direcciones de fuente y destino. ESP encripta y autentica.

Además de AH y ESP, utiliza ISAKMP/IDE para el manejo de llaves, que se encuentran documentados en varios RFC y documentos que circulan en Internet. IPSec se encuentra descrito a profundidad mas adelante.

Protocolos de la capa de aplicación.

En esta capa se encuentran protocolos destinados a la seguridad de alguna aplicación específica, por lo que existen una gran variedad de propuestas, tanto comerciales como de dominio público para ofrecer servicios de seguridad, se mencionan algunos reconocidos como estándares a manera de referencia.

DNS es el sistema de nombres que mantiene nombres como www.hotmail.com, DNSSEC es el sistema que contiene contramedidas a las vulnerabilidades encontradas, más servicios de seguridad. PGP es un protocolo ampliamente utilizado para el encriptamiento de mensajes de correo electrónico y firmas digitales. S/MIME es un protocolo ampliamente utilizado para la seguridad de mensajes, sea de correo electrónico o en servicios de directorio. Los protocolos X.400, X500 son estándares de ISO/CCITT para mensajes y directorios respectivamente, el X.509 es la porción del estándar X.500 para autenticación, en particular para certificados de llave pública y listas de revocación de certificados.

El protocolo de seguridad de mensajes (MSP, Message Security Protocol), es un protocolo de mensajes para ser utilizado con X.400 y protocolos de correo definidos en el RFC 822/SMTP, fue adoptado como protocolo estándar seguro para el sistema de mensajes de la Defensa de Estados Unidos.

1.2. PROTOCOLOS DE INTERNET (IP)

1.2.1. PROTOCOLO IPv4

La capa de Red provee el servicio orientado a no-conexión. Esta capa es responsable del enrutamiento de paquetes, de la definición de rutas

para su transmisión y de definir el esquema de direccionamiento para identificar cada destino sin ambigüedades.

IPv4 (Internet Protocol versión 4) es el protocolo de capa de red más popular hoy en día y tiene la infraestructura de enrutamiento muy madura. El direccionamiento es uno de los componentes más importantes de un protocolo de red, IPv4 maneja direcciones de 32 bits representadas en notación decimal separada por puntos A.B.C.D, cada símbolo es un byte y representa una parte de dirección de red y otra de computadora. La dirección de red se obtiene con un AND lógico con la máscara de red, todas las direcciones IP van acompañadas de una máscara de red. Por ejemplo, una dirección IPv4 salida de la Red-A es 158.97.28.12/255.255.252.0 o bien en otra notación, 158.97.28.12/22., es la computadora 12 de la subred 28, de la red 158.97.0.0 asignada de forma única a la red A y a la computadora dentro de Red-A.

Los componentes del encabezado de IPv4 se muestran en la figura 1.5, no todos son utilizados para efectos de seguridad.

Nota: los números en la parte superior de la figura representan los bytes.

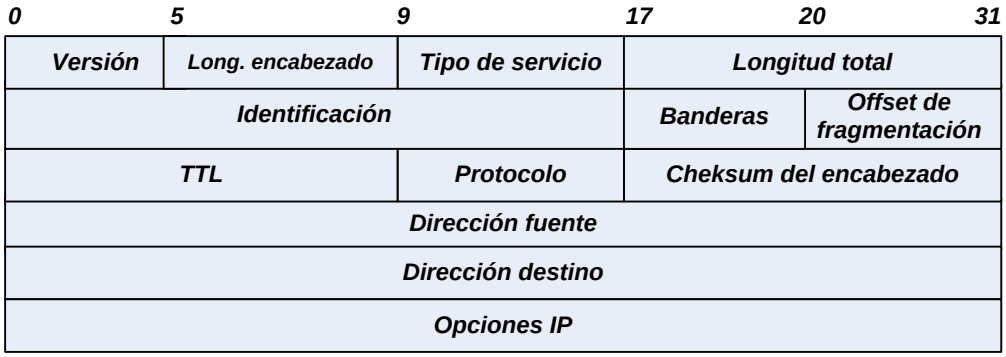


Figura 1.5. Encabezado IPv4.

La definición de componentes se describe a continuación:

Versión: Es un campo de 4 bits utilizado para indicar la versión, un 4 para IPv4, se utiliza para validar compatibilidad.

Longitud de encabezado: Indica la longitud del encabezado en 32 bits. La longitud máxima de un encabezado IPv4 es de 60 bytes. Esta es una de las limitantes resueltas en IPv6.

Tipo de servicio (TOS): Se utiliza para indicar los requerimientos de tráfico de un paquete, no ha sido utilizado y se encuentra en revisión por la IETF.

Longitud total: La longitud total del datagrama en bytes, incluyendo el encabezado. Indica el tamaño total del datagrama a la capa de red en el extremo receptor.

Identificación: Es un campo de 16 bits para identificar de manera única un datagrama IP. Este campo se utiliza principalmente para fragmentación, identifica de manera única cuál paquete IP pertenece a un datagrama IP.

Banderas: Sólo han sido definidos dos bits de los tres reservados. El primer bit especifica la no fragmentación del paquete. El segundo bit indica si es el último fragmento de un datagrama o si hay otros, este bit se utiliza también para la reconstrucción de los datagramas fragmentados.

Offset de fragmentación: Indica el offset del paquete IP dentro del datagrama IP.

Tiempo de vida (TTL): Un contador para eliminar ciclos, se asigna un valor por omisión, y cada router en la trayectoria lo decrementa en 1.

Protocolo: Indica el protocolo de transporte.

Checksum del encabezado: Se utiliza para validar la integridad del encabezado IP.

Dirección fuente y dirección destino: Indica las direcciones de 32 bits de la fuente y destino del paquete, respectivamente.

Opciones: Información adicional, no utilizada para cuestiones de seguridad.

1.2.2. PROTOCOLO IPv6

Una dirección IPv6 es de 128 bits de longitud y su representación es diferente, números hexadecimales separados por dos puntos, el concepto de máscara es similar y se ha implementado una jerarquía mucho más rica para disminuir los problemas de enrutamiento y direccionamiento. Por ejemplo, una dirección IPv6 válida de Red-A es 3ffe:8070:100f:1:a00:20ff:fec6:ba27/64 que indica la región geográfica, la institución, subred y computadora de forma única en la red mundial experimental de IPv6.

Existe un control universal por los organismos de Internet para la asignación de direcciones, de igual forma se está construyendo el direccionamiento para IPv6.

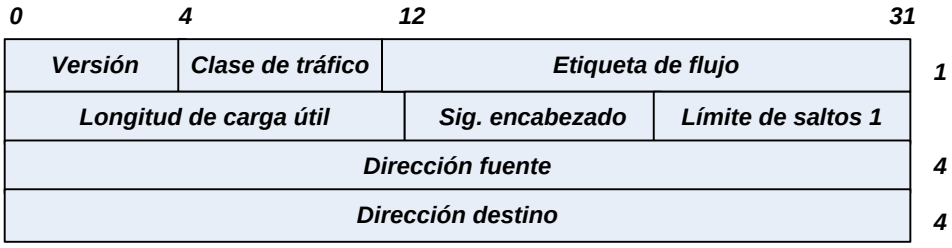


Figura 1.6. Encabezado de IPv6.

Los componentes del encabezado de IPv6 se muestran en la figura 1.6, la utilidad de los componentes se describe a continuación:

Versión: Indica la versión, 6 para IPv6.

Clase de tráfico: Campo de 8 bits para indicar los requerimientos de tráfico del paquete, similar a TOS de IPv4.

Etiqueta de flujo: Campo de 20 bits, experimental.

Longitud de carga útil: Campo de 16 bits que indica la longitud de la carga útil sin incluir el encabezado IPv6.

Siguiente encabezado: Campo de 8 bits, para indicar el uso de cabeceras de extensión.

Límite de saltos: Campo de 8 bits similar al TTL de IPv4.

Dirección fuente y destino: Campos de 128 bits para las direcciones fuente y destino del paquete, respectivamente.

Las Cabeceras de Extensión, son una de las modificaciones más relevantes del protocolo IP de siguiente generación, las extensiones de opción se insertan entre el encabezado de IPv6 y el encabezado de transporte como se muestra en la figura 1.7. Cada cabecera de opción recibe un identificador único y se codifica con el formato que se muestra en la figura 1.8.

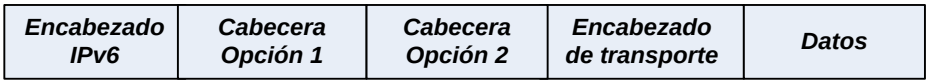


Figura 1.7. Encabezado IPv6 con cabeceras de opción.

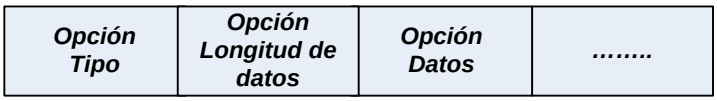


Figura 1.8. Formato de las opciones de IPv6

1.2.3. PROTOCOLO DE SEGURIDAD IP (IPSEC)

IPSec (Internet Protocol Security) es un conjunto de extensiones al protocolo IP. Es un estándar de la IETF (Internet Engineering Task Force) definido en el RFC 2401. Provee servicios de seguridad como autenticación, integridad, control de acceso y confidencialidad. Es implementado en la capa de Red, de tal forma que su funcionamiento es completamente transparente al nivel de aplicaciones, y es mucho más poderoso. IPSec provee un mecanismo estándar, robusto y con posibilidades de expansión, para proveer seguridad al protocolo IP y protocolos de capas superiores.

La arquitectura de IPSec.

La arquitectura de IPSec define la granularidad con la que el usuario puede especificar su política de seguridad. Permite que cierto tráfico sea identificado para recibir el nivel de protección deseado (Figura 1.9)

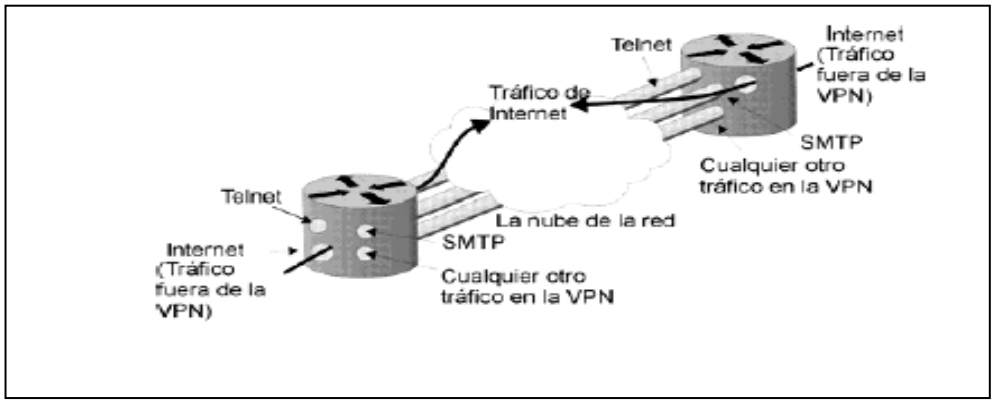


Figura 1.9. Túneles de comunicación protegidos por IPSec entre redes separadas.

IPSec está diseñado para proveer seguridad interoperable de alta calidad basada en criptografía, tanto para IPv4 como para IPv6. Está compuesto por dos protocolos de seguridad de tráfico, el Authentication Header (AH) y el Encapsulating Security Payload (ESP), además de protocolos y procedimientos para el manejo de llaves encriptadas. AH provee la prueba de los datos de origen en los paquetes recibidos, la integridad de los datos, y la protección contra-respuesta. ESP provee lo mismo que AH adicionando confidencialidad de datos y de flujo de tráfico limitado.

En la figura 1.10 se aprecia la arquitectura de IPSec. Al utilizar el mecanismo de AH se aplican algoritmos de autenticación, con la aplicación del mecanismo ESP, además de autenticación, también

algoritmos de encriptación. El esquema de interoperabilidad se maneja a través de Asociaciones de Seguridad (SA), almacenadas en una base de datos. Los parámetros que se negocian para establecer los canales seguros se denominan Dominio de Interpretación IPSec (Domain of Interpretation, DOI), bajo políticas pre-establecidas dentro de un esquema de funcionamiento estático con valores fijos y previamente establecidos, o bien, en un esquema de funcionamiento dinámico utilizando un protocolo de manejo de llaves, Interchange Key Exchange (IKE).

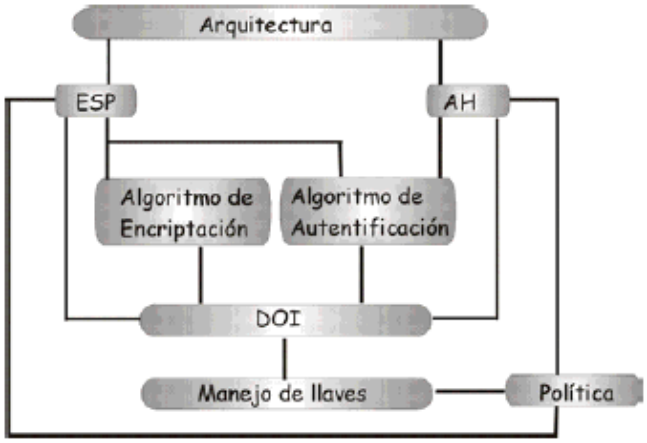


Figura 1.10. Arquitectura de IPSec.

Modos de funcionamiento de IPSec.

El diseño de IPSec plantea dos modos de funcionamiento para sus protocolos: transporte y túnel, la diferencia radica en la unidad que se esté protegiendo, en modo transporte se protege la carga útil IP (capa de transporte), en modo túnel se protegen paquetes IP (capa de red) y

se pueden implementar tres combinaciones: AH en modo transporte, ESP en modo transporte, ESP en modo túnel (AH en modo túnel tiene el mismo efecto que en modo transporte).

El modo transporte se aplica a nivel de hosts. AH y ESP en este modo interceptarán los paquetes procedentes de la capa de transporte a la capa de red y aplicarán la seguridad que haya sido configurada. En la figura 1.11 se aprecia un esquema de IPSec en modo transporte, si la política de seguridad define que los paquetes deben ser encriptados, se utiliza ESP en modo transporte, en caso que solo haya sido requerida autenticación, se utiliza AH en modo transporte.

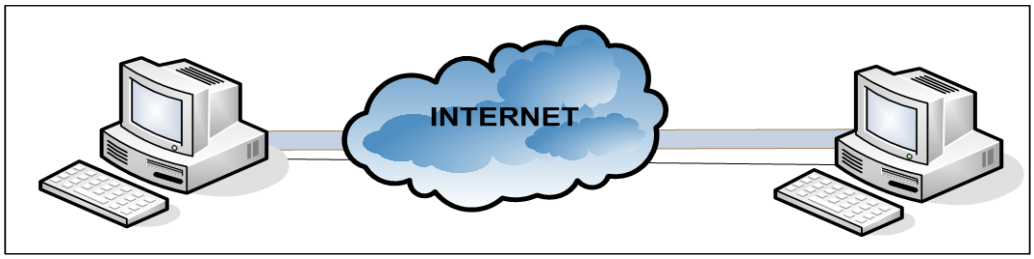


Figura 1.11. Hosts A y B implementando ESP en modo transporte.

Los paquetes de la capa de transporte como TCP y UDP pasan a la capa de red, que agrega el encabezado IP y pasa a las capas inferiores; cuando se habilita IPSec en modo transporte, los paquetes de la capa de transporte pasan al componente de IPSec (que es implementado como parte de la capa de red, en el caso de sistemas operativos), el componente de IPSec agrega los encabezados AH y/o

ESP, y la capa de red agrega su encabezado IP. En el caso que se apliquen ambos protocolos, primero debe aplicarse la cabecera de ESP y después de AH, para que la integridad de datos se aplique a la carga útil de ESP que contiene la carga útil de la capa de transporte, esto se ilustra en la figura 1.12.

Figura 1.12. Formato del paquete con AH y ESP.

El modo túnel se utiliza cuando la seguridad es aplicada por un dispositivo diferente al generador de los paquetes, como el caso de las VPN, o bien, cuando el paquete necesita ser asegurado hacia un punto seguro como destino y es diferente al destino final, como se ilustra en la figura 1.13, el flujo de tráfico es entre A y B, e IPSec puede aplicarse con una asociación de seguridad entre RA y RB, o bien, una asociación de seguridad entre A y RB.

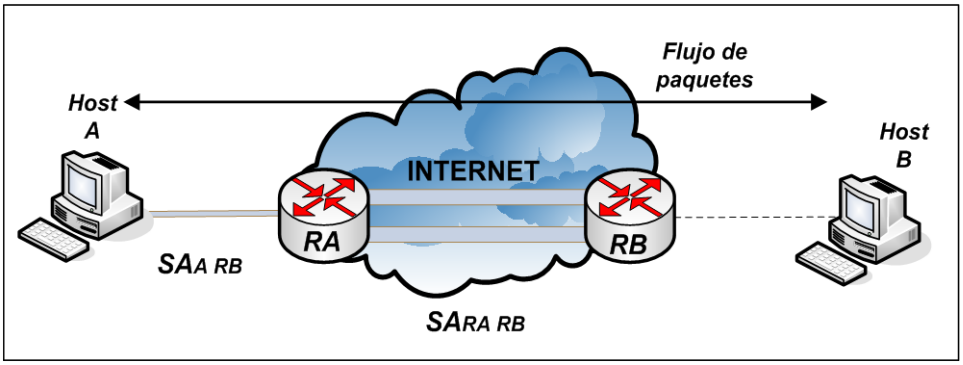


Figura 1.13. Aplicación de IPSec en modo túnel.

IPSec en modo túnel, tiene dos encabezados IP, interior y exterior. El encabezado interior es creado por el host y el encabezado exterior es agregado por el dispositivo que está proporcionando los servicios de seguridad. IPSec encapsula el paquete IP con los encabezados de IPSec y agrega un encabezado exterior de IP como se ilustra en la figura 1.14.

Figura 1.14. Formato del paquete aplicando IPSec en modo túnel.

IPSec también soporta túneles anidados, aunque no son recomendados por lo complicado de su construcción, mantenimiento y consumo de recursos de red. La figura 1.15 muestra dos túneles, A envía un paquete a B, la política indica que debe ser autenticado con el router RB, además existe una VPN entre RA y RB, de tal forma que el paquete que ve RB es el que se muestra en la figura 1.16, el encabezado exterior es un paquete ESP entunelado y contiene un paquete AH entunelado, el paquete AH contiene el paquete IP para el host B generado por el host A.

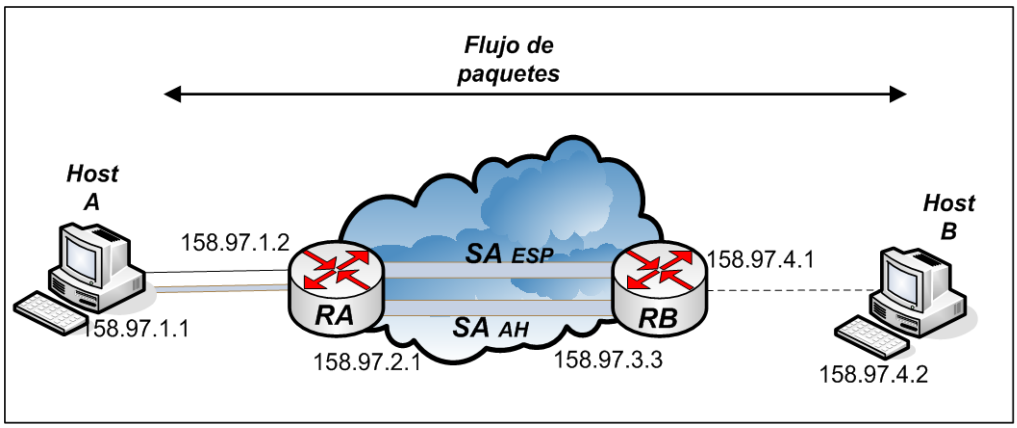


Figura 1.15. Ejemplo de túneles anidados.

Encabezado IP	ESP	Encabezado IP	AH	Encabezado IP	Datos
Fuente: 158.97.2.1 *Destino: 158.97.3.3*		*Fuente: 158.97.1.1* *Destino: 158.97.3.3*		*Fuente: 158.97.1.1* *Destino: 158.97.4.2*	

Figura 1.16. Formato del paquete del túnel anidado.

Asociaciones de seguridad.

Una asociación de seguridad (SA) es la forma básica de IPSec, es el contrato entre dos entidades que desean comunicarse en forma segura. Las SA determinan los protocolos a utilizar, las transformaciones, las llaves y la duración de validez de dichas llaves. Las SA son almacenadas en una base de datos (SADB), son de un solo sentido, es decir, cada entidad con IPSec tiene una SA para el tráfico que entra, y otra SA para el tráfico que sale. Además de ser

unidireccionales, también son específicas al protocolo, hay SA separadas para AH y para ESP.

Indice de parámetros de seguridad (Security Parameter Index, SPI).

El SPI es una entidad de 32 bits que identifica de manera única una SA. Es el mecanismo concebido para que en una comunicación segura, la fuente identifique cual SA utilizar para asegurar un paquete por enviar, y el destino identifique cual SA utilizar para verificar la seguridad del paquete recibido. El SPI se incluye en los encabezados ESP y AH, el destino utiliza la dupla <spi, dst protocol> para identificar de forma única la SA.

Gestión de las SA.

Para el manejo de SA se establecen dos tareas: creación y borrado; estas actividades pueden ser manuales o a través del protocolo de manejo de llaves (IKE).

La creación es un proceso de dos etapas: 1) negociación de parámetros de la SA, 2) actualización de la SADB. El manejo manual de llaves es obligatorio en toda implementación, el proceso de definición de SPI y parámetros es totalmente manual, y permanecerán hasta que sean manualmente borrados. En el manejo dinámico de llaves, se utiliza un protocolo en Internet llamado IKE. El kernel con

IPSec habilitado, invoca IKE si se trata de una comunicación segura y no encuentra una SA. IKE negocia la SA con el destino o con el siguiente salto (host o router), dependiendo de la política y crea la SA en la SADB.

Igualmente las SA pueden ser borradas manualmente o con IKE, los criterios de borrado pueden ser: tiempo de vida expirado, llaves comprometidas, solicitud explícita para borrarse, o el número de bytes utilizado excede un umbral especificado en la política.

Parámetros.

Los parámetros por negociar en una SA, tanto para AH como para ESP son los siguientes:

Número de secuencia: Un campo de 32 bits utilizado en el procesamiento de paquetes de salida, es parte de los encabezados de AH y/o ESP, su valor inicial es 0, se incrementa en uno cada vez que la SA es utilizada, se utiliza para detectar ataques del tipo “replay”.

Sobreflujo del número de secuencia: Campo utilizado en el procesamiento de paquetes de salida y se establece cuando hay sobreflujo del campo de número de secuencia. La política determina qué hacer si este campo está activado.

Ventana de antireply: Campo utilizado en el procesamiento de paquetes de entrada. Se activa si IPSec detecta paquetes retransmitidos por hosts sospechosos.

Tiempo de vida: El tiempo de validez de una SA, se especifica en términos de bytes asegurados con la SA, no se recomienda enviar más de 4Gb de paquetes utilizando la misma SA. Para evitar la pérdida de la conexión segura, se manejan dos límites, soft y hard. Al llegar al límite soft el kernel es notificado para que inicie una nueva negociación antes del límite hard que es cuando la SA expira.

Modo: Los valores son: túnel, transporte o indistinto. Si el valor es indistinto la SA puede ser utilizada para modo túnel o modo transporte.

Destino del túnel: Campo utilizado para el modo túnel, indica la dirección IP de destino del encabezado exterior.

Parámetros PMTU: IPSec no fragmenta o reensambla paquetes, sin embargo, agrega un encabezado IPSec y por lo tanto impacta la longitud del PMTU. IPSec debe participar en la determinación del PMTU (Protocol Maximum Transfer Unit), una SA mantiene dos valores: el PMTU y el campo de edad.

Políticas de seguridad en IPSec.

La política es uno de los componentes más importantes de la arquitectura de IPSec, determina los servicios de seguridad que serán aplicados a un paquete. Las políticas de seguridad son también almacenadas en una base de datos (Security Policy Database, SPD) indexada por seleccionadores.

La SPD es consultada tanto para el procesamiento de salida como el de entrada, se propone un administrador de la SPD para agregar, borrar y modificar; no hay un estándar que lo defina, pero se propone que los seleccionadores contengan los siguientes campos:

Dirección fuente: Puede ser indistinta, un rango de direcciones, un prefijo de red, o una dirección IP específica. Indistinta en el caso de que sea la misma política para todos los paquetes con un mismo host de origen, el rango de direcciones y prefijo de red, para los gateways de seguridad y para VPNs, la dirección específica para un host con varias direcciones, o en un gateway cuando los requerimientos de algún host sean específicos.

Dirección destino: Puede ser indistinta, un rango de direcciones, un prefijo de red, o una dirección IP específica (homologada o no). Los tres primeros para gateways de seguridad, la dirección específica como índice para la SPD.

Nombre: Nombre de un usuario o sistema sobre el cual se aplique la política de forma específica.

Protocolo: El protocolo de transporte.

Puertos de capas superiores: Los puertos fuente y destino sobre los que se aplica la política.

IP Encapsulating Security Payload (ESP).

ESP es un encabezado de protocolo insertado en el datagrama IP para proveer servicios de confidencialidad, autenticación del origen de los datos, *antireplay* e integridad de datos a IP. Es un estándar definido en el RFC 2406. El encabezado ESP se inserta después del encabezado IP y antes del encabezado del protocolo de capa superior (modo transporte) o antes del encabezado IP encapsulado (modo túnel).

El encabezado de protocolo (IPv4, IPv6 o extensión) que inmediatamente precede al encabezado ESP contendrá el valor 50 en su campo de protocolo (IPv4), o siguiente cabecera (IPv6).

El formato de los paquetes ESP para una SA dada es fijo durante la duración de la SA. El encabezado ESP tiene la forma definida en la figura 1.17, el SPI y número de secuencia fueron definidos antes, la carga útil de datos son los datos protegidos, el relleno (de hasta 255

bytes) se utiliza en ESP por varias circunstancias: Algunos algoritmos criptográficos requieren que el elemento de entrada sea un múltiplo del tamaño de su bloque, si no se especifica confidencialidad en la SA, se utiliza el relleno para justificar los campos *longitud de relleno* y s*iguiente cabecera* del encabezado ESP, para esconder el tamaño real de la carga útil; el contenido del relleno es dependiente del algoritmo de criptografía, el algoritmo puede definir un valor de relleno que debe ser verificado por el receptor para el proceso de desencriptado. El campo de longitud de relleno define cuánto relleno se agregó, el campo de siguiente cabecera indica el tipo de dato contenido en la carga útil de acuerdo al conjunto de números de Protocolo IP definidos por IANA (Internet Assigned Numbers Authority). El campo de datos de autenticación contiene el valor de verificación de integridad calculado sobre el paquete ESP menos los datos de autenticación.

ESP aplicado en modo transporte solo se utiliza en implementaciones del tipo host y provee protección a los protocolos de capas superiores, pero no al encabezado IP.

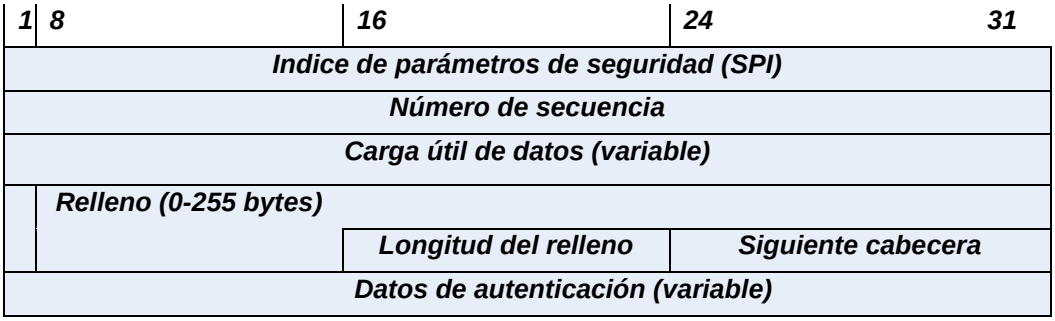


Figura 1.17. El encabezado ESP.

El encabezado ESP se inserta después del encabezado IP y antes del protocolo superior (TCP, UDP, ICMP, etc.) o antes de cualquier encabezado IP que haya sido previamente insertado. En la figura 1.18 se ilustra la transformación del paquete IP al aplicar ESP en modo transporte para IPv4; en la figura 1.19 se muestra el caso para IPv6.

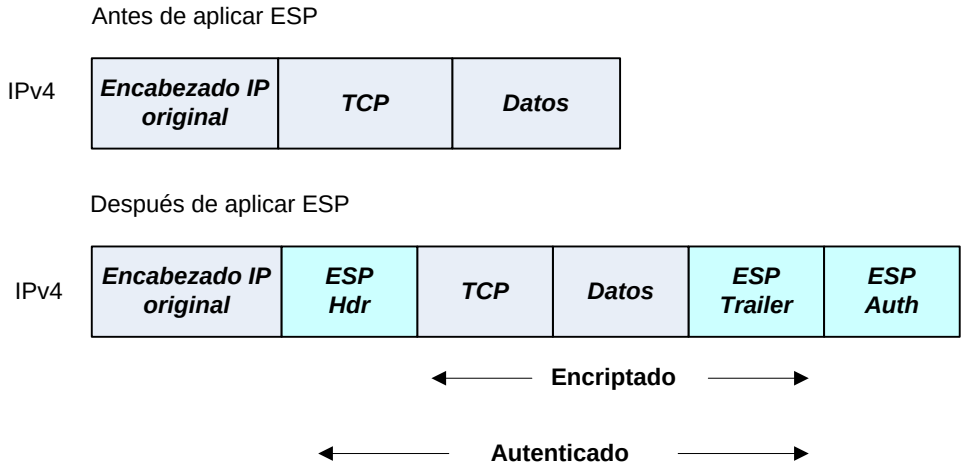


Figura 1.18. Transformación del paquete IPv4 al aplicar ESP en modo transporte.

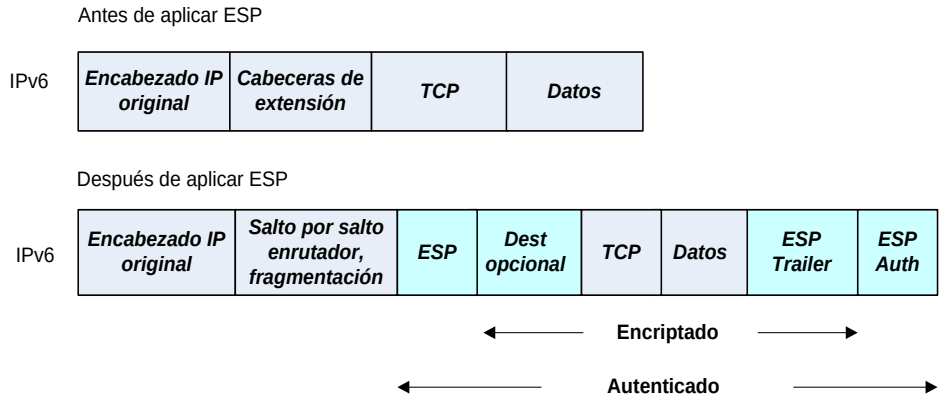


Figura 1.19. Transformación del paquete IPv6 al aplicar ESP en modo transporte.

En modo túnel, ESP puede ser empleado en hosts o en gateways. El encabezado IP interior contiene las direcciones del destino y origen del paquete, y el encabezado exterior puede contener direcciones diferentes, comúnmente direcciones de gateways de seguridad en el camino entre el origen y destino. La posición de los encabezados ESP en modo túnel con respecto a los encabezados IP exteriores es igual que en modo transporte. En la figura 1.20 se muestran los encabezados ESP para IPv4 e IPv6.

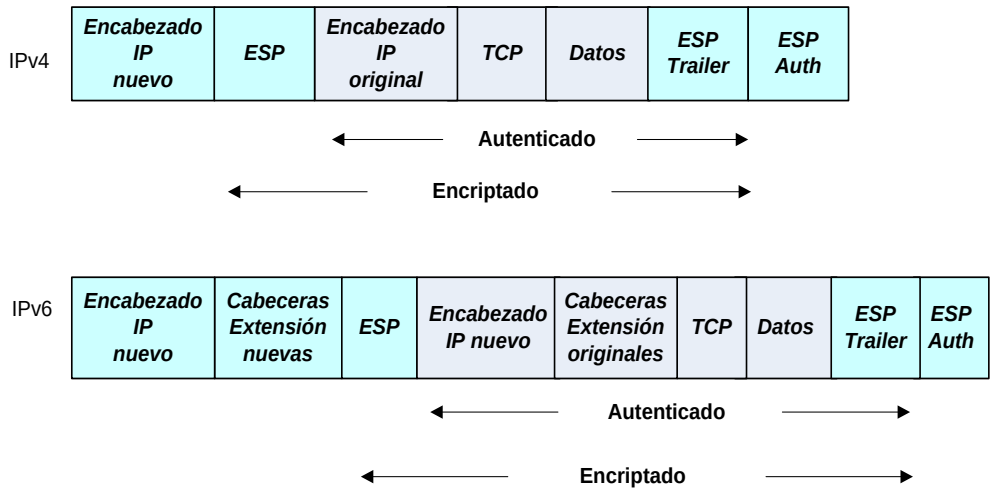


Figura 1.20. Transformación del paquete IP al aplicar ESP en modo túnel.

En caso de no haberse indicado la confidencialidad en la SA, el algoritmo de criptografía es nulo, en caso de aplicar confidencialidad a un paquete que se envía, el proceso aplicado en general es el siguiente:

1. Encapsular en el campo de carga útil de ESP:
    - Para modo transporte, solo la información original del protocolo de capa superior.
    - Para modo túnel, el datagrama IP original completo.
2. Agregar el relleno necesario.
3. Encriptar el resultado (carga útil de datos, relleno, longitud del relleno y la siguiente cabecera) usando la llave, el algoritmo de

criptografía, el modo indicado en la SA y si existe, datos de sincronización criptográfica.

En la parte del receptor se sigue en general el siguiente procedimiento para desencriptar los paquetes recibidos:

1. Desencriptar la carga útil de ESP, relleno, longitud del relleno, y siguiente cabecera, utilizando la llave, el algoritmo de criptografía, el modo y en su caso, los datos de sincronización criptográfica, indicados en la SA.
2. Procesar el relleno según haya sido especificado por el algoritmo utilizado.
3. Reconstruir el datagrama IP original:

    - Para modo transporte, el encabezado IP original más la información del protocolo de capa superior original en el campo de carga útil de ESP.
    - Para modo túnel, el encabezado IP entunelado, más el datagrama IP completo en el campo de carga útil de ESP.

Es importante mencionar que el encriptamiento no debe ser sustituto por la autenticación, la autenticación es el servicio básico de una comunicación segura, reforzada con el encriptamiento de datos.

IP Authentication Header (AH).

AH es el protocolo IPSec utilizado para proveer servicios de integridad de datos, autenticación del origen de los datos, y *antireplay* para IP. Es un estándar definido en el RFC 2402. La principal diferencia entre la autenticación provista entre ESP y AH tiene que ver con la cobertura, ESP no protege los campos del encabezado IP, a menos que sean encapsulados por ESP (modo túnel). El encabezado de protocolo (IPv4, IPv6 o extensión) que inmediatamente precede al encabezado AH contendrá el valor 51 en su campo de protocolo (IPv4), o siguiente cabecera (IPv6).

La figura 1.21 muestra el encabezado AH, todos los campos son obligatorios, tienen funciones similares a las explicadas en ESP, el campo reservado no se utiliza y su valor debe ser cero.

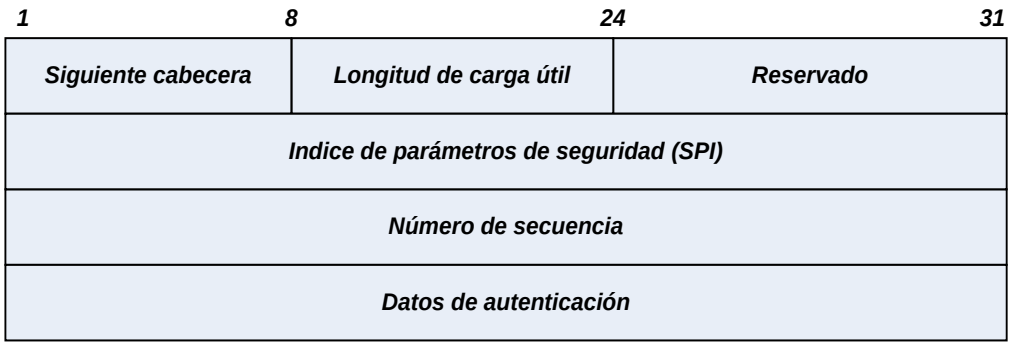


Figura 1.21. Encabezado AH.

Al igual que ESP, AH puede aplicarse tanto en modo túnel como transporte. Las figuras 1.22 y 1.23 muestran la ubicación de AH al aplicar IPSec en modo transporte en los paquetes IP.

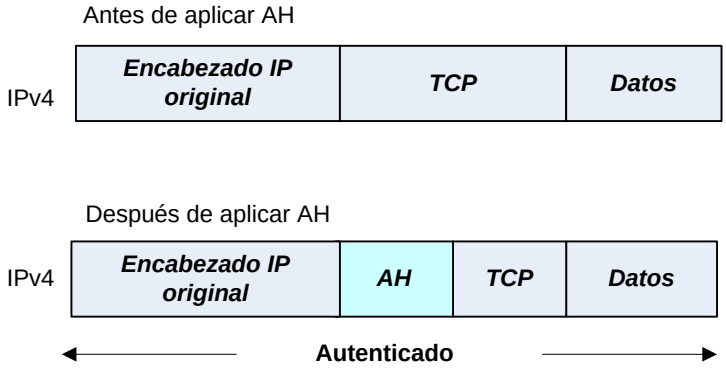


Figura 1.22. Transformación del paquete IPv4 al aplicar AH en modo transporte.

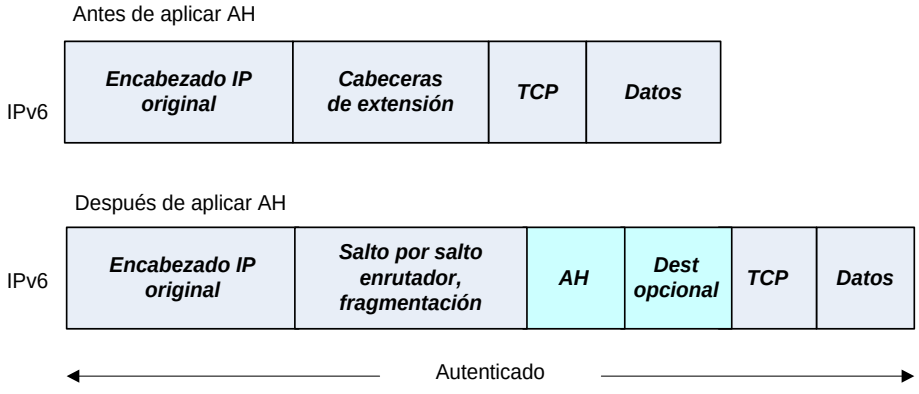


Figura 1.23. Transformación del paquete IPv6 al aplicar AH en modo transporte.

La aplicación de AH en modo túnel, tiene una ubicación similar a la de ESP, en la figura 1.24 se muestra la transformación de los paquetes IP al aplicar AH en modo túnel.

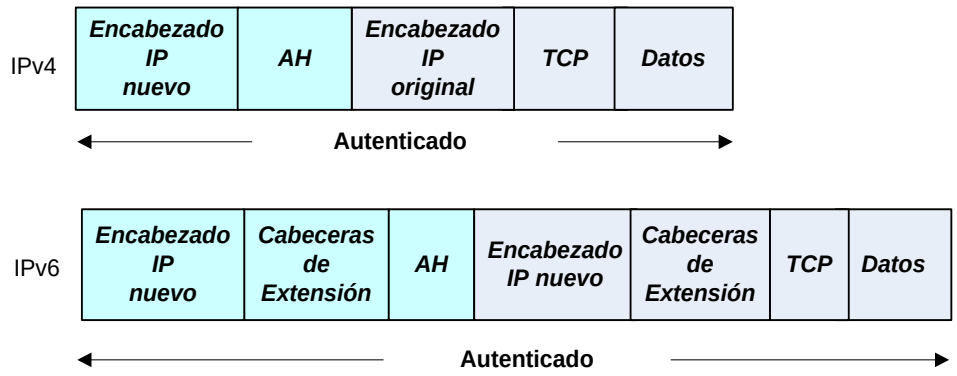


Figura 1.24. Transformación del paquete IP al aplicar AH en modo túnel.

El proceso de cálculo del valor de verificación de integridad (Integrity Check Value, ICV) que utiliza AH, llena con ceros los campos vulnerables a cambios en tránsito (TOS, Flags, Fragment, TTL, Header checksum en un encabezado IPv4) y se calcula sobre lo siguiente:

- Los campos del encabezado IP que sean inmunes a cambios en tránsito o pueda predecirse su valor (Versión, longitud de carga útil, longitud total, identificación, dirección de fuente y destino en un encabezado IPv4).
- El encabezado AH (siguiente cabecera, longitud de relleno, reservado, SPI, número de secuencia y datos de autenticación (que es puesta a cero para este cálculo), y bytes de relleno en caso que existan.

- Los datos del protocolo de capa superior, que se asume son inmunes a cambios en tránsito.

Internet Key Exchange (IKE).

El protocolo IKE no es parte de IPSec, es una alternativa para crear las Asociaciones de Seguridad de forma dinámica, está definido en el RFC 2409. IKE es un protocolo híbrido basado en el marco definido por el Protocolo de manejo de llaves y asociaciones de seguridad de Internet (Internet Security Association and Key Management protocol, ISAKMP) definido en el RFC2408, y otros dos protocolos de manejo de llaves Oakley y SKEME. Las implementaciones de IPSec están forzadas a soportar el manejo manual y solo algunas de ellas consideran IKE, que ha resultado demasiado complejo e inapropiado.

Implementación de IPSec.

La implementación de IPSec puede hacerse en hosts, gateways/routers, y/o firewalls, resultando conveniente la implementación en éstos últimos al complementar mutuamente sus funciones. Típicamente modificando la pila de IP para soportar IPSec de forma nativa, cuando esto no es posible, puede implementarse como interceptor que extrae e inserta paquetes en la pila de IP "Bump in the Stack" (BITS), o bien utilizando un dispositivo de encriptación

externo dedicado "Bump in the Wire" (BITW) como se esquematiza en la figura 1.25.

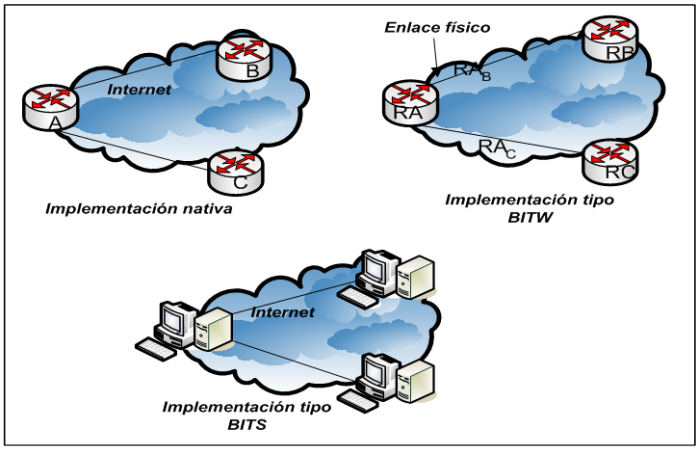


Figura 1.25. Tipos de implementaciones de IPSec.

IPSec está diseñado para operar en hosts y/o en gateways, en modo túnel para proteger datagramas IP completos (VPN), o en modo de transporte para proteger protocolos de capas superiores. A la fecha existen algunas implementaciones, sin embargo, la mayoría limitadas a la aplicación de VPN únicamente, sobre todo en implementaciones de forma nativa, de hecho es denominado por algunos como el "protocolo VPN". En los últimos años han emergido los proyectos para implementar seguridad en sistemas operativos, esquemas BITS, en busca de brindar una plataforma base de seguridad independiente de las aplicaciones preferidas por el usuario.

Configuraciones de IPSec.

Cuando la implementación de IPSec radica en un host o sistema final, los paquetes pueden ser asegurados de extremo-a-extremo, es decir desde el origen de los datos hasta su destino final. La figura 1.26 muestra este esquema, donde cada paquete que sale del host es asegurado y puede inclusive determinarse que todo paquete que no haya sido asegurado por IPSec sea eliminado. El resultado de un esquema de seguridad extremo-a-extremo, IPSec en modo transporte generalmente, donde todo el tráfico (Telnet, SMTP, HTTP, etc.) entre ambos extremos puede ser asegurado, o bien, de forma particular a través de la definición explícita de SA.

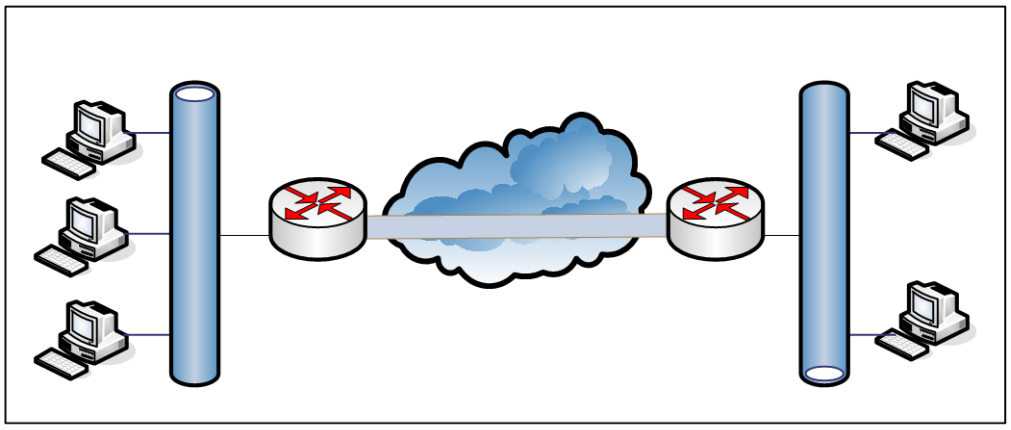


Figura 1.26. Seguridad extremo-a-extremo a través de la red.

Algo importante de mencionar de la seguridad extremo-a-extremo, es que puede afectar el funcionamiento de otras aplicaciones que requieran inspeccionar los paquetes en tránsito (Firewalls, QoS, etc.), y no puedan hacerlo, solo verán paquetes ESP. Quizá la

implementación más común son las VPN, que han sido vistas como una excelente alternativa de ahorro, en lugar de contratar líneas dedicadas, utilizar la red pública con servicios de seguridad. Cuando IPSec se aplica a routers en modo túnel, y dos routers establecen túneles a través de los cuales envían tráfico desde una subred localmente protegida hacia otra subred remotamente protegida; la figura 1.27 muestra un esquema de este tipo.

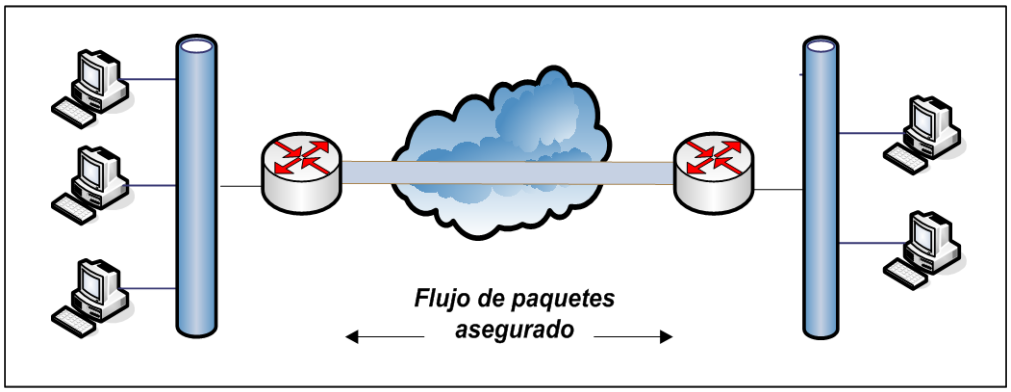


Figura 1.27. Una VPN a través de Internet.

Existe otro tipo de implementación que es una combinación de la extremo-a-extremo donde un host encripta y desencripta tráfico que envía y recibe, y la VPN en donde es un router el que hace este trabajo. En la configuración del tipo "*Road Warrior*", una computadora implementa IPSec y es capaz de asegurar los paquetes que envía y verificar la seguridad de los paquetes que recibe, su extremo IPSec es

un router que protege la red con la cual se desea establecer la comunicación. La figura 1.28 ilustra este esquema.

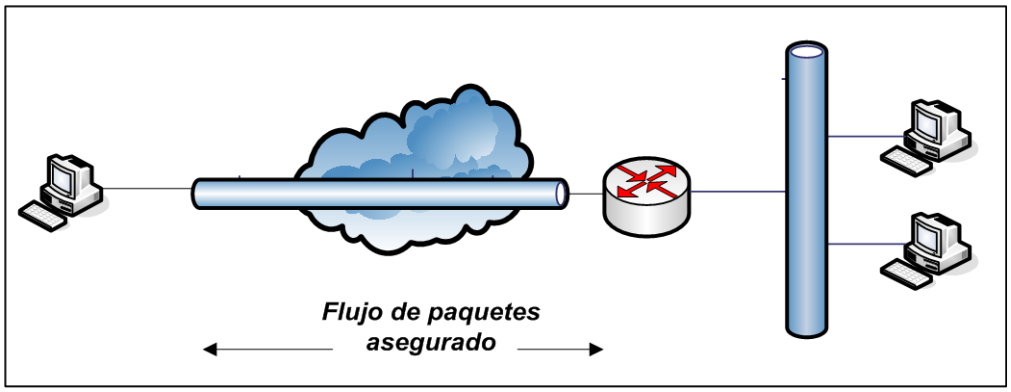


Figura 1.28. Esquema de configuración de un road warrior.

También es posible la implementación de túneles anidados, un ejemplo podría ser una institución que tiene un gateway de seguridad para proteger su red de ataques del exterior, pero además tiene otro gateway de seguridad en su red interna para protección de ataques internos. La figura 1.29 muestra este esquema, difícil de mantener y establecer, pero quizá útil y necesario para ciertas necesidades entre instituciones con instalaciones remotas.

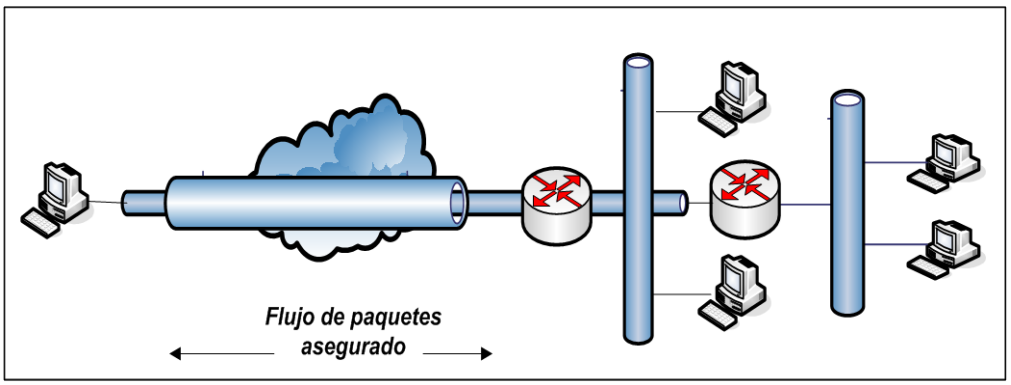


Figura 1.29. Esquema con túneles anidados.

1.3. PROTOCOLOS WAN

1.3.1. TIPOS DE PROTOCOLOS

Los protocolos de la capa física de las WAN describen cómo suministrar conexiones eléctricas, mecánicas, operacionales y funcionales para los servicios de WAN. Estos servicios a menudo se obtienen de proveedores de servicios de WAN como los RBOC, los proveedores de servicio alternos y las empresas de servicios postales, telefónicos y telegráficos (PTT).

Los protocolos de enlace de datos de las WAN describen cómo se transportan las tramas entre sistemas a través de un solo enlace de datos. Incluyen protocolos diseñados para operar a través de servicios conmutados dedicados punto a punto, multipunto y multiacceso, como ATM y Frame Relay. Los estándares de las WAN son definidos y

administrados por una serie de autoridades reconocidas, tales como las siguientes:

- Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T), antiguamente denominado Comité Consultivo Internacional Telegráfico y Telefónico (CCITT)
- Organización Internacional de Normalización (ISO)
- Fuerza de Tareas de Ingeniería de Internet (IETF)
- Asociación de Industrias Electrónicas (EIA)

Normalmente los estándares de WAN describen los requisitos de la capa física y de la capa de enlace de datos. La capa física de las WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de terminación de circuito de datos (DCE). Normalmente el DCE es el proveedor del servicio, mientras que el DTE es el dispositivo conectado. En este modelo, los servicios ofrecidos al DTE están disponibles a través de un módem o CSU/DSU.

Varios estándares de capa física especifican esta interfaz:

- EIA/TIA-232
- EIA/TIA-449
- V.24
- V.35

- X.21
- G.703
- EIA-530

1.3.1.1. FRAME RELAY

Frame Relay se define, oficialmente, como un servicio portador RDSI de banda estrecha de conmutación de paquetes, y ha sido especialmente adaptado para velocidades de hasta 2,048 Mbps., aunque nada le impide superarlas.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben de llegar ordenadas al destinatario, envista que todas siguen el mismo camino a través de la red.

TECNOLOGIAS

Las redes Frame Relay se construyen partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama Frame Relay. También incorporan los nodos que conmutan las tramas Frame Relay en

función del identificador de conexión, a través de la ruta establecida para la conexión en la red.

Este equipo se denomina FRAD o "Ensamblador/Desensamblador Frame Relay" (Frame Relay Assembler/Disassembler) y el nodo de red se denomina FRND o "Dispositivo de Red Frame Relay" (Frame Relay Network Device).

Las tramas y cabeceras de Frame Relay pueden tener diferentes longitudes, porque tiene una gran variedad de opciones disponibles en la implementación, conocidos como anexos a las definiciones del estándar básico.

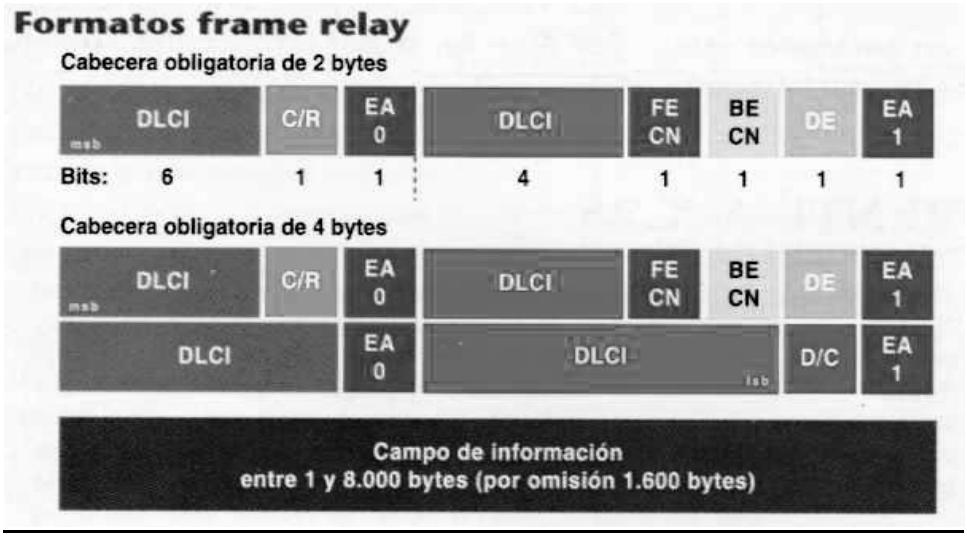


Figura 1.30. Formato de Frame Relay

DE o "elegible para ser rechazada" (Discard Eligibility). El bit DE es usado para identificar tramas que pueden ser rechazadas en la red en caso de congestión.

FECN o "notificación de congestión explícita de envío" (Forward Explicit Congestion Notification).

BECN o "notificación de congestión explícita de reenvío" (Backward Explicit Congestion Notification).

DLCI: Data Link Connection Identifier

Identificador de Conexión de Enlace de Datos: Es la cabecera de la dirección de un paquete Frame Relay. Con este identificador el FRND sabe como debe transportar el paquete que identifica el PVC correspondiente.

PVC: Permament Virtual Connection/Circuit

Circuito virtual Permanente: Conexión virtual permanente punto a punto entre dos dispositivos frame Relay que acceden a una nube FR.

Un PVC es identificado por una lista de DLCI/stream configurado a través de la red entre dos dispositivos de usuario final.

SVC: Switched Virtual Connection/Circuit

Circuito virtual Conmutado: Conexión virtual punto a punto no permanente en una red FR entre dos dispositivos FR de usuario final.

FRL: Frame Relay Link

Define el enlace físico entre dos switches FR o switche-usuario final

Valores que puede tener el DLCI

2^10=1024 DLCI

DLCI	Aplicación
0	Anexo D/A Link Protocol
1-15	Reservado
16-1007	Circuitos virtuales a usar
1008-1018	Reservado
1019-1022	Multi-cast virtual circuit
1023	Local Management Interface

Tabla 1.2. Distribución de los DLCI

Si el usuario "A" desea una comunicación con el usuario "B", primero establecerá un Circuito Virtual (VC o Virtual Circuit), que los una. La información a ser enviada se segmenta en tramas a las que se añade el DLCI.

Una vez que las tramas son entregadas a la red, son conmutadas según unas tablas de enrutamiento que se encargan de asociar cada DLCI de entrada a un puerto de salida y un nuevo DLCI.

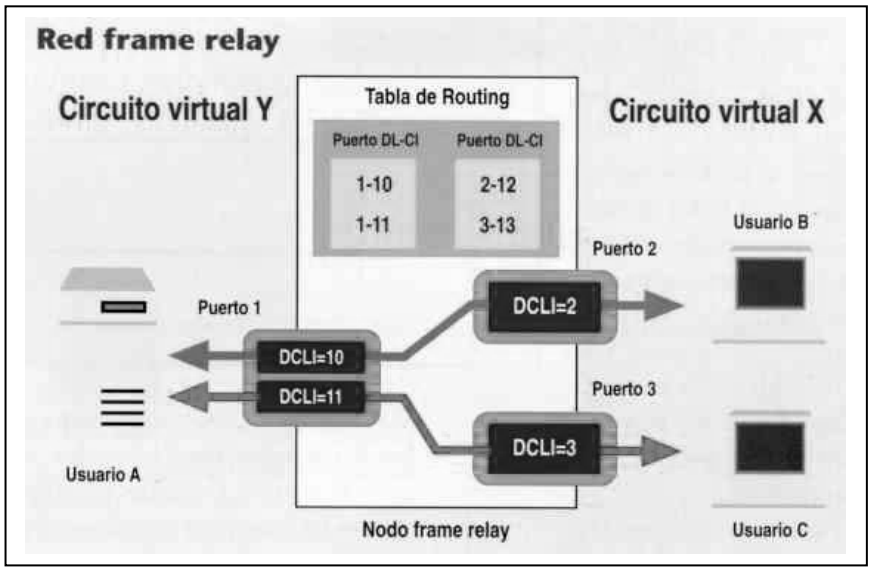


Figura 1.31. Red Frame Relay

En la actualidad las redes públicas sólo ofrecen Circuitos Virtuales Permanentes (PVC). En el futuro podremos disponer de Circuitos Virtuales Conmutados (SVC), según los cuales el usuario establecerá la conexión mediante protocolos de nivel 3, y el DLCI será asignado dinámicamente.

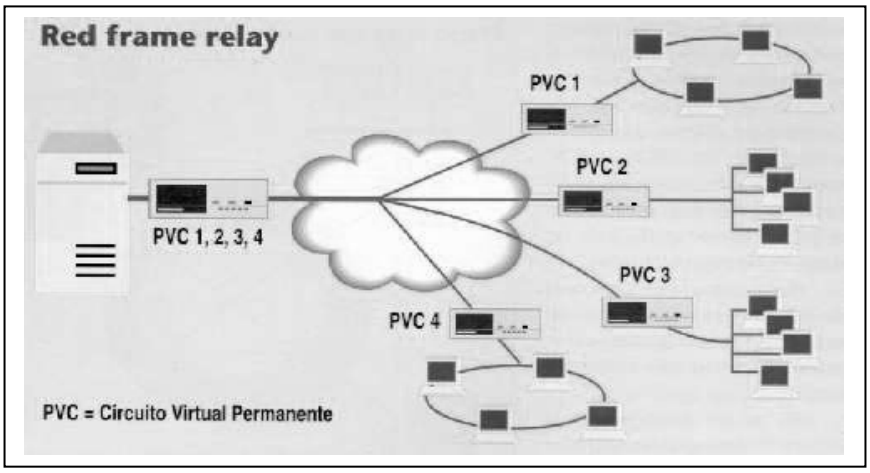


Figura 1.32. Circuitos Virtuales Permanentes

A la hora de contratar un enlace Frame Relay, hay que tener en cuenta varios parámetros. Por supuesto, el primero de ellos es la velocidad máxima del acceso (Vt), que dependerá de la calidad o tipo de línea empleada.

Pero hay un parámetro más importante: se trata del CIR (velocidad media de transmisión o Committed Information Rate). Es la velocidad que la red se compromete a servir como mínimo. Se contrata un CIR para cada PVC o bien se negocia dinámicamente en el caso de SVC's.

El Committed Burst Size (Bc) es el volumen de tráfico alcanzable transmitiendo a la velocidad media (CIR).

Por último la ráfaga máxima o Excess Burst Size (Be) es el volumen de tráfico adicional sobre el volumen alcanzable.

Para el control de todos estos parámetros se fija un intervalo de referencia (tc). Así, cuando el usuario transmite tramas, dentro del intervalo tc, a la velocidad máxima (Vt), el volumen de tráfico se acumula y la red lo acepta siempre que este por debajo de Bc. Pero si se continúa transmitiendo hasta superar Bc, las tramas empezarán a ser marcadas mediante el bit DE (serán consideradas como desechables).

Por ello, si se continúa transmitiendo superando el nivel marcado por Bc+Be, la red no admitirá ninguna trama más.

Por supuesto la tarificación dentro de cada volumen (Bc/Be) no es igual, puesto que en el caso de Be, existe la posibilidad de que las tramas sean descartadas

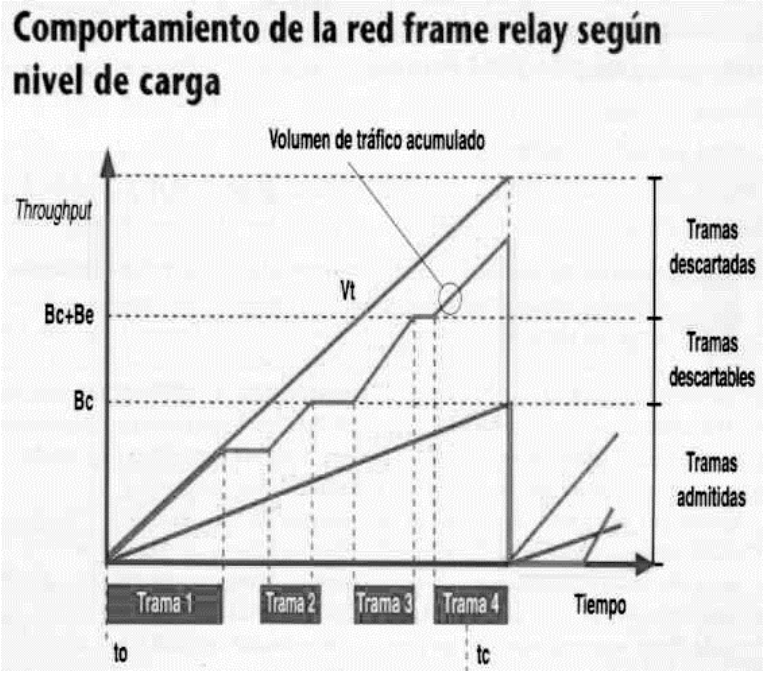


Figura 1.33. Comportamiento de la Red Frame Relay

1.3.1.2. MODO DE TRANSFERENCIA ASÍNCRONA (ATM)

La tecnología llamada *Asynchronous Transfer Mode* (ATM) Modo de Transferencia Asíncrona es el corazón de los servicios digitales integrados que ofrecerán las nuevas redes digitales de servicios integrados de Banda Ancha (B-ISDN) por conmutación de celdas fijas de 53 bytes.

ATM combina la simplicidad de la multiplexación por división en el tiempo (Time Division Multiplex TDM) encontrado en la conmutación de circuitos, con la eficiencia de las redes de conmutación de paquetes con multiplexación estadística, el mismo que asegura que

el tráfico de grandes volúmenes sea flexiblemente conmutado al destino correcto

MULTIPLEXACION EN ATM:

Un examen más cercano del protocolo ATM y cómo opera ayudará a explicar cómo los circuitos virtuales, las rutas virtuales, los conmutadores y los servicios que ellos acarrean se afectan entre sí.

La figura 1.34 muestra un formato básico y la jerarquía de ATM. Una conexión ATM, consiste de "celdas" de información contenidos en un circuito virtual (VC). Estas celdas provienen de diferentes fuentes representadas como generadores de bits a tasas de transferencia constantes como la voz y a tasas variables tipo ráfagas (bursty traffic) como los datos. Cada celda compuesta por 53 bytes, de los cuales 48 (opcionalmente 44) son para transporte de información y los restantes para uso de campos de control (cabecera) con información de "quién soy" y "a donde voy"; es identificada por un "virtual circuit identifier" VCI y un "virtual path identifier" VPI dentro de esos campos de control, que incluyen tanto el enrutamiento de celdas como el tipo de conexión.

La organización de la cabecera (header) variará levemente

dependiendo de sí la información relacionada es para interfaces de red a red o de usuario a red. Las celdas son enrutadas individualmente a través de los conmutadores basados en estos identificadores, los cuales tienen significado local - pueden ser cambiados de interface a interface.

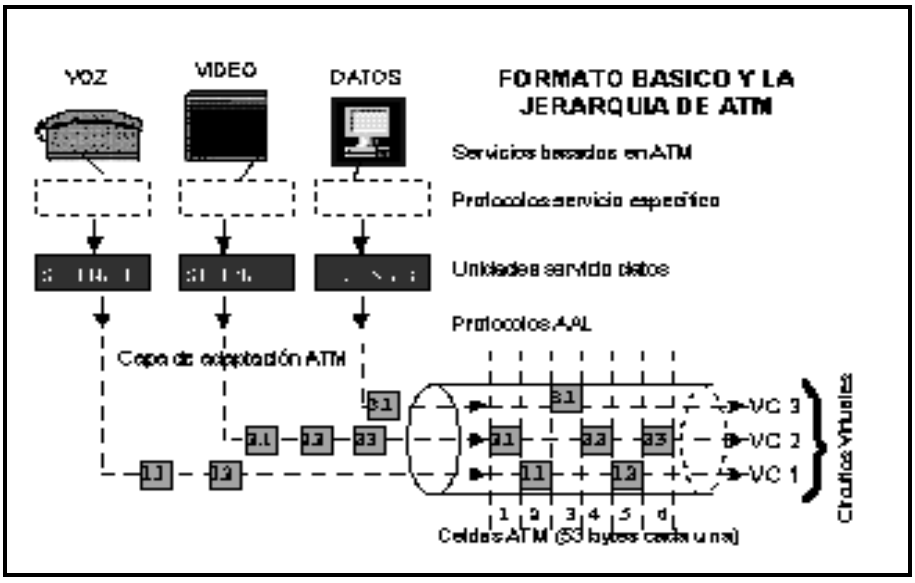


Fig. 1.34. Formato Básico de ATM

La técnica ATM multiplexa muchas celdas de circuitos virtuales en una ruta (path) virtual colocándolas en particiones (slots), similar a la técnica TDM. Sin embargo, ATM llena cada slot con celdas de un circuito virtual a la primera oportunidad, similar a la operación de una red conmutada de paquetes. La figura 1.35 describe los procesos de conmutación implícitos en los VC

switches y los VP switches.

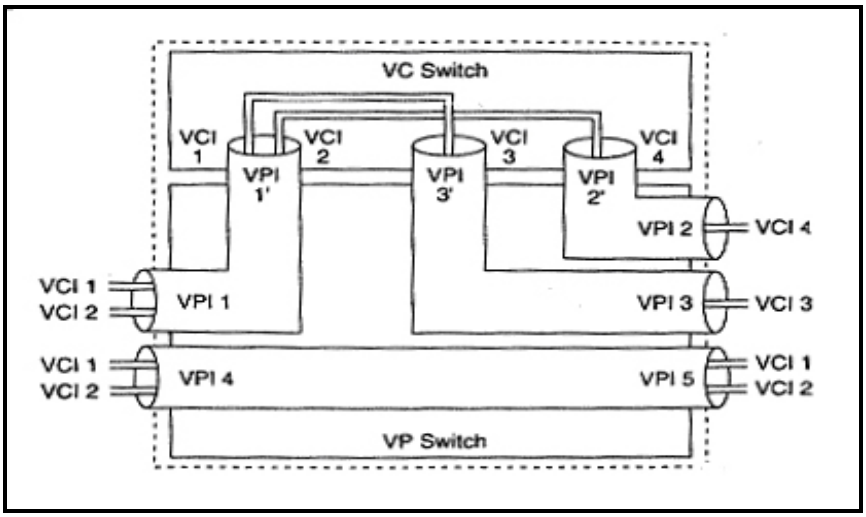


Figura 1.35. Procesos de Conmutación

Los slots de celda no usados son llenados con celdas "idle", identificadas por un patrón específico en la cabecera de la celda.

Este sistema no es igual al llamado "bit stuffing" en la multiplexación Asíncrona, porque aplica a celdas enteras.

Diferentes categorías de tráfico son convertidas en celdas ATM vía la capa de adaptación de ATM (AAL - ATM Adaptation Layer), de acuerdo con el protocolo usado.

PROTOCOLO ATM:

El protocolo ATM consta de tres niveles o capas básicas (Ver figura 1.36).

La primera capa llamada capa física (Physical Layer), define las interfaces físicas con los medios de transmisión, y el protocolo de trama para la red ATM es responsable de la correcta transmisión y recepción de los bits en el medio físico apropiado.

A diferencia de muchas tecnologías LAN como Ethernet, que especifica ciertos medios de transmisión, (10 base T, 10 base 5, etc.) ATM es independiente del transporte físico. Las celdas ATM pueden ser transportadas en redes SONET (Synchronous Optical Network), SDH (Synchronous Digital Hierarchy), T3/E3, TI/EI o aún en modems de 9600 bps.

Hay dos subcapas en la capa física que separan el medio físico de transmisión y la extracción de los datos:

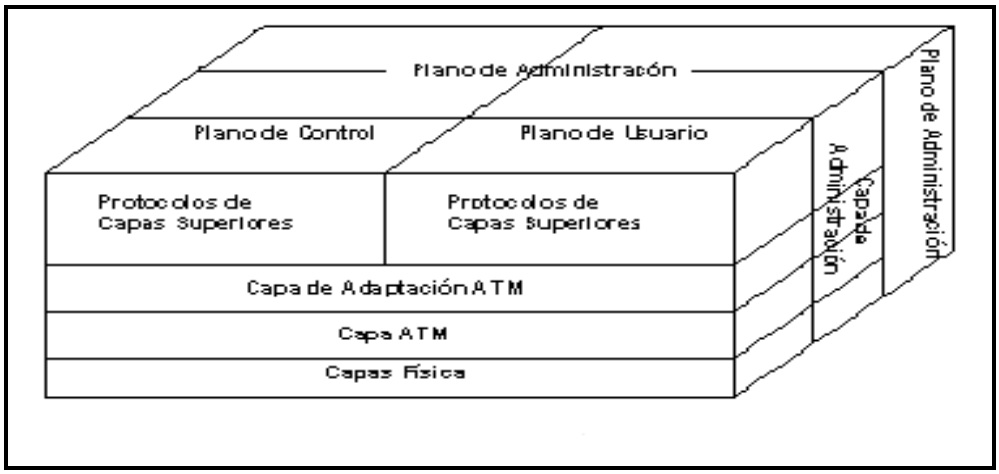


Figura 1.36. Protocolo de Modelo de Referencia para ATM de Banda Ancha

La subcapa PMD (Physical Medium Depedent) tiene que ver con los detalles que se especifican para velocidades de transmisión, tipos de conectores físicos, extracción de reloj, etc., Por ejemplo, la tasa de datos SONET que se usa, es parte del PMD. La subcapa TC (Transmission Convergence) tiene que ver con la extracción de información contenida desde la misma capa física. Esto incluye la generación y el chequeo del Header Error Corrección (HEC), extrayendo celdas desde el flujo de bits de entrada y el procesamiento de celdas "idles" y el reconocimiento del límite de la celda. Otra función importante es intercambiar información de operación y mantenimiento (OAM) con el plano de administración.

La segunda capa es la capa ATM. Ello define la estructura de la celda y cómo las celdas fluyen sobre las conexiones lógicas en una red ATM, esta capa es independiente del servicio. El formato de una celda ATM es muy simple. Consiste de 5 bytes de cabecera y 48 bytes para información.

Las celdas son transmitidas serialmente y se propagan en estricta secuencia numérica a través de la red. El tamaño de la celda ha sido escogido como un compromiso entre una larga celda, que es muy eficiente para transmitir largas tramas de datos

y longitudes de celdas cortas que minimizan el retardo de procesamiento de extremo a extremo, que son buenas para voz, vídeo y protocolos sensibles al retardo. A pesar de que no se diseñó específicamente para eso, la longitud de la celda ATM acomoda convenientemente dos Fast Packets IPX de 24 bytes cada uno.

Los comités de estándares han definido dos tipos de cabeceras ATM: los User-to-Network Interface (UNI) y la Network to Network Interface (NNI). La UNI es un modo nativo de interfaz ATM que define la interfaz entre el equipo del cliente (Customer Premises Equipment), tal como hubs o routers ATM y la red de área ancha ATM (ATM WAN). La NNI define la interfase entre los nodos de la redes (los switches o conmutadores) o entre redes. La NNI puede usarse como una interfase entre una red ATM de un usuario privado y la red ATM de un proveedor público (carrier). Específicamente, la función principal de ambos tipos de cabeceras de UNI y la NNI, es identificar las "Virtual paths identifiers" (VPIS) y los "virtual circuits" o virtual channels"(VCIS) como identificadores para el ruteo y la conmutación de las celdas ATM.

La capa de adaptación de ATM:

La tercera capa es la ATM Adaptation Layer (AAL). La AAL juega un rol clave en el manejo de múltiples tipos de tráfico para usar la red ATM, y es dependiente del servicio. Específicamente, su trabajo es adaptar los servicios dados por la capa ATM a aquellos servicios que son requeridos por las capas más altas, tales como emulación de circuitos, (circuit emulation), vídeo, audio, frame relay, etc. La AAL recibe los datos de varias fuentes o aplicaciones y las convierte en los segmentos de 48 bytes. Cinco tipos de servicios AAL están definidos actualmente:

La capa de Adaptación de ATM yace entre el ATM layer y las capas más altas que usan el servicio ATM. Su propósito principal es resolver cualquier disparidad entre un servicio requerido por el usuario y atender los servicios disponibles del ATM layer. La capa de adaptación introduce la información en paquetes ATM y controla los errores de la transmisión. La información transportada por la capa de adaptación se divide en cuatro clases según las propiedades siguientes:

1. Que la información que está siendo transportada dependa o no del tiempo.
2. Tasa de bit constante/variable.
3. Modo de conexión.

Estas propiedades definen ocho clases posibles, cuatro se definen como B-ISDN Clases de servicios. La capa de adaptación de ATM define 4 servicios para equiparar las 4 clases definidas por B-ISDN:

- AAL-1
- AAL-2
- AAL-3
- AAL-4

La capa de adaptación se divide en dos subcapas:

Capa de convergencia (convergence sublayer (CS)):

En esta capa se calculan los valores que deben llevar la cabecera y los payloads del mensaje. La información en la cabecera y en el payload depende de la clase de información que va a ser transportada.

Capa de Segmentación y reensamblaje (segmentation and reassembly (SAR))

Esta capa recibe los datos de la capa de convergencia y los divide en trozos formando los paquetes de ATM. Agrega la cabecera que llevara la información necesaria para el reensamblaje en el destino.

La figura 1.37 aporta una mejor comprensión de ellas. La subcapa CS es dependiente del servicio y se encarga de recibir y paquetizar los datos provenientes de varias aplicaciones en tramas o paquete de datos longitud variable.

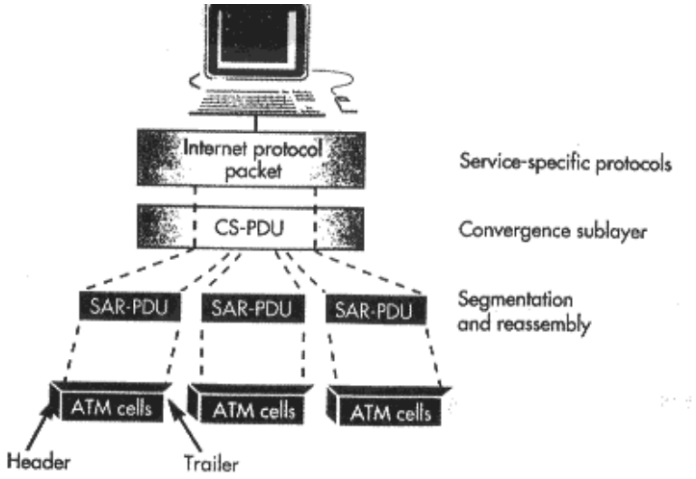


Figura 1.37. Subcapas de CS y SAR

Estos paquetes son conocidos como (CS - PDU) CONVERGENCE SUBLAYER PROTOCOL DATA UNITS.

Luego, la sub capa recibe los SAR CS-PDU, los reparte en porciones del tamaño de la celda ATM para su transmisión. También realiza la función inversa (reemsamblado) para las unidades de información de orden superior. Cada porción es ubicada en su propia unidad de protocolo de segmentación y reemsable conocida como (SAR-PDU) SEGMENTATION AND REASSEMBLER PROTOCOL DATA UNIT, de 48 bytes.

Finalmente cada SAR - PDU se ubica en el caudal de celdas ATM con su header y trailer respectivos.

AAL1:

AAL-1 se usa para transferir tasas de bits constantes que dependen del tiempo. Debe enviar por lo tanto información que regule el tiempo con los datos. AAL-1 provee recuperación de errores e indica la información con errores que no podrá ser recuperada.

ALL 2:

AAL-2 se usa para transferir datos con tasa de bits variable que dependen del tiempo. Envía la información del tiempo conjuntamente con los datos para que esta pueda recuperarse en el destino. AAL-2 provee recuperación de errores e indica la información que no puede recuperarse.

AAL 3:

AAL-3 se diseña para transferir los datos con tasa de bits variable que son independientes del tiempo. AAL-3 puede ser dividido en dos modos de operación:

Fiable: En caso de perdida o mala recepción de datos estos vuelven a ser enviados. El control de flujo es soportado.

No fiable: La recuperación del error es dejado para capas mas altas y el control de flujo es opcional.

ALL 4:

AAL-4 se diseña para transportar datos con tasa de bits variable independientes del tiempo. Es similar al AAL3 y también puede operar en transmisión fiable y o fiable. AAL-4 provee la capacidad de transferir datos fuera de una conexión explícita.

AAL 2, AAL 3/4 y AAL 5 manejan varios tipos de servicios de datos sobre la base de tasas de bits variables tales como Switched Multimegabit Data Service (SMDS), Frame Relay o tráfico de redes de área local (LAN). AAL 2 y AAL 3 soportan paquetes orientados a conexión. (Ver figura 1.38)

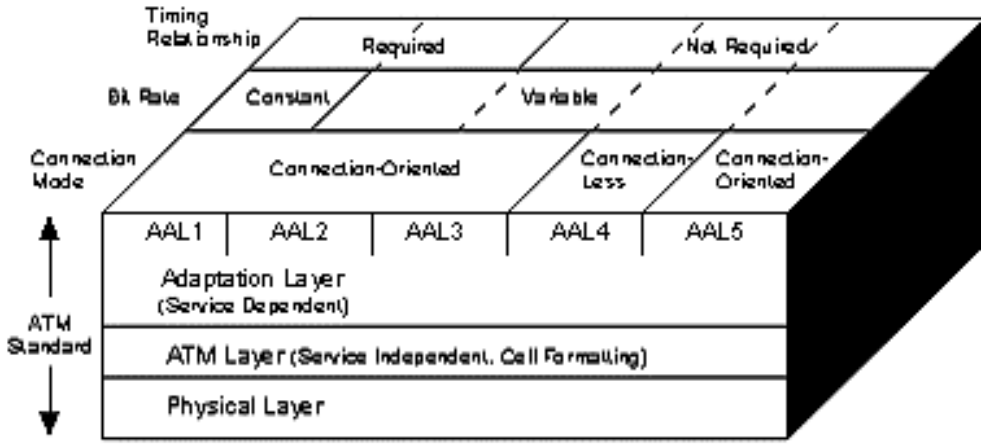


Figura 1.38. ATM y AAL

CAPITULO 2

REDES PRIVADAS VIRTUALES (VPN)

2.1. DEFINICION DE VPN

Una VPN (Virtual Private Network) es una tecnología en la que se establecen canales seguros de comunicación que ofrecen protección a los datos transmitidos mediante el uso de algoritmos de encriptación y/o autentificación criptográfica. Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red publica.

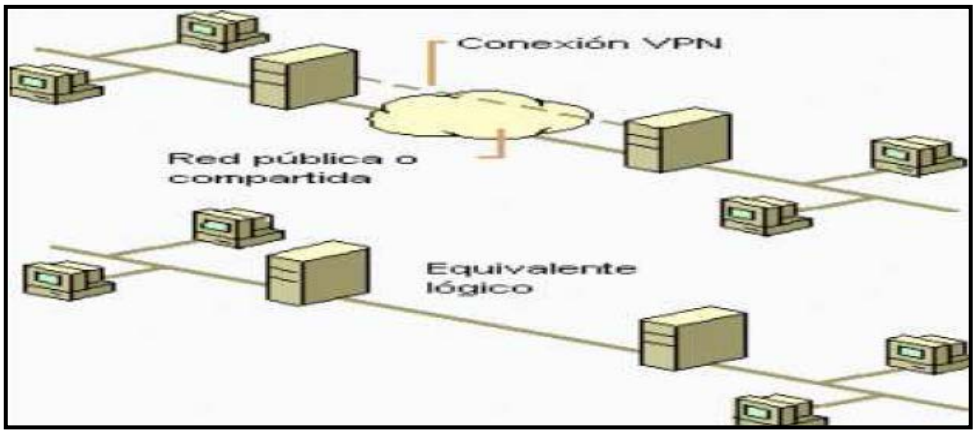


Figura 2.1. Túnel VPN

En la figura 2.2 se muestra como viajan los datos a través de una VPN, del servidor parten los datos, llegando al firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a la nube de Internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad garantizada, con un ancho de banda también garantizado lleguen a su vez al firewall remoto y terminan en el servidor remoto.

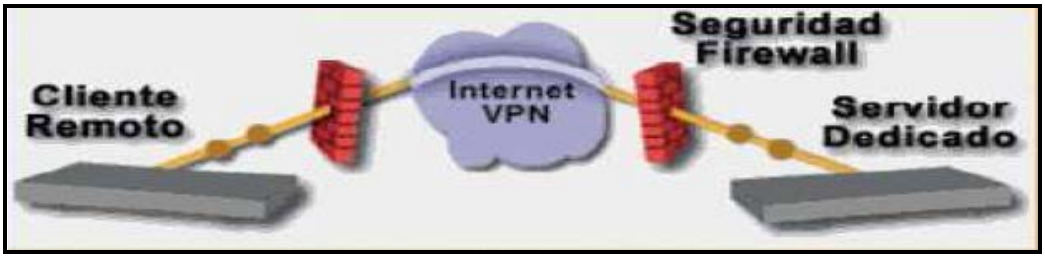


Figura 2.2. Datos a través de una VPN

Una VPN es *virtual* porque no es físicamente una red distinta, es *privada* porque la información que transita por los túneles es encriptada para brindar confidencialidad, y es una *red* porque consiste de computadoras y enlaces de comunicación, pudiendo incluir routers, switches y gateways de seguridad.

La solución VPN global tiene ciertos componentes:

- El proveedor de servicios (SP) es la empresa propietaria de la infraestructura (el equipo y los medios de transmisión) que ofrece

líneas dedicadas emuladas a sus clientes. El SP ofrece un servicio de red privada virtual a un cliente.

- El cliente se conecta a la red del SP a través de un dispositivo de equipo terminal del cliente (CPE). El CPE suele ser un dispositivo ensamblador/ desensamblador de paquetes (PAD) que proporcionan total conectividad de terminal, un bridge o un router. El dispositivo CPE también se denomina dispositivo límite del cliente (CE).
- El dispositivo CPE se conecta a través de medios de transmisión (línea dedicada, conexión telefónica) al equipo del SP, que puede ser X.25, Frame Relay o un Switch ATM o, incluso, un Router IP. El dispositivo de contorno de SP también se llama dispositivo límite del proveedor (PE).
- El SP suele tener un equipo adicional en el núcleo de su red (también llamada red P). Estos dispositivos se llaman dispositivos P. Ejemplo. router P.
- Una parte contigua de la red del cliente o usuario se llama un sitio. Un sitio se puede conectar a la red P mediante una o varias líneas de transmisión, empleando uno o varios dispositivos CE y PE, según los requisitos de redundancia.
- Una línea dedicada emulada que se le proporciona al cliente mediante el SP como circuito virtual (VC). El VC puede estar

constantemente disponible (PVC) o se puede establecer bajo demanda mediante un circuito virtual conmutado (SVC).

- El SP puede cargar una tarifa plana para el servicio VPN, que habitualmente depende del ancho de banda disponible para el cliente, una tarifa basada en el uso, que puede depender del volumen de datos intercambiados o de la duración del mismo.

2.2. TECNOLOGIAS DE TUNELES

Por tunneling entendemos la transmisión de paquetes de datos de un determinado protocolo (IP) encapsulados en otro, de manera que el contenido del paquete original pueda llegar inalterado a su destino, creando algo así como una conexión punto a punto virtual a través de una red IP.

Existen diferentes tipos de protocolos de tunneling, como GRE (RFC1701), IPSec, PPTP, L2TP (RFC2661).

GRE (Generic Routing Encapsulation):

Se utiliza normalmente en el caso de intercambios entre routers conectados mediante un acceso permanente a una red IP, donde este permite encapsular un protocolo arbitrario sobre otro protocolo arbitrario. Fue desarrollado por CISCO pero ahora es un estándar.

Al paquete IP original se le coloca un nuevo encabezado IP, en donde el campo es Protocol=47, luego de este viene el encabezado GRE.

Permite envío de Multicast e IPV6, reduce el MTU del medio en 24 bytes (20 bytes nuevo encabezado IP y 4 bytes de GRE mínimo) y puede operar detrás de firewall (pasando por el protocolo 47) y detrás de NAT.

Se puede llevar túneles GRE sobre IPSEC, para obtener seguridad llevando otros protocolos.

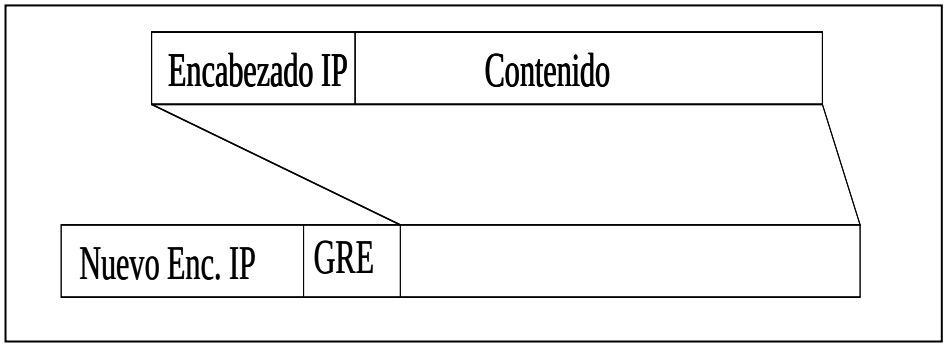


Figura 2.3. Encapsulación GRE

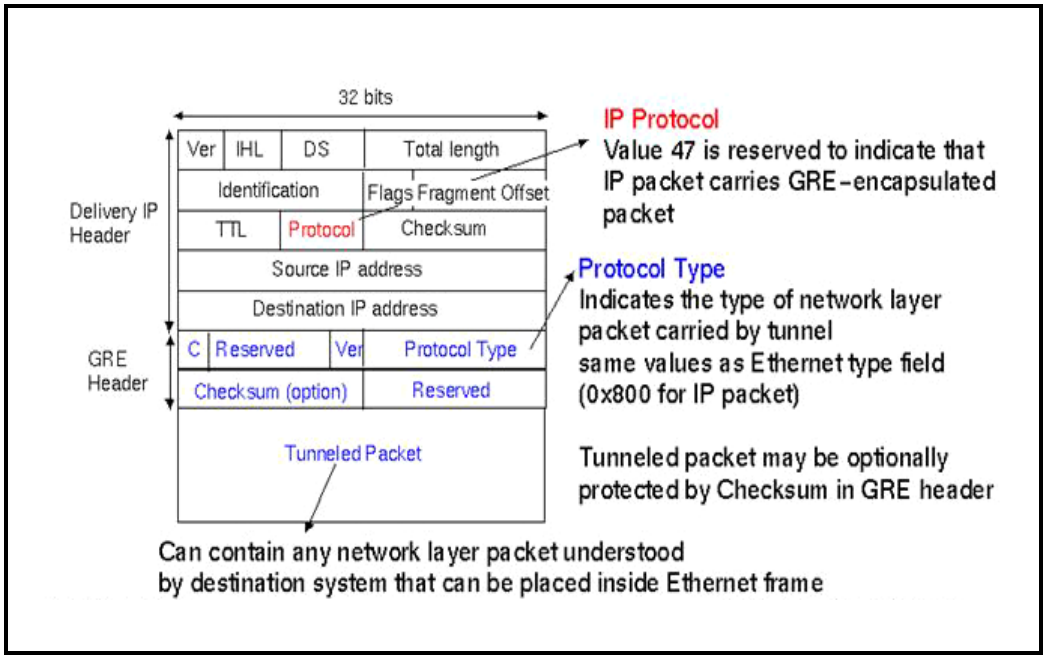


Figura 2.4. Header GRE

PPTP (Point-to-Point Tunneling Protocol)

Es quizás 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.

El protocolo PPTP fue propuesto por el Foro PPTP (PPTP Forum), compuesto por 3Com, Ascend (ahora Lucent), Microsoft, ECI Telematics y USRobotics.

Debido a la integración que hizo Microsoft en sus sistemas operativos Windows NT, y luego en Windows98 y posteriores, PPTP tuvo gran acogida en el mercado mundial, a tal punto que un protocolo de capa 2

lanzado por Cisco Systems al mismo tiempo, prácticamente no se conoció, L2F (Layer-2-Forwarding).

El protocolo más comúnmente usado para acceso conmutado a Internet es el protocolo punto-a-punto (PPP).

PPTP se soporta sobre toda la funcionalidad que PPP le brinda a un acceso conmutado para construir sus túneles a través de Internet. PPTP encapsula paquetes PPP usando una versión modificada del Protocolo de Encapsulamiento Ruteado Genérico (GRE – Generic Routing Encapsulation). Dado lo anterior, PPTP no solo es capaz de encapsular paquetes IP, sino IPX y NETBEUI, los protocolos de red local más usados.

La figura 2.5 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.

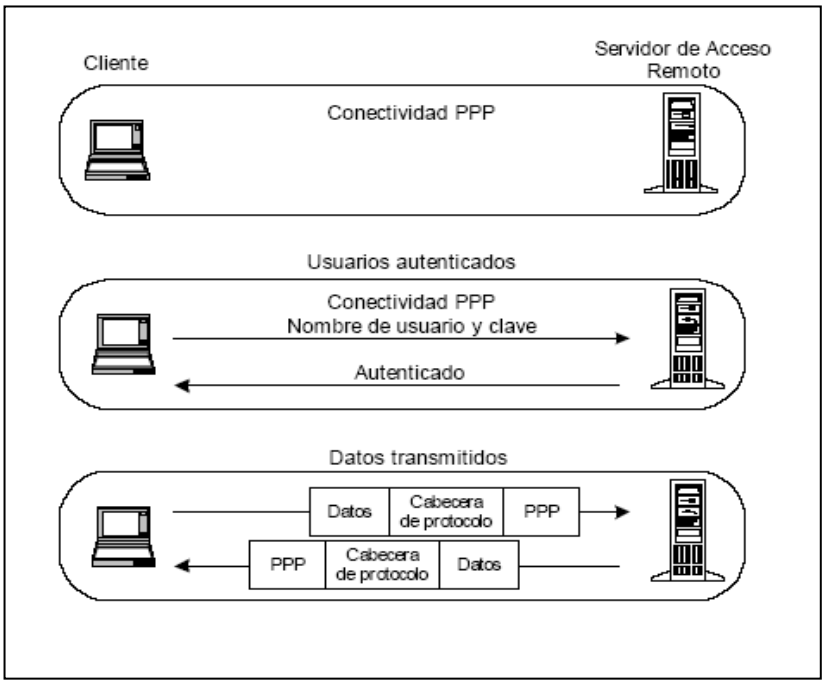


Figura 2.5. Conexión PPP típica entre un host y un RAS

PPTP utiliza los mecanismos de autenticación que generalmente están asociados a PPP tales como PAP y CHAP, una versión mejorada de CHAP llamada MS-CHAP y desarrollada por Microsoft se encuentra en sus sistemas operativos Windows NT, 2000 y XP. Otra mejora que le ha hecho Microsoft al protocolo PPTP es la incorporación del método de cifrado MPPE (Microsoft Point-to-Point Encription).

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.

Relación entre PPP Y PPTP

PPP es el protocolo más comúnmente usado para acceso a Internet, 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.

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 autenticado15. La autenticación es un paso previo para comenzar la fase de control de protocolos de red. En PPP, la autenticación puede ser implementada con PAP o CHAP16. 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 porque el usuario interactúa con el sistema autenticador respondiendo acertadamente a un requerimiento

de desafío (challenge) al host remoto, estos sistemas de autenticación son llamados de tres vías.

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

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

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

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

y el servidor PPTP. Esta conexión es usada para intercambiar mensajes de control.

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

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

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

PPTP opera con un protocolo de capa 2, debe incluir una cabecera que depende del medio de transmisión del túnel, esta puede ser Ethernet, Frame Relay o PPP. La figura 2.6 muestra la estructura en los diferentes sitios de un túnel de un paquete IP usando encapsulacion PPTP desde el sistema cliente hasta la LAN corporativa.

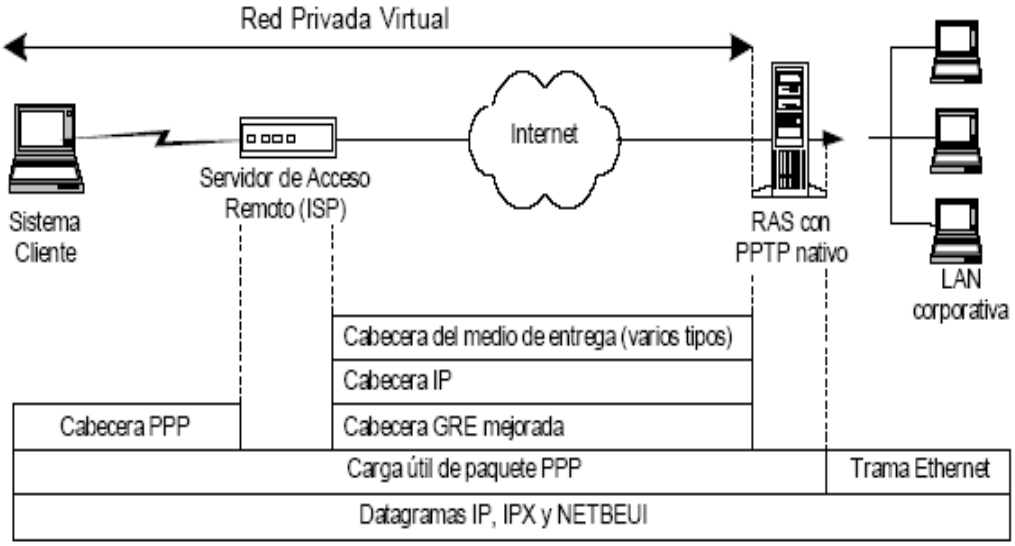


Figura 2.6 Estructura de un túnel PPTP

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 2.7 muestra un escenario de túneles voluntarios creados desde dos clientes distintos a un mismo servidor PPTP a través de Internet.

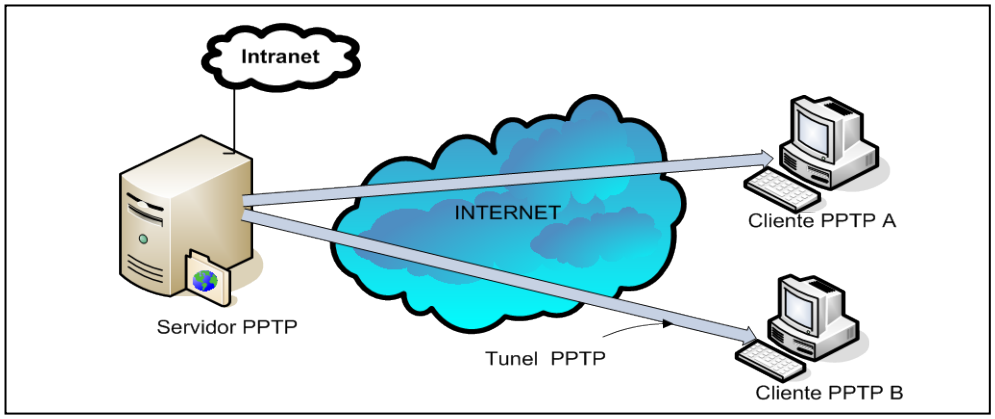


Figura 2.7. Túneles Voluntarios

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

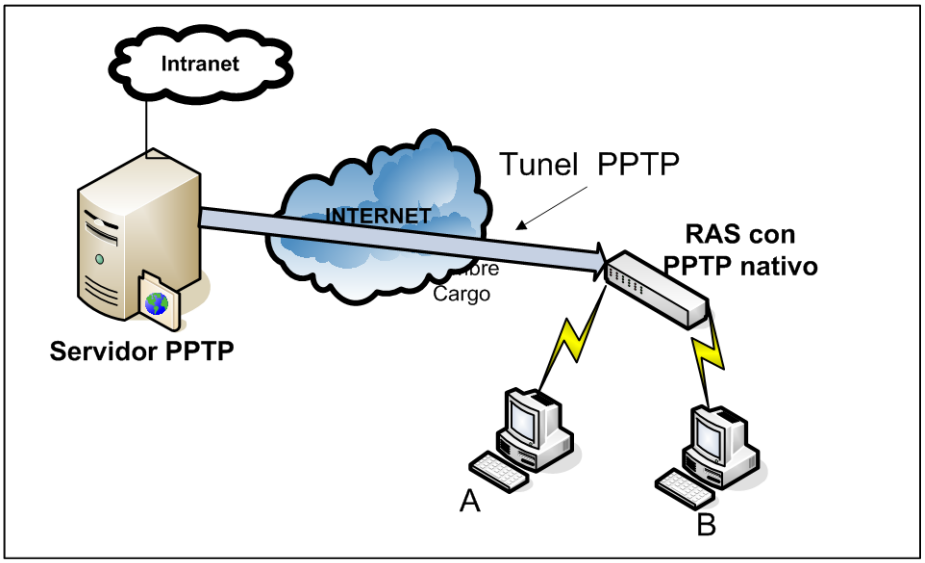


Figura 2.8 Túneles Permanentes

Dado que los túneles permanentes tienen predeterminados sus puntos finales y que el usuario no puede acceder a Internet, estos túneles ofrecen mejor control de acceso que los túneles voluntarios. Otra ventaja de los túneles permanentes, es que reducen el ancho de banda utilizado, porque 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 que 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. La información asociada con cada usuario puede residir en el servidor Radius en el que ese servidor de acceso esta autenticando todas las conexiones.

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

Entunelamiento LAN-to-LAN

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

La implementación de Microsoft para entunelamiento LAN-to-LAN exige la presencia de dos servidores PPTP que tienen la función de hacer de gateways seguros de las dos redes locales. Sin embargo, la gran desventaja de usar PPTP en topologías LAN-to-LAN es la inseguridad inherente a la arquitectura del protocolo. En efecto, la autenticación y el cifrado son controlados por protocolos que ofrecen un nivel muy bajo de confiabilidad, como CHAP o MS-CHAP. La figura 2.9 muestra una topología de red LAN-to-LAN entre una pareja de servidores PPTP usando un túnel PPTP sobre Internet, para los usuarios tanto de la LAN corporativa A como de la B el túnel es transparente, y a nivel lógico se trabaja como en una única red local.

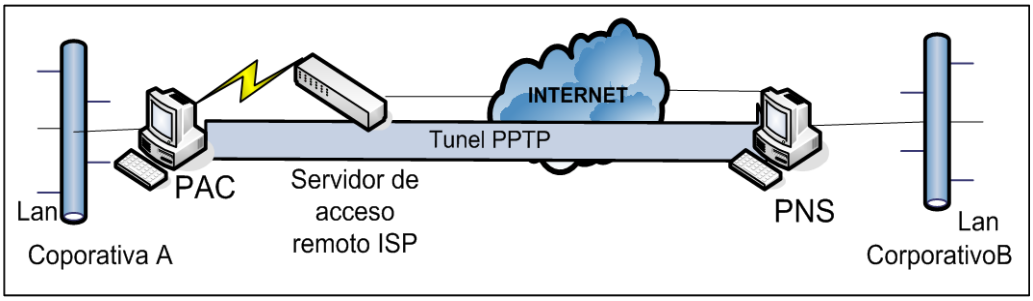


Figura 2.9 Topología LAN-to-LAN usando un túnel PPTP

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.

Componentes de una VPN PPTP

Servidores PPTP

Un servidor PPTP tiene dos funciones básicas: actuar como el punto final del túnel PPTP y reenviar los paquetes a y desde el computador en

la red privada. Para reenviar los paquetes al computador destino, el servidor desencapsula el paquete PPTP obteniendo el nombre del computador o la dirección IP privada que se encuentra dentro de este.

Una de las características de los servidores PPTP es la de poder filtrar únicamente el tráfico PPTP dependiendo de si esta condición aparece o no en el perfil del usuario, de esta manera, se puede restringir a un usuario para que se conecte a la red local o se conecte a Internet.

Por lo general los servidores PPTP están en las premisas de la red corporativa, en algunos casos el servidor PPTP está ubicado dentro de la red privada y está protegido por el firewall. Cuando esto ocurre, es necesario abrir el puerto TCP 1723, o si el firewall permite filtrar no por puerto sino por protocolo, se deberá permitir el protocolo GRE.

Software cliente PPTP

Como se dijo anteriormente, si el NAS de la ISP soporta PPTP no se necesita ningún software o hardware adicional en el extremo final del cliente, solamente que éste pueda establecer una conexión PPP. Por otro lado, si la ISP no soporta PPTP, el cliente deberá utilizar un software cliente PPTP en su computador para poder crear el túnel. Para esto primero deberá establecer una conexión PPP marcando vía modem a la ISP, y una vez establecida, deberá realizar una segunda

conexión PPTP usando un puerto virtual proveído por el software cliente PPTP.

Todos los sistemas operativos Windows 95, Windows 98, Windows NT, Windows 2000 y Windows XP cuentan con un cliente PPTP nativo. También existen clientes PPTP para Linux.

Servidores de Acceso de Red

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

Dentro de un túnel PPTP se pueden encontrar NAS actuando como clientes PPTP o simplemente como un concentrador de acceso PPP.

PPTP permite que las funciones realizadas por un servidor de acceso a la red (NAS) sean separadas usando una arquitectura cliente-servidor. Comúnmente, las siguientes funciones son implementadas por un NAS:

1. Brindar una interfaz física entre la red telefónica pública conmutada y los módems. Esto incluye conversiones A/D y D/A, conversiones síncronas a asíncronas y manipulaciones de flujos de datos.
2. Terminación lógica de enlaces PPP.
3. Autenticación de enlaces PPP.
4. Sumarización de canales (protocolo multilink PPP).
5. Terminación lógica de protocolos de control de red (NCP).
6. Enrutamiento multiprotocolo y bridging.
7. PPTP divide estas funciones entre los dos componentes que se definen en el protocolo, a saber PAC y PNS. El PAC o concentrador de acceso PPTP es el responsable de las funciones 1, 2 y algunas veces 3. El PNS o servidor de red PPTP, es el responsable de las funciones 3, 4, 5 y 6.

El protocolo PPTP es única y exclusivamente implementado entre el PAC y el PNS. Un PAC puede atender muchos PNSs. Un único PNS puede ser asociado a muchos PACs.

Estructura del Protocolo

PPTP define una conexión de control entre cada pareja PAC-PNS que opera sobre TCP; y un túnel IP operando sobre la misma pareja PAC-

PNS y es usado para transportar paquetes PPP con encapsulamiento GRE.

Conexión de control

Antes que el entunelamiento PPP ocurra entre un PAC y un PNS, una conexión de control debe ser establecida entre ellos. La conexión de control es una sesión TCP que mantiene control sobre la llamada e intercambia mensajes de información. Por cada pareja PAC-PNS debe existir una conexión de control y un túnel. La conexión de control es la responsable por el establecimiento, el manejo y la liberación de las sesiones que existen en el túnel.

El PNS y el PAC establecen la conexión de control usando mensajes Start-Control-Connection-Request y Start-Control-Connection-Reply.
Esos mensajes son también usados para intercambiar información básica entre los dos extremos del túnel. La conexión de control puede comunicar cambios entre las dos partes con un mensaje Set-Link-Info. Una sesión puede ser liberada por el PAC o por el PNS.

La conexión de control es mantenida a sí misma por mensajes de eco keep-alive. Esto asegura que una falla en la conectividad entre el PNS y el PAC pueda ser detectada tempranamente. Otras fallas pueden ser reportadas por mensajes Wan-Error-Notify.

PPTP define un conjunto de mensajes enviados como datos TCP en la conexión de control entre un PNS y un PAC. La sesión TCP es establecida hacia el puerto 1723. El puerto origen es asignado a cualquier número de puerto que no esté siendo usado en el momento del establecimiento del túnel.

Cada mensaje en la conexión de control PPTP comienza con una cabecera fija de ocho octetos, ésta cabecera contiene la longitud total del mensaje, un indicador del tipo de mensaje PPTP y una “magic cookie”.

Los tipos de mensajes de control de conexión definidos por el protocolo PPTP son: mensajes de control y mensajes de gestión; éstos últimos aún no se encuentran definidos y se han reservado para aplicaciones futuras.

La “magic cookie” es la constante 0x1A2B3C4D. Su función básica es asegurarle al receptor que está sincronizado con el flujo de datos TCP. La pérdida de sincronización no conlleva a una resincronización, sino a un cierre inmediato de la sesión TCP de la conexión de control.

Los mensajes de control definidos por el protocolo PPTP son:

Gestión de la conexión de control

Start-Control-Connection-Request

Start-Control-Connection-Reply

Stop-Control-Connection-Request

Stop-Control-Connection-Reply

Echo-Request

Echo-Reply

Gestión de la llamada

Outgoing-Call-Request

Outgoing-Call-Reply

Incoming-Call-Request

Incoming-Call-Reply

Incoming-Call-Connected

Call-Clear-Request

Call-Disconnect-Notify

Reporte de errores

WAN-Error-Notify

Control de la sesión PPP

Set-Link-Info

Operación del Túnel

PPTP necesita el establecimiento de un túnel por cada pareja PNS-PAC.

Este túnel se utiliza para transportar todos los paquetes PPP de las diferentes sesiones involucradas en la pareja PNS-PAC. Una clave que se encuentra presente en la cabecera GRE indica qué paquetes PPP pertenecen a qué sesión.

De ésta manera, los paquetes PPP son multiplexados y desmultiplexados sobre un único túnel existente entre una pareja PNS-PAC. El valor del campo Clave es definido dentro del proceso de establecimiento de la llamada.

La cabecera GRE también contiene información de reconocimiento y de secuencialización con la cual se realiza control de congestión y detección de errores en el túnel.

Los datos del usuario transportados por el protocolo PPTP son esencialmente paquetes de datos PPP. Los paquetes PPP son transportados entre el PAC y el PNS, encapsulados en paquetes GRE los cuales a su vez son transportados sobre IP. Los paquetes encapsulados PPP son esencialmente paquetes de datos PPP sin ningún elemento de tramado de medio específico. Los paquetes IP transmitidos sobre los túneles entre un PAC y un PNS tienen la estructura general que se muestra en la figura 2.10

Figura 2.10. Estructura general de un paquete IP encapsulado PPTP

L2TP (Layer 2 Tunneling Protocol)

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

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

segundo, cuando la conexión está configurada y la autenticación la realiza el gateway corporativo.

Todas las anteriores características de L2F han sido transportadas a L2TP.

Como PPTP, L2TP utiliza la funcionalidad de PPP para proveer acceso conmutado que puede ser tunelizado a través de Internet a un sitio destino.

Sin embargo, como se ha mencionado anteriormente, L2TP define su propio protocolo de entunelamiento basado en L2F permitiendo transporte sobre una amplia variedad de medios de empaquetamiento tales como X.25, Frame Relay y ATM.

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

Microsoft incluye L2TP a partir del sistema operativo Windows 2000, porque las mejoras de L2TP con respecto a PPTP saltan a la vista.

Componentes Básicos de un Túnel L2TP

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.

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.

Túnel

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

Topología de L2TP

La figura 2.11 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.

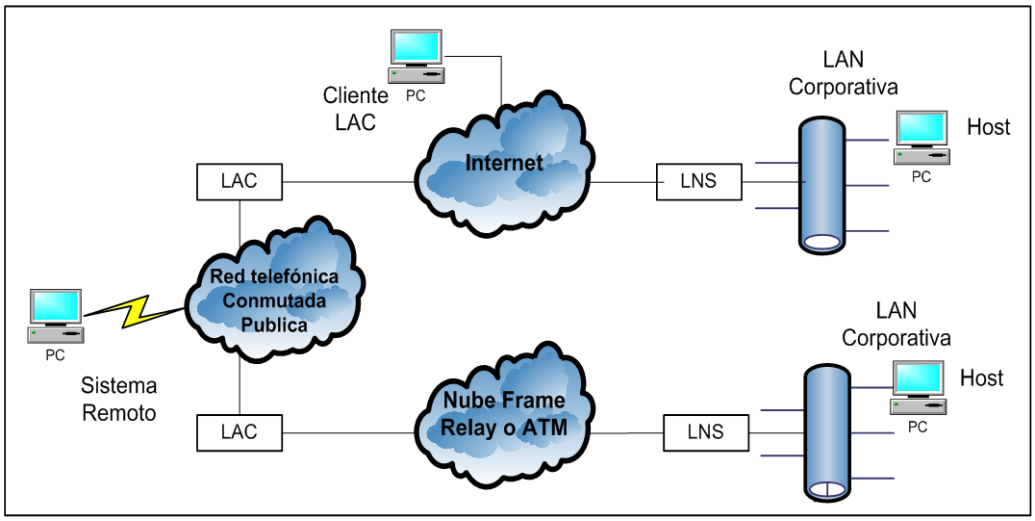


Figura 2.11 Distintos escenarios de túneles L2TP

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 acounting 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.

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 están siendo transportadas sobre el túnel. Los mensajes de control utilizan un canal de control confiable con el que L2TP garantiza la entrega. Los mensajes de datos no son retransmitidos cuando ocurren pérdidas de paquetes.

La figura 2.12 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 que 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.

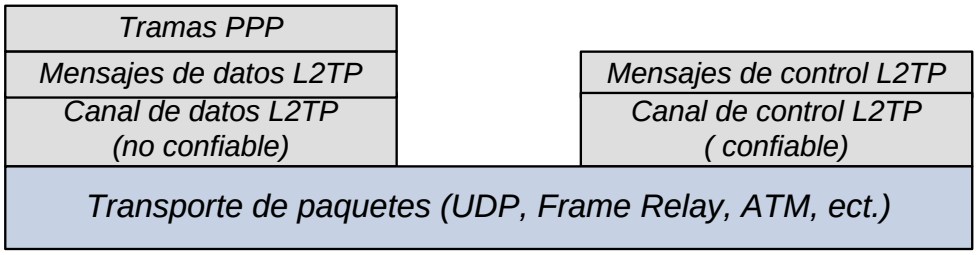


Figura 2.12 Estructura del protocolo L2TP

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 2.13 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 2.13. 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 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 mensajes 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 está 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 que la carga útil de datos es esperada a que inicie o a que se encuentre.

Tipos de Mensajes de Control

El protocolo L2TP define los siguientes tipos de mensajes de control para la creación, mantenimiento y finalización del túnel.

Manejo de la conexión de control

0 (reserved)

1 (SCCRQ) Start-Control-Connection-Request

2 (SCCRP) Start-Control-Connection-Reply

3 (SCCCN) Start-Control-Connection-Connected

4 (StopCCN) Stop-Control-Connection-Notification

5 (reserved)

6 (HELLO) Hello

Manejo de la llamada

7 (OCRQ) Outgoing-Call-Request

8 (OCRP) Outgoing-Call-Reply

9 (OCCN) Outgoing-Call-Connected

10 (ICRQ) Incoming-Call-Request

11 (ICRP) Incoming-Call-Reply

12 (ICCN) Incoming-Call-Connected

13 (reserved)

14 (CDN) Call-Disconnect-Notify

Reporte de errores

15 (WEN) WAN-Error-Notify

Control de la sesión PPP

16 (SLI) Set-Link-Info

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.

La figura 2.14 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.

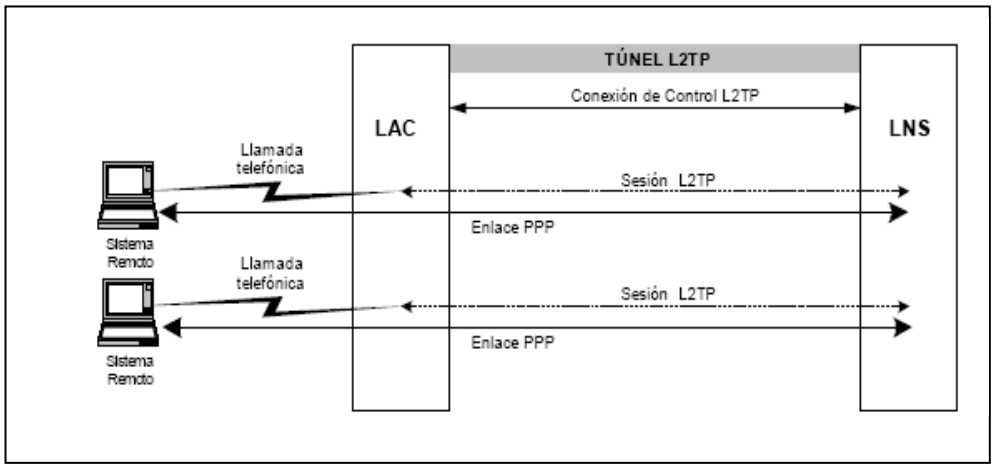


Figura 2.14 Entunelamiento de tramas PPP usando L2TP

Establecimiento de la Conexión de Control

La conexión de control es la conexión inicial que debe llevarse a cabo entre un LAC y un LNS antes que puedan crearse sesiones a través de ésta.

El establecimiento de la conexión de control incluye la verificación de la identidad del extremo remoto entre otros. Un intercambio de tres mensajes como se muestra en la figura 2.15 es utilizado para configurar la conexión de control.

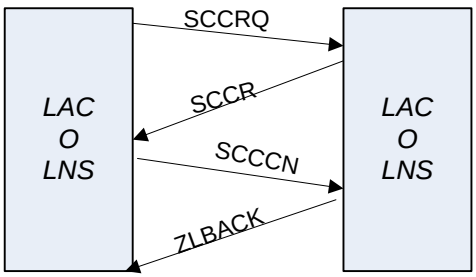


Figura 2.15 Establecimiento de una conexión de control

El ZLB ACK es enviado si no hay más mensajes esperando en cola para ese extremo.

Autenticación del Túnel

L2TP incorpora un sistema de autenticación simple y opcional parecido a CHAP durante el establecimiento de la conexión de control. Si un LAC o LNS desea autenticar la identidad de su pareja, éste le envía un challenge en el mensaje SCCRQ o SCCRP, a lo que su pareja responde con un challenge response, el que debe ser enviado en el SCCRP o SCCCN respectivamente. Si la respuesta enviada y la respuesta recibida de su pareja no concuerdan, el establecimiento del túnel no debe ser permitido.

Establecimiento de la Sesión

Después del establecimiento exitoso de la conexión de control, sesiones individuales pueden ser creadas. Cada sesión corresponde a un único stream PPP entre el LAC y el LNS. A diferencia del establecimiento de la conexión de control, el establecimiento de la sesión es direccional con respecto al LAC y al LNS. El LAC solicita al LNS aceptar una sesión para una llamada entrante, y el LNS solicita al LAC aceptar una sesión para una llamada saliente.

Establecimiento de una Llamada Entrante

La figura 2.16 muestra la secuencia típica de intercambio de tres mensajes para configurar la sesión.

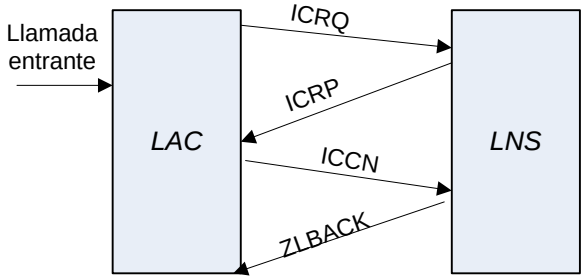


Figura 2.16. Establecimiento de una llamada entrante

El ZLB ACK es enviado si no hay más mensajes esperando en cola para la pareja remota.

Establecimiento de una Llamada Saliente

La figura 2.17 muestra la secuencia típica de intercambio de tres mensajes para configurar la sesión.

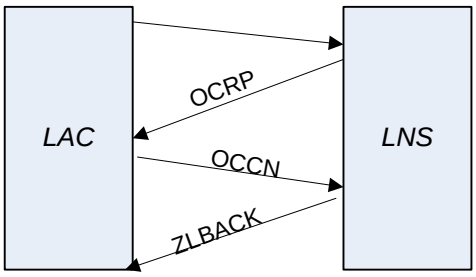


Figura 2.17 Establecimiento de una llamada saliente

El ZLB ACK es enviado si no hay más mensajes esperando en cola para la pareja remota.

Reenvío de Tramas PPP

Una vez que el establecimiento del túnel se ha completado, las tramas PPP desde el sistema remoto son recibidas en el LAC, encapsuladas en L2TP y reenviadas sobre el túnel apropiado. El LNS recibe el paquete L2TP y procesa la trama PPP encapsulada como si fuera recibida en una interfaz PPP local.

El emisor de un mensaje asociado con una sesión y un túnel particular, coloca el identificador de sesión y de túnel en los campos Session ID y Tunnel ID de la cabecera para todos los mensajes salientes. De ésta manera, las tramas PPP son multiplexadas y desmultiplexadas sobre un único túnel entre una pareja LNS-LAC.

El valor de 0 para el Session ID y Tunnel ID es especial y no debe ser usado. Para los casos donde el Session ID no ha sido aún asignado (por ejemplo durante el establecimiento de una nueva sesión o túnel), el campo Session ID debe ser enviado como 0, igualmente, para los casos donde el Tunnel ID aún no ha sido asignado desde el nodo remoto.

Uso de Números de Secuencia en el Canal de Datos

Los números de secuencias son definidos en la cabecera L2TP para los mensajes de control y opcionalmente para los mensajes de datos. Estos son usados para proveer un transporte confiable para los mensajes de control y una secuencialización opcional para los mensajes de datos.

Cada nodo mantiene una secuencia de números diferentes para la conexión de control y para cada sesión de datos individual dentro del túnel.

A diferencia del canal de control L2TP, el canal de datos no usa números de secuencia para retransmitir mensajes de datos perdidos, en vez de éstos, los mensajes de datos pueden usar números de secuencia para detectar paquetes perdidos y/o restaurar la secuencia original de paquetes que se ha perdido durante el transporte. El LAC, le puede solicitar al LNS que la secuencia de números esté presente en los mensajes de datos. El LNS controla el envío o no de la secuencia de números, si el LAC recibe mensajes de datos sin la secuencia de números presente, éste deberá parar cualquier secuencia de datos futura. Si el LAC recibe mensajes de datos con una secuencia de números presente, este deberá comenzar a enviar números de secuencia en todos los mensajes de datos salientes futuros. Estos procesos de habilitar o deshabilitar la secuencia de números puede ocurrir en cualquier momento de la transferencia de paquetes. Es recomendable activar estas características en todos los LNS para asegurar un correcto ordenamiento de todos los paquetes entrantes.

Keepalive (Hello)

Un mecanismo de keepalive es empleado por L2TP para diferenciar periodos de tiempo fuera de periodos extensos de no control o inactividad de datos en el túnel. Esto se realiza enviando mensajes de control Hello después de que un periodo de tiempo específico ha transcurrido desde que el último mensaje de control o de datos fue recibido en el túnel. Como con cualquier otro mensaje de control, si el mensaje Hello no es recibido oportunamente el túnel es declarado down y es reconfigurado. Con este mecanismo se asegura que cualquier falla de conectividad entre el LNS y el LAC sea detectada oportunamente por ambos lados del túnel.

Terminación de la Sesión

Tanto el LAC como el LNS pueden terminar una sesión, esto se logra por medio de un mensaje de control CDN, la figura 2.18 es un ejemplo típico del intercambio de mensajes de control para terminar una sesión.

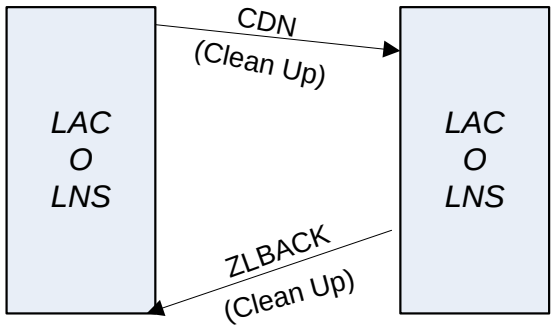


Figura 2.18 Terminación de la sesión

Terminación de la Conexión de Control

Al igual que con una sesión, la conexión de control puede ser finalizada por el LAC o por el LNS, esto se logra enviando un mensaje de control StopCCN. La figura 2.19 ilustra el intercambio de mensajes de control entre un LAC y un LNS necesarios para terminar una conexión de control.

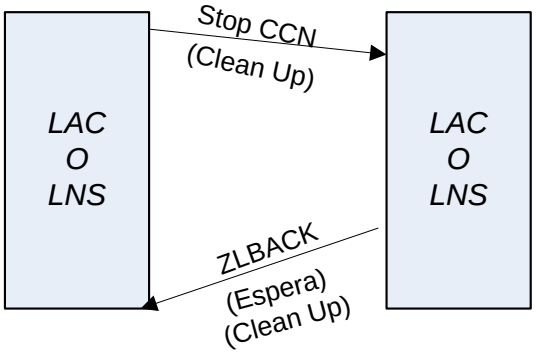


Figura 2.19 Terminación de la conexión de control

Para terminar el túnel y todas las sesiones en él, es necesario solamente en envío de un StopCCN, no se necesita bajar sesión por sesión individualmente.

2.3. TIPOS DE VPN

2.3.1 CAPA 3 VPN

Las formas como se puede hacer una VPN de capa 3 son las siguientes:

VPN con tunneling IPSec, VPN con tunneling GRE, modelo de router compartido para VPN de igual a igual, modelo de router dedicado, MPLS/VPN.

Modelo de router compartido:

El modelo de router compartido varios clientes pueden conectarse al mismo router PE (router de contorno del Proveedor). Donde las listas de acceso se tienen que configurar en cada interfaz PE-CE (router del cliente) del router PE para asegurar el aislamiento entre los clientes VPN, a fin de evitar que un cliente VPN entre en otra VPN, o evitar que un cliente VPN realice un DoS a otro cliente VPN.

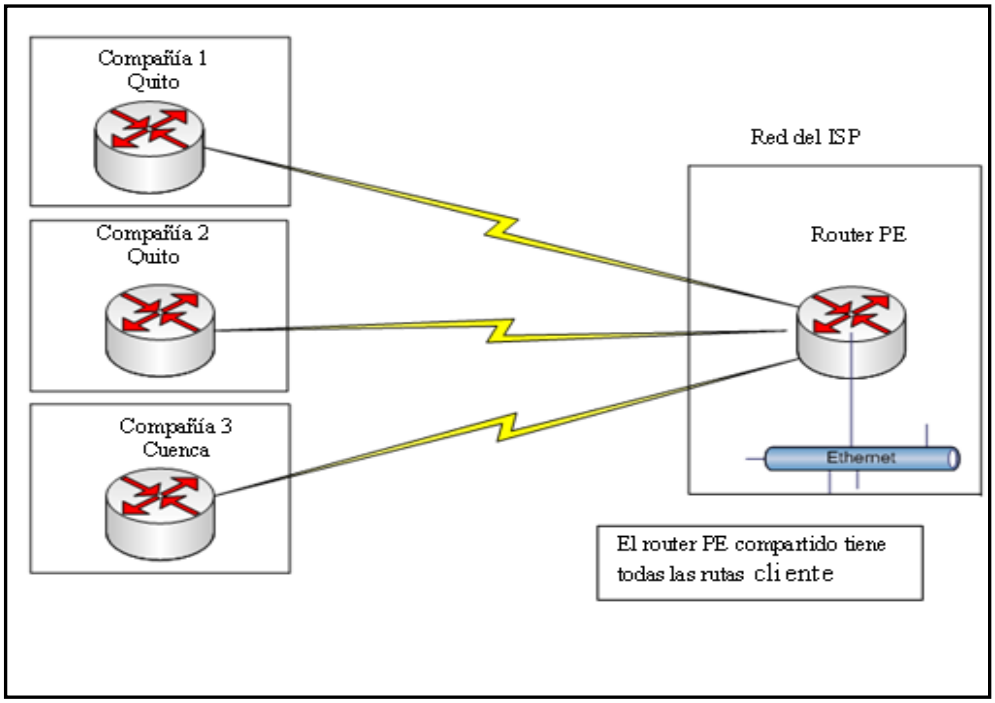


Figura 2.20. Configuración de Router Compartido

Método del router dedicado:

Este método cada cliente VPN tiene sus propios rourtes PE dedicados y por tanto, solo tiene acceso a otras rutas almacenadas en la tabla de enrutamiento de ese router PE.

Utiliza protocolos de enrutamiento para crear tablas de enrutamiento por cada VPN sobre routers PE. Las tablas de enrutamiento de los routers PE solo contienen las rutas publicadas por el cliente VPN conectado a ella, dando como resultado, un aislamiento entre los clientes VPN.

Este enrutamiento se puede implementar así:

- Cualquier protocolo de enrutamiento se ejecuta entre el router PE y el router CE.
- BGP se ejecuta entre el router PE y el router P (router Proveedor).
- Los routers P solo propagan rutas con la comunidad BGP apropiada a los routers PE. Este modo los routers PE únicamente reciben las rutas que se originaron desde los router CE en sus VPN.
- El router PE redistribuye las rutas recibidas desde el router CE mediante BGP, marcadas con él ID del cliente, y propaga las rutas a los routers P. Así los routers P contienen todas las rutas de todos los routers VPN.

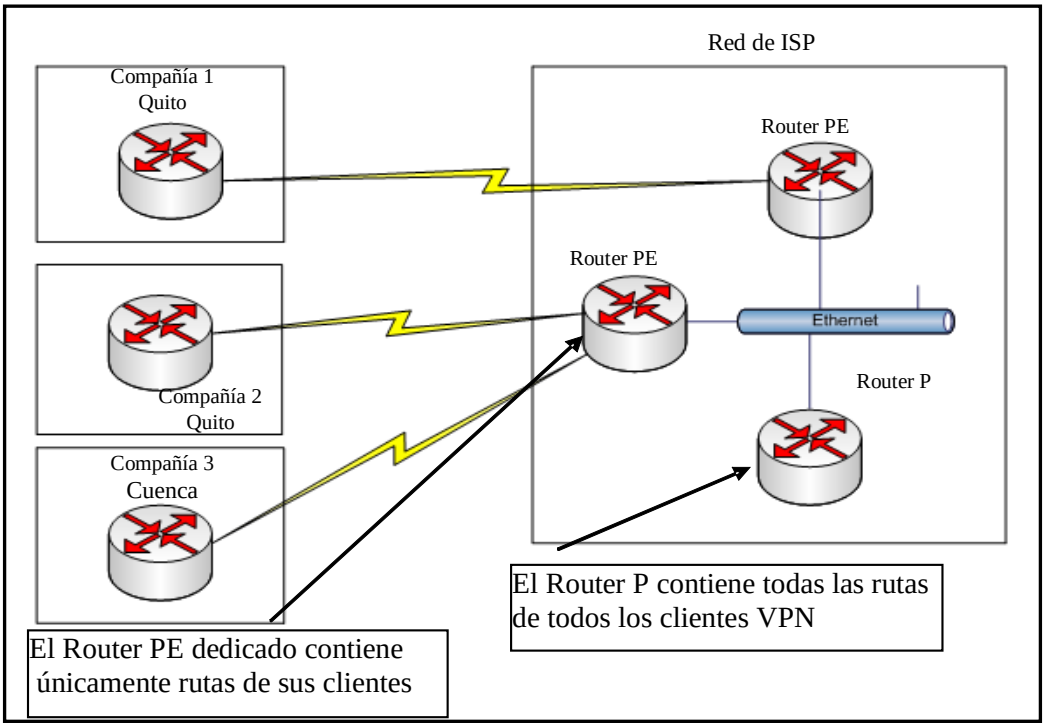


Figura 2.21. Configuración de un Router Dedicado.

MPLS/VPN

La arquitectura MPLS/VPN proporciona la capacidad de encargar una infraestructura de red IP que entregue los servicios de una red privada.

Esta tecnología proporciona una elegante solución al dilema: cada VPN tiene su propia tabla de enrutamiento y envió en el router, por lo que cada cliente o sitio que pertenezca a dicha VPN solo se le proporciona acceso al conjunto de rutas que contenga esa tabla. De este modo cualquier router PE en una red MPLS/VPN contiene un cierto numero de tablas de enrutamiento, una por cada VPN, y una tabla de enrutamiento global que se utiliza para alcanzar otros routers de la red proveedora y además alcanzar el resto de Internet.

Conceptos Básicos de la Arquitectura MPLS/VPN

La combinación de la tabla de enrutamiento IP VPN y la tabla de envió IP VPN asociada se conoce como instancia de envió y enrutamiento VPN **(VRF).**

La adición de una secuencia de 64 bits al principio de la dirección IPv4 se conoce como **Distintivo de Ruta** y es distinta para cada VPN para que las direcciones contenidas en todas las VPN sean únicas en el Backbone IP/MPLS.

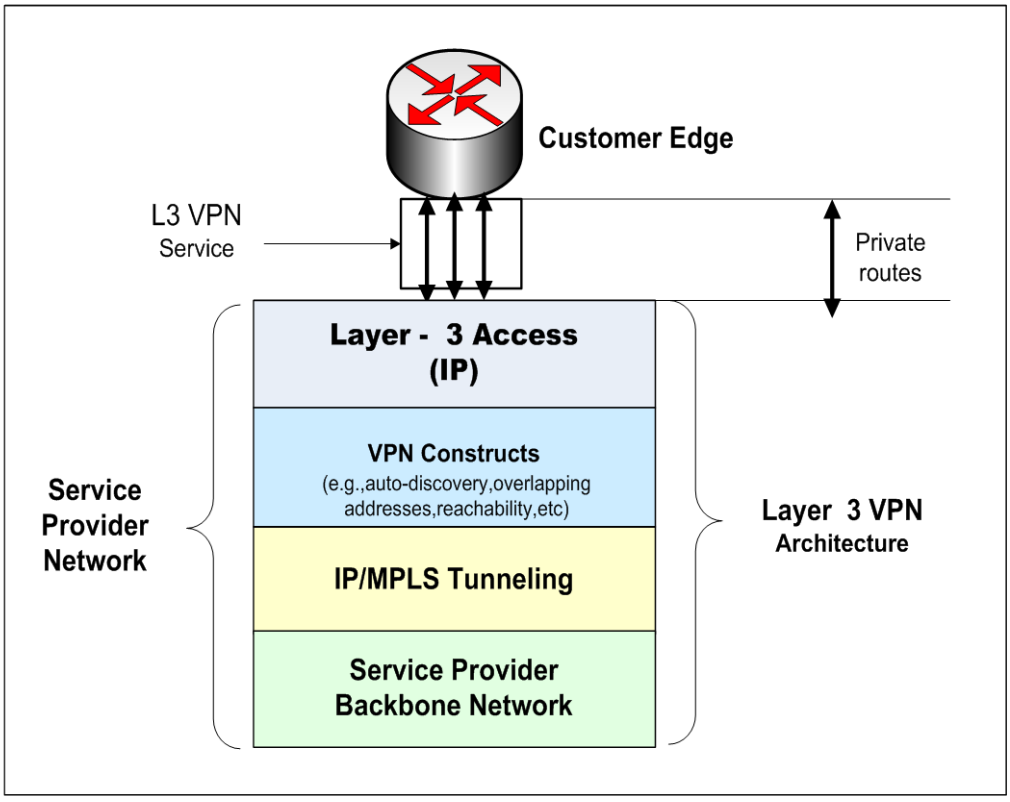


Figura 2.22. VPNs en NB de Capa 3: Vista de las Capas

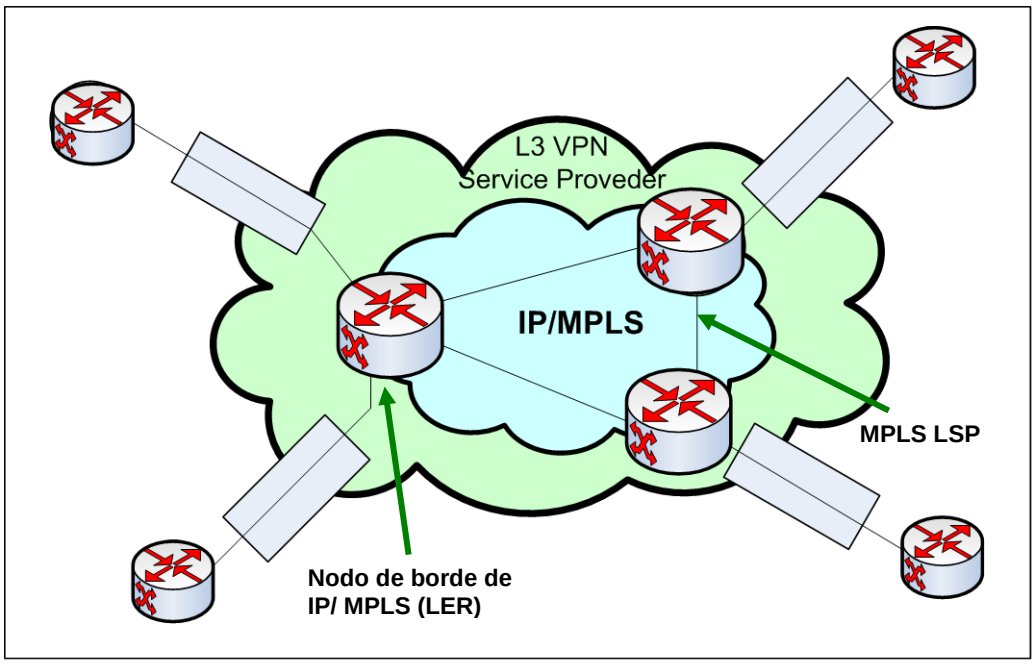


Figura 2.23. VPN de NB L3: Vista del Ruteo y Reenvió

2.3.2 CAPA 2 VPN

Las VPN de capa 2 son las llamadas VPN tradicionales las mismas que el proveedor de servicios ofrece como un conjunto de líneas dedicadas emuladas. Estas líneas dedicadas se llaman circuitos virtuales VC, los cuales pueden ser circuitos virtuales permanentes (PVC) y circuitos virtuales conmutados (SVC).

Los protocolos de enlace más utilizados para crear esta VPN son: Frame Relay y ATM. Donde el cliente establece comunicación router a router entre los dispositivos CPE sobre los VC proporcionado por el PS. Los datos del protocolo de enrutamiento siempre se intercambian entre

los dispositivos del cliente, y el SP no tiene conocimiento de la estructura externa de la red del cliente.

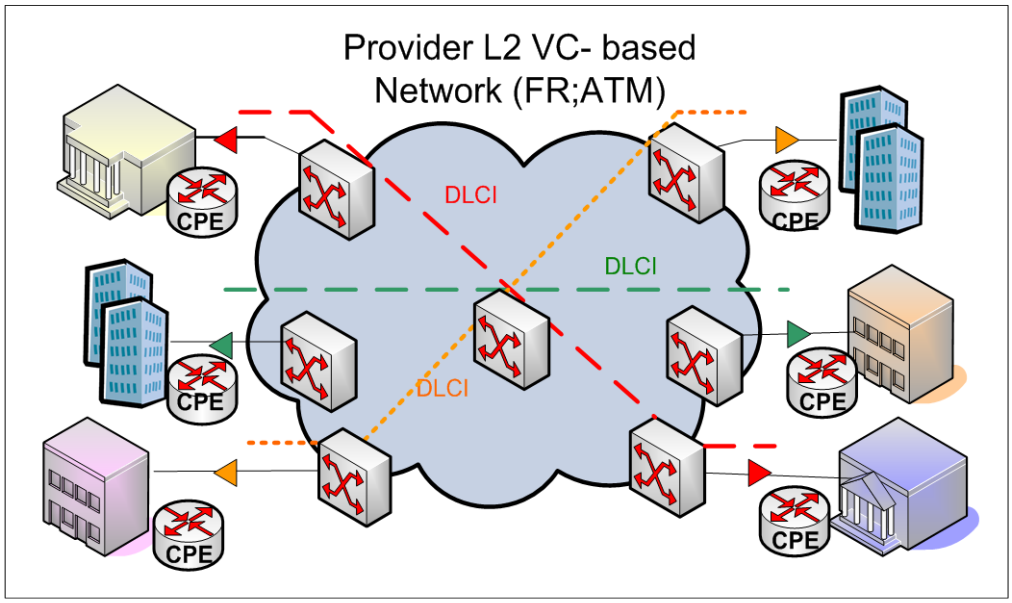


Figura 2.24. Redes basadas en Circuitos Virtuales

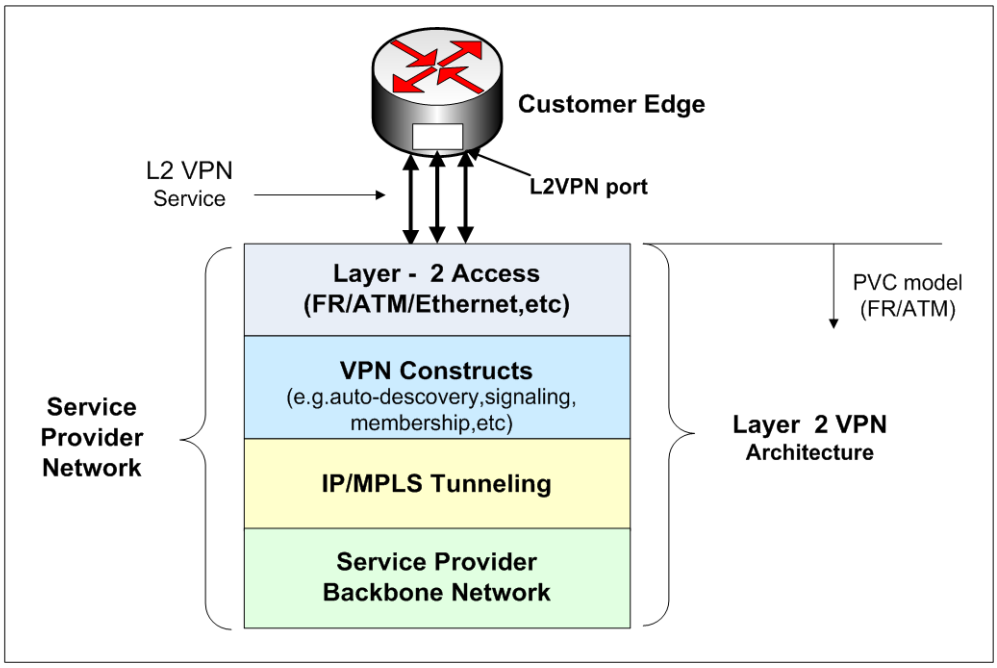


Figura 2.25. VPNs en NB de Capa 2: Una vista a sus capas

FRAME RELAY:

Circuitos virtuales Frame Relay

Frame Relay es una tecnología WAN que usa enlaces orientados a conexión, esto significa que una comunicación se define entre un par de dispositivos y que cada una de las conexiones existentes en la red tiene un identificador asociado particular. Este servicio es implementado usando circuitos virtuales, los cuales son conexiones lógicas creadas entre dos dispositivos DTE a través de la red conmutada de paquetes Frame Relay. Sobra decir que este circuito es bidireccional.

Un circuito lógico puede crearse a través de múltiples dispositivos intermediarios DCE dentro de la red Frame Relay.

Los circuitos virtuales Frame Relay se pueden dividir en dos categorías: circuitos virtuales conmutados (SVCs) y circuitos virtuales permanentes (PVCs).

Circuitos Virtuales Conmutados (SVCs)

Los SVCs son conexiones temporales y que se usan en situaciones donde la transferencia de datos entre un par de dispositivos DTE es esporádica a través de la red Frame Relay. Los SVCs tienen 4 estados operacionales:

- Call Setup: Cuando se realiza la negociación y el establecimiento de un circuito virtual entre dos DTEs.
- Data Transfer: Cuando los datos entre los dos DTEs son transmitidos sobre el circuito virtual.
- Idle: Cuando la conexión entre los dos DTEs está todavía activa, pero no hay tráfico de datos. Si por cierto periodo de tiempo el circuito se encuentra en este estado, se procede a terminar la conexión.
- Call Termination: Cuando el circuito virtual entre los dos DTEs es terminado.

Si después de terminado el circuito los dispositivos DTEs necesitan transmitir más datos, se deberá establecer un nuevo SVC, y así sucesivamente.

Este tipo de circuitos virtuales no es muy usado, de hecho muchos fabricantes no incluyen esta característica dentro de sus equipos Frame Relay.

Circuitos Virtuales Permanentes (PVCs)

Los PVCs son conexiones establecidas permanentemente y que se usan en donde la transferencia de datos es continua entre dos dispositivos DTE. Este tipo de conexiones no requieren hacer una

llamada de configuración ni de terminación como en los SVCs. De hecho los PVCs siempre operan en uno de los siguientes dos estados:

- Data transfer: Cuando los DTEs están intercambiando tráfico.
- Idle: Cuando no hay transferencia de datos, pero la conexión sigue activa. A diferencia de los SVCs, un PVC puede estar indefinidamente en este estado y el enlace no es terminado.

Identificadores de Conexión de Enlace de Datos (DLCI)

Los circuitos virtuales Frame Relay son identificados por DLCIs. Los valores de los DLCIs son asignados por el proveedor de servicio y tienen solo significado a nivel local, esto quiere decir que en una red Frame Relay pueden existir varios DLCIs con el mismo valor, pero no puede haber varios DTEs con un mismo DLCI conectados al mismo Packet Switch. Nótese que en la figura 2.26 existen valores repetidos de DLCIs pero no en un mismo DCE. Además, los dos extremos del PVC pueden tener valores diferentes.

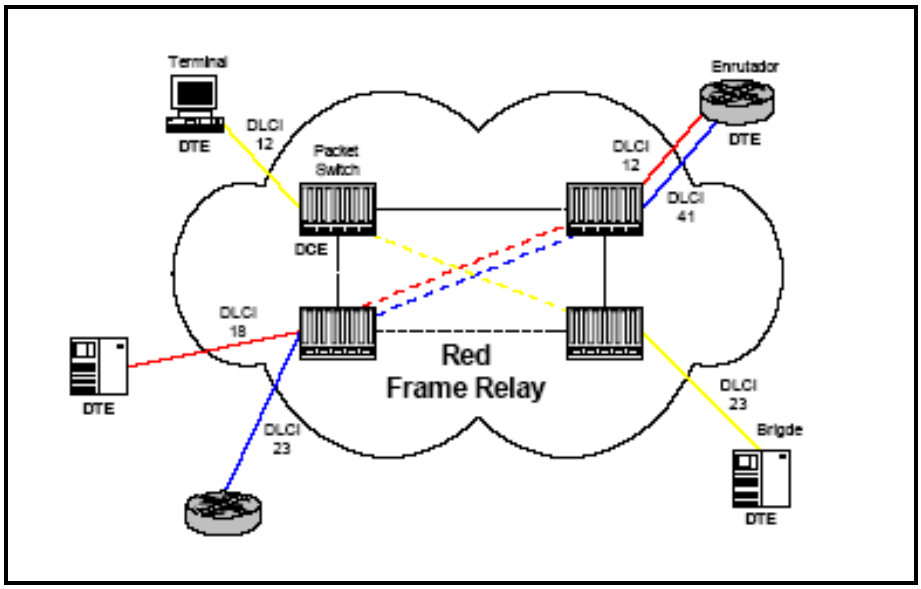


Figura 2.26. Ejemplo de asignación de valores DLCI en una red Frame Relay.

ATM:

Conexiones Virtuales ATM

Las redes ATM son básicamente redes orientadas a conexión, esto significa que se tienen que configurar canales virtuales (VC) a través de la red para la adecuada transferencia de datos. Haciendo la analogía con Frame Relay, un canal virtual equivale a un circuito virtual.

En ATM existen dos tipos de conexiones: los caminos virtuales (Virtual Paths – VPs), que son identificados por medio de VPIs (Virtual Path Identifiers), y los canales virtuales, que son identificados con una combinación de VPIs y de VCIs (Virtual Channel Identifier).

Un camino virtual es una suma de canales virtuales, cada uno es conmutado transparentemente sobre la red ATM. La figura 2.27 muestra esta relación entre VCs y VPs.

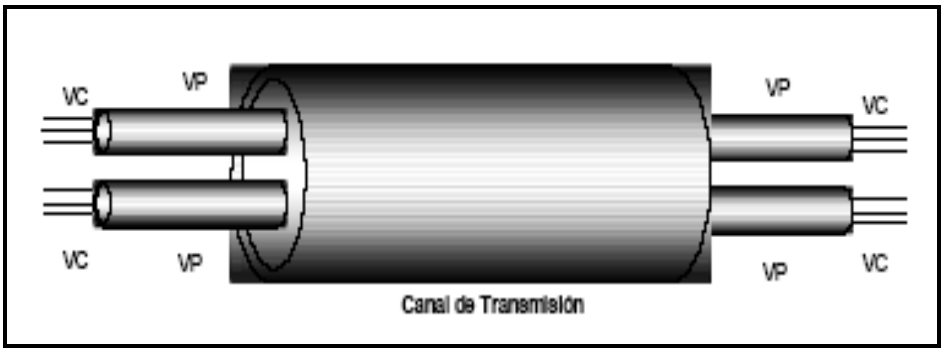


Figura 2.27. Canales Virtuales (VC) dentro de caminos virtuales (VP)

Conmutación ATM

La función básica de un Switch ATM es la de reenviar. Una celda es recibida a través de un enlace con un valor conocido VCI o VPI. El switch mira en su tabla local de traslación para determinar el puerto (o puertos) de salida para este tráfico y les coloca un nuevo VPI o VCI, y así se repite este esquema hasta que el tráfico es recibido por el punto terminal ATM. Como se puede ver, cada vez que una celda es retransmitida se le asigna un nuevo VPI o VCI, por esto se dice que estos valores solo tienen significado local y que se pueden reutilizar en otros puntos de la red cuando así se necesite.

CAPITULO 3

MULTIPROTOCOL LABEL SWITCHING

3.1. CONMUTACION MULTINIVEL (MULTILAYER SWITCHING)

3.1.1. EVOLUCION DE LA CONMUTACION MULTINIVEL

La conmutación multinivel describe la integración de la conmutación de capa 2 y el enrutamiento de capa 3. Hoy, algunas redes ISP se construyen usando el *modelo Overlay* que corre una topología de enrutamiento IP que esta sobre y es independiente de la topología conmutada de capa 2. Los switches de capa 2 proveen conectividad de alta velocidad, mientras los routers IP de frontera—interconectados por una malla de capa 2 de circuitos virtuales —proveen la inteligencia para reenviar datagramas IP. La dificultad con esta integración recae en la complejidad del mapeo entre dos arquitecturas distintas que requieren la definición y el mantenimiento de topologías separadas, protocolos de enrutamientos, protocolos de

señalización y los esquemas de asignación de recursos. El surgimiento de las soluciones de conmutación multiniveles y MPLS es parte de la evolución de la Internet para disminuir complejidad de combinar la conmutación de capa 2 y el enrutamiento de capa 3 en una solución totalmente integrada.

3.1.2. FUNDAMENTOS DE LA CONMUTACION MULTINIVEL

Antes de empezar el debate de conmutación multinivel en la Internet, es importante para entender los bloques constructivos fundamentales comunes para todas las soluciones de conmutación multinivel y MPLS:

- La separación del control y componentes de reenvío.
- El algoritmo de intercambio de etiquetas de reenvió.

3.1.2.1. SEPARACION DE LAS FUNCIONES DE CONTROL (ROUTING) Y REENVIO (FORWARDING)

Todas las soluciones de conmutación de multicapas, incluyendo MPLS, están compuestas de dos componentes funcionales distintos — un componente de control y un componente de reenvío (Figura 3.1.). El componente de control usa protocolos estándar (OSPF, IS-IS, y BGP-4) de determinación del recorrido para intercambiar información con otros routers para construir y mantener una tabla de envío. Cuando los paquetes llegan, el componente de reenvío registra la tabla de reenvío mantenida por el componente de control

para hacer una decisión de determinación del recorrido para cada paquete. Específicamente, el componente de reenvío examina información contenida en el encabezado del paquete, registra la tabla de envío por un acierto, y dirige el paquete de la interfaz de entrada a la interfaz de salida a través de la conmutación de fábrica del sistema para completamente separar el componente de control del componente de reenvío, cada componente puede ser independientemente desarrollado y modificado. El único requisito es que el componente de control continúe comunicándose con el componente de reenvío para la administración de los paquetes de tabla de envió. Veremos que la implementación de un algoritmo de reenvío sumamente simple, tal como el intercambio de etiquetas, pueden proveer las capacidades de reenvío extendidas necesarias para dar soporte a servicios de clientes que generan renta nueva.

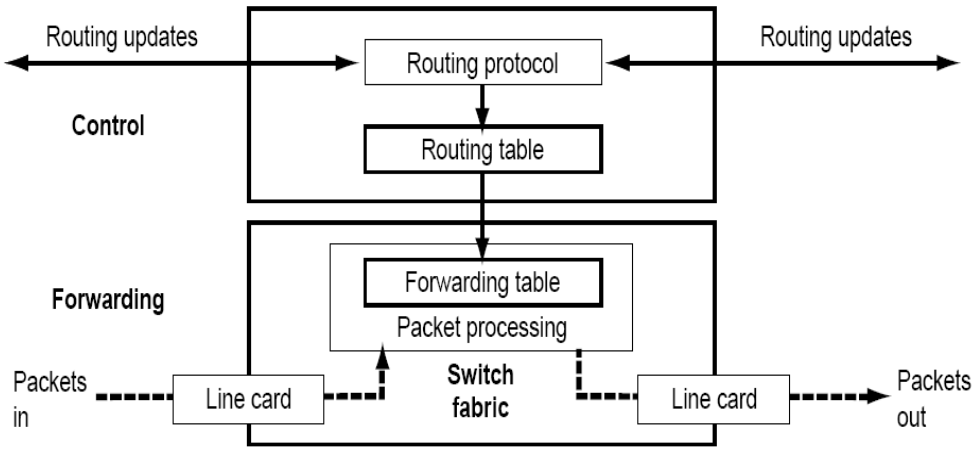


Figura 3.1. Funcionamiento del Componente de Control y Envio

3.1.2.2. ALGORITMO DE INTERCAMBIO DE ETIQUETAS DE REENVIO

El componente de reenvío de virtualmente todas las soluciones de conmutación de multicapas y MPLS se basa en una etiqueta haciendo un algoritmo de intercambio de reenvió. Este es el mismo algoritmo usado a reenviar datos en ATM y switches Frame Relay. La Señalización y la distribución de etiquetas es fundamental para la operación del algoritmo de intercambio de envió de etiquetas.

Una etiqueta es un valor corto, de longitud fija conllevado en el encabezado del paquete para identificar a un Forwarding Equivalence Class (FEC). Una etiqueta es análoga para un identificador de conexión, algo semejante como un ATM VPI/VCI o un Frame Relay DLCI, porque tiene sólo significado local en el enlace, no codifica información del encabezado de nivel de red, y los mapas de trafico para un FEC específico. Un FEC es un set de paquetes que son enviados sobre el mismo camino a través de una red aun si sus últimos destinos son diferentes.

El algoritmo de intercambio de envió de etiquetas requiere la clasificación del paquete en el borde de admisión de la red para asignar una etiqueta inicial a cada paquete. En la Figura 3.2, el Switch de entrada de etiquetas recibe un paquete sin etiqueta con una dirección de destino de 192.4.2.1. EL Switch de etiquetas realiza

una consulta de tablas de enrutamiento más largo y traza un mapa del paquete para un FEC — 192.4/16. El Switch de entrada de etiquetas luego asigna una etiqueta (con un valor de 5) al paquete y el remite al siguiente salto en el (LSP).

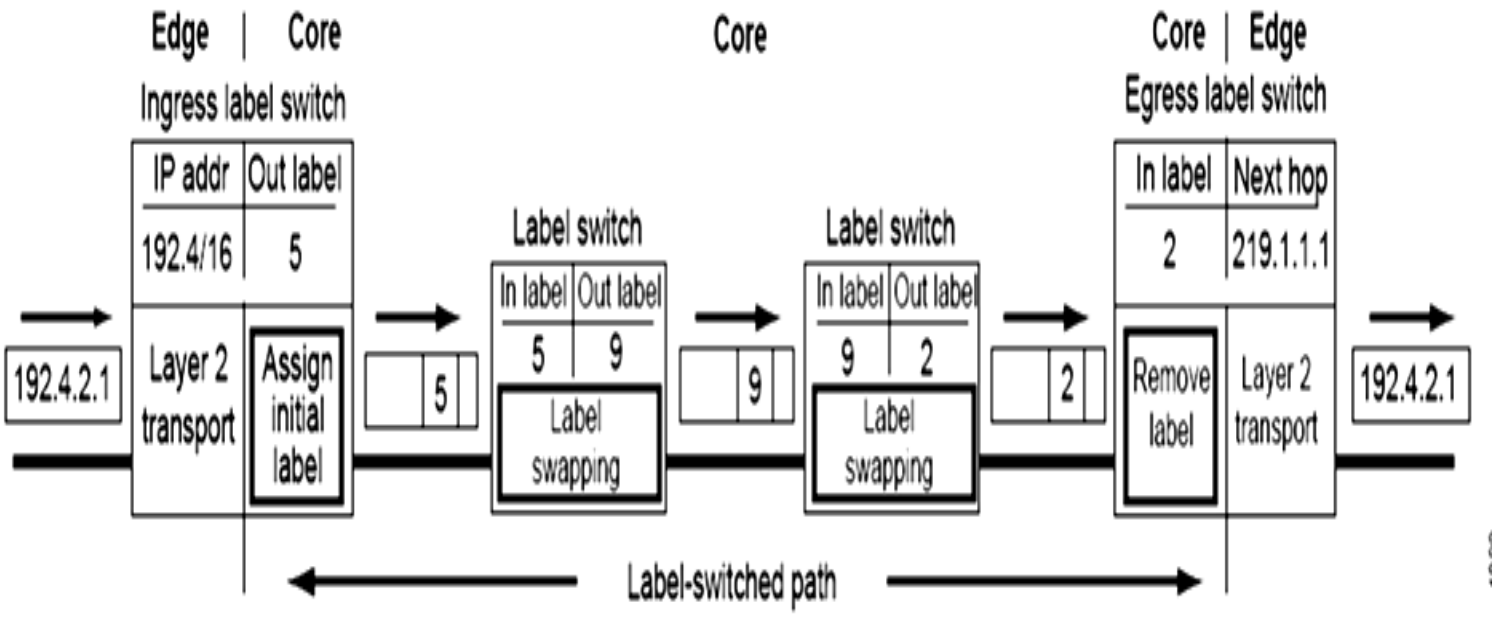


Figura 3.2 Asignación y viaje de la etiqueta en el núcleo

Un LSP equivale funcionalmente a un circuito virtual porque define una entrada o salida de un camino a través de una red que es seguido por todos los paquetes asignados para un FEC específico. La primera etiqueta de conmutación en un LSP es llamada de entrada, o fin de cabecera, de la etiqueta de conmutación. La última etiqueta de conmutación en un LSP es llamado de salida, o fin de cola, de la etiqueta de conmutación.

En el corazón de la red, las etiquetas de conmutación ignoran el encabezado de nivel de red del paquete y simplemente reenvían el paquete usando el algoritmo de intercambio de etiqueta. Cuándo un paquete etiquetado llega a un Switch, el componente de reenvío usa el número de la terminal de entrada y lo etiqueta para realizar una exacta búsqueda en su tabla de reenvío. Cuando un similar es encontrado, el componente de reenvío recupera la etiqueta saliente, la interfaz saliente, y la siguiente dirección de salto de la tabla de reenvío. El componente de reenvío luego intercambia o reemplaza la etiqueta entrante con la etiqueta saliente y dirige el paquete a la interfaz con rumbo exterior para la transmisión al siguiente salto en el LSP.

Cuándo el paquete etiquetado llega al Switch de salida de etiqueta, el componente de reenvío registra su tabla de reenvío. Si el siguiente

salto no es en el Switch de etiqueta, entonces el Switch de salida descarta la etiqueta y adelanta el paquete usando un reenvío convencional IP del similar más largo.

El intercambiar etiquetas provee un número significativo de beneficios operacionales cuándo es comparado el salto convencional con el salto en el enrutamiento de la capa de red:

- El intercambiar etiquetas le da a un proveedor de servicios una flexibilidad tremenda en la forma que asigna los paquetes a las FECs. Por ejemplo, para un simular reenvió convencional IP, el Switch de entrada de etiqueta puede ser configurado para asignar un paquete a un FEC basado en su dirección de destino. Sin embargo, los paquetes también pueden ser asignados a un FEC basado en un número ilimitado de consideraciones basadas en políticas — la dirección de la fuente aisladamente, el tipo aplicativo, el punto de entrada en la red que intercambia etiqueta, el punto de salida de la red que intercambia etiqueta, la CoS transportada en el encabezado del paquete, o cualquier combinación de lo anterior.
- Los proveedores de servicios pueden construir LSPs hechos a la medida que soportan requisitos aplicativos específicos. Los

LSPs pueden ser diseñados para minimizar el número de saltos, responsabilizarse por ciertos requisitos de ancho de banda, dar soporte a los requisitos precisos de actuación, pasar por un lado los puntos potenciales de congestión; el tráfico directo fuera del camino predeterminado seleccionado por el IGP, o simplemente forzar el trafico a través de ciertos enlaces o ciertos nodos en la red.

- El beneficio más importante del algoritmo de intercambio de etiqueta de reenvió es su habilidad para tomar cualquier tipo de tráfico del usuario, asociarse con un FEC, y trazar un mapa del FEC para un LSP que ha sido específicamente diseñado para satisfacer los requisitos del FEC. La implementación de tecnologías basadas en técnicas de intercambio de etiqueta de reenvió, ofrecen a los ISPs un control preciso sobre el flujo de tráfico en sus redes. Este nivel sin precedente de control resulta en una red que maneja más eficazmente y provee más servicio previsible.

3.1.3. CONMUTACION MULTINIVEL COMO ALTERNATIVA A IP SOBRE ATM

A mediados de los 90 IP fue ganando terreno como protocolo de red a otras arquitecturas en uso (SNA, IPX, AppleTalk, OSI...). Por otro lado, hay que recordar que los backbones IP que los proveedores de

servicio (SP) habían empezado a desplegar en esos años estaban construidos a base de routers conectados por líneas dedicadas T1/E1 y T3/E3. El crecimiento explosivo de la Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. La respuesta de los SPs fue el incremento del número de enlaces y de la capacidad de los mismos. Del mismo modo, los SPs se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de enrutamiento (basados en métricas del menor número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo. Había que idear otras alternativas de ingeniería de tráfico.

Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los routers tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los switches ATM con las capacidades de control de los routers IP. A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de telecomunicación. Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los SPs. Por un lado, proporcionaba mayores velocidades (155 Mbps) y, por otro, las características de respuesta determinísticas de los

circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó adeptos entre la comunidad de SPs, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de switches ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los routers de la periferia. Cada router comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los routers ven los PVCs como enlaces punto a punto entre cada par. En la figura 3.3 se representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre la anterior.

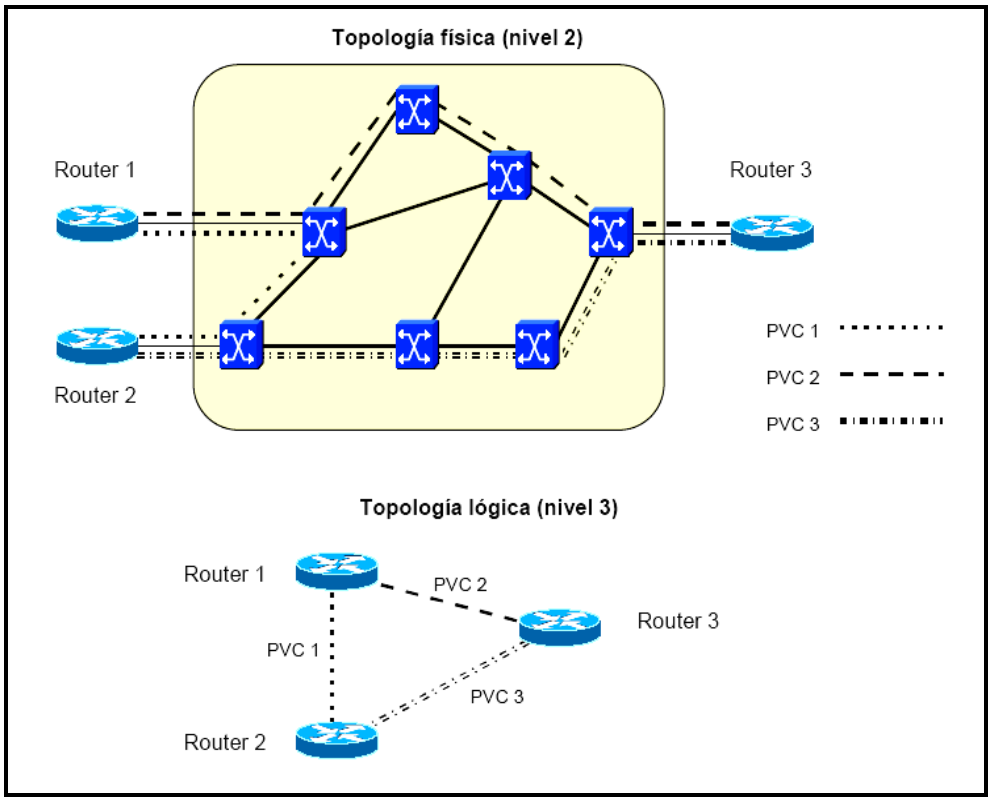


Figura 3.3. Topología física ATM y topología lógica IP superpuesta

La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y routing) y el envío de las celdas por hardware (conmutación). En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada switch de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs. Las etiquetas tienen solamente significado local en los switches y son la base de la rapidez en la conmutación de celdas. La potencia de esta solución de topologías superpuestas está en la infraestructura ATM

del Backbone; el papel de los routers IP queda relegado a la periferia, que, a mitad de los 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software. En la figura 3.4 se representa el modelo IP/ATM con la separación de funciones entre lo que es routing IP en el nivel 3 (control y envío de paquetes) y lo que es conmutación en el nivel 2 (control/señalización y envío de celdas). Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas.

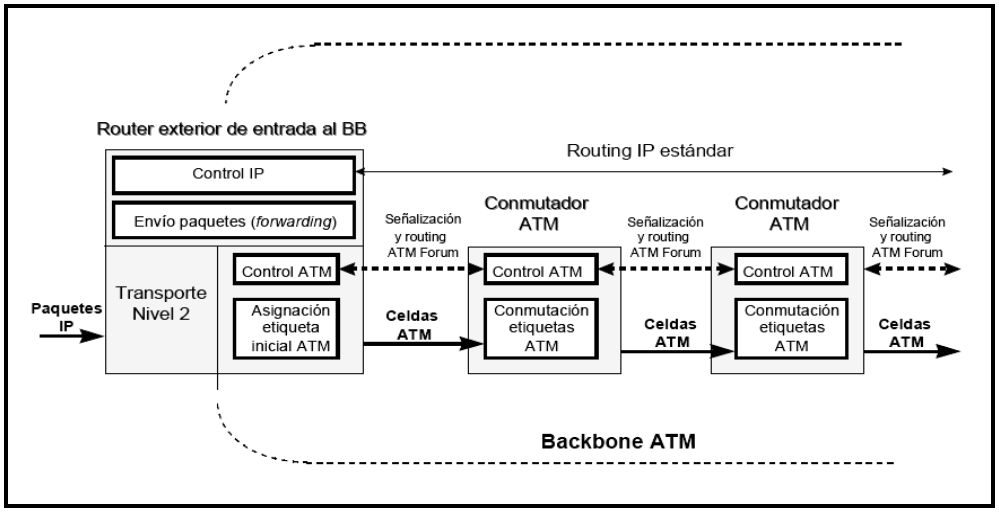


Figura 3.4. Modelo funcional IP sobre ATM

La solución de superponer IP sobre ATM permite aprovechar la infraestructura ATM existente. Las ventajas inmediatas son el ancho de banda disponible a precios competitivos y la rapidez de transporte

de datos que proporcionan los switches. En los casos de SPs de primer nivel, ellos poseen y operan el Backbone ATM al servicio de sus redes IP. Los caminos físicos de los PVCs se calculan a partir de la necesidades del tráfico IP, utilizando la clase de servicio ATM UBR (Unspecified Bit Rate), que en este caso el ATM se utiliza solamente como infraestructura de transporte de alta velocidad (no hay necesidad de apoyarse en los mecanismos inherentes del ATM para control de la congestión y clases de servicio). La ingeniería de tráfico se hace a base de proporcionar a los routers los PVCs necesarios, con una topología lógica entre routers totalmente mallada. El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de las subinterfaces en los routers con los PVCs, y estos a su vez intercambian información de enrutamiento correspondiente al protocolo interno IGP entre routers. Lo habitual es que, entre cada par de routers, haya un PVC principal y otro de respaldo, que entra automáticamente en funcionamiento cuando falla el principal.

Sin embargo, el modelo IP/ATM tiene también sus inconvenientes: Hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio unos mayores costes de gestión global de sus redes. Existe, además, lo que se llama la "tasa impuesta por la celda", un overhead aproximado del 20% que causa el transporte de datagramas IP sobre

las celdas ATM y que reduce en ese mismo porcentaje el ancho de banda disponible. Por otro lado, la solución IP/ATM presenta los típicos problemas de crecimiento exponencial n x (n-1) al aumentar el número de nodos IP sobre una topología completamente mallada. Piénsese, p. Ej., en una red con 5 routers externos con una topología virtual totalmente mallada sobre una red ATM. Son necesarios 5 x 4 =20 PVCs (uno en cada sentido de transmisión). Si se añade un sexto router se necesitan 10 PVCs más para mantener la misma estructura (6 x 5=30). Un dato adicional del crecimiento exponencial de rutas es el mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP.

Como conclusión, podemos decir que el modelo IP/ATM, si bien presenta ventajas evidentes en la integración de los niveles 2 y 3, lo hace de modo discontinuo, a base de mantener dos redes separadas. El MPLS, tal como se verá en las secciones siguientes, logra esa integración de niveles sin discontinuidades.

3.1.4. DIFERENCIAS FUNDAMENTALES ENTRE SOLUCIONES DE CONMUTACION MULTINIVEL

Mientras las diversas soluciones de conmutación multiniveles han tenido en común numerosas características, ellos confiaron en dos

avances fundamentalmente diferentes para iniciar la asignación y la distribución de ataduras de la etiqueta a establecer en los LSPs:

- Modelo de Manejo de Datos
- Modelo de Manejo de Control

3.1.4.1. MODELO DE MANEJO DE DATOS (DATA DRIVER MODEL)

En el modelo de manejo de datos, las ataduras de la etiqueta son creadas cuando los paquetes de datos del usuario llegan. Un flujo es una secuencia de paquetes que hacen las direcciones IPs de misma fuente y TCP o número de puertos UDP. Un switch multinivel puede crear una etiqueta atadora tan pronto como vea el primer paquete en un tráfico fluir o esperar hasta que ha visto un número de paquetes en el flujo. El beneficio de esperar de un número de paquetes asegura que el flujo es largo lo suficiente como para merecer los gastos fijos de asignar y distribuir una etiqueta. Las soluciones multiniveles de alternación que implementaron el acercamiento manejado de datos fueron IP Switching (Ipsilon) y el Cell Switching Router (Toshiba). Note que MPLS no da soporte al modelo de manejo de datos.

La ventaja del modelo de manejo de datos es que una atadura de la etiqueta es creada sólo cuando allí hay un flujo de tráfico

que usa la atadura de la etiqueta. Sin embargo, este modelo tiene un número de limitaciones para la implementación en el corazón de una red grande de un ISP, dónde puede haber un número enorme de tráfico individual fluyendo:

- Cada switch múltinivel debe proveer un sofisticado y un alto rendimiento en la clasificación de paquetes con capacidades para identificar flujos de tráfico.
- Típicamente, hay una latencia entre el reconocimiento de un flujo y la asignación de una etiqueta para el flujo. Esto quiere decir que cada switch multinivel también debe soportar un gran reenvió de datos IP durante la fase de esquema, así es que los paquetes que no han sido asignados a un flujo, no puede ser reenviados y descartados.
- La cantidad de control de tráfico que necesito distribuir ataduras de etiqueta es directamente proporcional al número de tráfico que fluye.
- La presencia de un número significativo de flujos relativamente de breve duración pueden imponer un calvario en operaciones de la red.
- Los dictámenes convencionales de sabiduría, que el modelo de manejo de datos no tiene las propiedades de

escalamiento requerido para la aplicación en el corazón del Internet.

CELL SWITCHING ROUTER (CSR) DE TOSHIBA:

Esta idea fue desarrollada por Toshiba y fue presentada al IETF en 1994. Su utilización comercial se centró en redes académicas de Japón.

Esta solución fue una de las primeras propuestas que trataba de utilizar los protocolos de enrutamiento del mundo IP para controlar switches ATM, y básicamente fue diseñada para conectar subredes IP utilizando una aproximación clásica de "IP sobre ATM".

En este caso los distintos Switches de etiquetas se comunican utilizando circuitos virtuales típicos de ATM, y las etiquetas son asignadas basándose en las características de los flujos de datos que se deben conmutar.

Un nuevo protocolo, denominado Flow Attribute Notification Protocol (FANP), es el responsable de identificar los VCs (circuitos virtuales) entre los nodos CSR. Asimismo se utiliza este protocolo para establecer la asociación entre los flujos de datos individuales y los VCs dedicados.

CONMUTACIÓN IP (IP SWITCHING) DE IPSILON:

Esta solución fue desarrollada por Ipsilon (posteriormente adquirida por Nokia) y lanzada al mercado a comienzos del año 1996.

Se basa en un dispositivo que puede realizar funciones de switch ATM, al que se le ha eliminado el plano de control (es decir todas aquellas funciones relacionadas con los protocolos de señalización) y también de router IP de una manera sencilla y eficiente.

Los dispositivos de conmutación IP utilizan los distintos flujos de tráfico para el establecimiento de etiquetas (que en este caso son cabeceras ATM). El funcionamiento de estos dispositivos puede describirse resumidamente de la siguiente forma: Un dispositivo de conmutación IP funciona como un router normal hasta que detecta que existe una cierta cantidad de tráfico dirigida hacia un destino concreto. Una vez detectada esta situación, establece un VC ATM para este flujo de datos concretos.

Para realizar correctamente estas funciones se definieron dos nuevos protocolos, uno destinado a establecer la relación entre los flujos de datos y las etiquetas denominados Ipsilon Flow

Management Protocol (IFMP); y otro para gestionar las funciones del switch ATM y controlar el establecimiento de los CV a través de él, conocido como General Switch Management Protocol (GSMP).

3.1.4.2. MODELO DE MANEJO DE CONTROL (CONTROL DRIVER MODEL)

En el modelo de manejo de control, las ataduras de la etiqueta son creadas cuando la información de control llega.

Las etiquetas son asignadas en respuesta al procesamiento normal del protocolo de enrutamiento de tráfico, control de tráfico como el RSVP traffic, o en respuesta a la configuración estática. Las soluciones multiniveles de alternación que implementaron el modelo de manejo de control fueron Tag Switching (Cisco Systems), IP Navigator (Ascend / Lucent), y ARIS (IBM). Además, MPLS usa el modelo de manejo de control.

El modelo de manejo de control tiene un número de beneficios para la implementación en el corazón de una gran red de un ISP:

- Las etiquetas son asignadas y distribuidas antes de la llegada de los datos de tráfico del usuario. Esto quiere decir que si una ruta existe en la tabla de reenvió IP, entonces una

etiqueta ha sido ubicada para la ruta, así es que el trafico que llegara a un Conmutador multinivel puede ser una etiqueta inmediatamente intercambiada.

- La dimensionalidad es significativamente mejor en el modelo de manejo de datos, porque el número de los caminos de etiqueta conmutadas son proporcionales para el número de entradas en la tabla de reenvió IP, no para el número de flujos individuales de tráfico. Para la ingeniería de tráfico en redes grandes del ISP, la escalada pudo estar empatada mejor — proporcional para el número de salida puntuales en la red. La asignación de etiqueta se basó en prefijos, en vez de flujos individuales, que permite a una sola etiqueta representar a un FEC.
- En una topología estable, la asignación de la etiqueta y distribución del overhead es más bajo que en el modelo de manejo de datos porque los caminos de etiquetas conmutadas están establecidos sólo después de un cambio de topología o la llegada del tráfico de control, y no con la llegada de cada flujo “nuevo” de tráfico.
- Cada paquete en un flujo es una etiqueta conmutada, no simplemente la cola del flujo en el modelo de manejo de datos

CONMUTACIÓN DE ETIQUETAS DE CISCO (TAG SWITCHING):

La solución desarrollada por Cisco para la conmutación de etiquetas fue bautizada como "Tag Switching". Esta solución, a diferencia de las comentadas anteriormente, se basa en el establecimiento de "caminos virtuales" entre los extremos de la red sin que existan flujos de datos que estimulen o dirijan el establecimiento de estos caminos virtuales; es decir, estos caminos son establecidos por necesidades de control de la red antes de que existan los flujos de datos que los utilicen.

Básicamente una red de conmutación de etiquetas consiste en un conjunto de routers frontera (Tag Edge Routers), encargados de añadir a la entrada y eliminar a la salida la información (tag) de enrutamiento interno, y un conjunto de routers internos, denominados Tag Switching Routers, encargados de conmutar y encaminar los flujo de datos basándose en la etiqueta o "tag" añadida a la entrada.

El esfuerzo de normalización que empezó Cisco con la conmutación de etiquetas culminó en el grupo de trabajo MPLS (Multiprotocol Label Switching) del IETF y hoy día MPLS se utiliza como un término genérico para referirse a la conmutación de etiquetas.

ARIS (AGREGATE ROUTE-BASED IP SWITCHING) DE IBM:

Otro de los gigantes de la industria, IBM, desarrolló su propia solución en el entorno de la conmutación de etiquetas. Esta solución conocida como ARIS es conceptualmente similar a la solución de Cisco anteriormente descrita. En este caso, los caminos, y por tanto las etiquetas asociadas, son establecidos como respuesta a las acciones de control del tráfico. Los routers que soportan esta tecnología son conocidos como "Integrated Switch Routers" (ISR) en la terminología IBM.

La idea que subyacía a la hora de diseñar ARIS fue la utilización de ATM como nivel de enlace, por lo que los protocolos propios de ARIS son protocolos "peer-to-peer" o entre iguales, que se establecen entre los ISR implicados directamente a nivel IP y permiten establecer conexiones con los vecinos e intercambiar las correspondientes etiquetas asociadas a los distintos flujos de datos. Este mecanismo de distribución de etiquetas comienza en el extremo donde finaliza el flujo de datos en la red ARIS, también conocido como "egress router", y es propagado de forma ordenada hasta el ISR que comenzó el flujo.

3.2. ARQUITECTURA MPLS

3.2.1. CONCEPTOS BASICOS DE MPLS – DESCRIPCION GENERAL

La arquitectura se divide en dos componentes: El componente de envió (forwarding), también denominada Plano de Datos, y el componente de control (routing), también denominado Plano de Control.

El Plano de Datos emplea una base de datos de envió de etiquetas mantenida por la conmutación de etiquetas, para ejecutar el envió de paquetes de datos basándose en las etiquetas transportadas por los paquetes.

El plano de control es el responsable de la creación y el mantenimiento de la información de envió de etiquetas entre un grupo de switches de etiquetas interconectadas

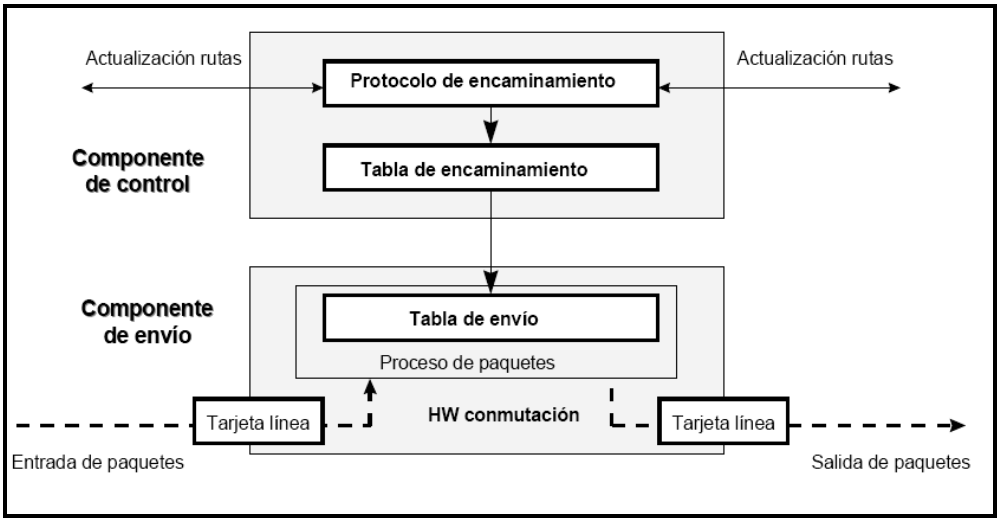


Figura 3.5. Componentes funcionales: Componente de control y Componente de reenvío

TIPOS DE NODOS MPLS:

Los dispositivos utilizados en MPLS son los routers de conmutación por etiquetas (Label Switching Router - LSR). Todo router o switch que implementa distribución de etiquetas y que pueda enviar paquetes basándose en etiquetas, entra en esta categoría.

Existen diferentes tipos de LSRs que se diferencian por la funcionalidad que proporcionan a la infraestructura de red. Estos diferentes tipos de LSRs son: LSR ATM, LSR ATM de contorno y LSR de frontera.

Un LSR ATM es un Switch ATM que puede actuar como un LSR. El mismo efectúa el enrutamiento IP y la asignación de etiquetas en el

plano de control y envía los paquetes de datos utilizando mecanismo de de conmutación de Celdas ATM adicionales en el plano de datos. En resumen la conmutación ATM de un Switch ATM se utiliza como tabla de envió de etiquetas de un nodo MPLS.

Los LSR ATM de frontera pueden recibir un paquete etiquetado o no etiquetado, segmentarlo en celdas ATM y enviar las celdas hacia el siguiente salto LSR ATM. Puede recibir celdas de un LSR ATM adyacente y, reensamblar estas celdas en el paquete original y después enviar el paquete como paquete etiquetado o no etiquetado.

Los LSRs de frontera son los encargados de realizar la imposición de etiquetas (push), y la determinación de etiquetas (pop) de los paquetes en la Red MPLS. La imposición de etiquetas es el acto de añadir una etiqueta o pila de etiquetas, a un paquete en el punto de entrada del dominio MPLS. La determinación de etiquetas es lo contrario, es decir, el acto de eliminar la etiqueta de un paquete en el punto de salida antes de que se envié a un vecino que esta fuera del dominio MPLS. Para poder realizar este trabajo estos LSRs deben implementar el componente de control y el componente de reenvío tanto del enrutamiento convencional como de la conmutación de etiquetas.

Si un paquete entra en la red, el router frontera utilizará el componente de reenvío de la conmutación de etiquetas para determinar la etiqueta que debe ponerle al paquete. Si el siguiente salto no es un LSR y el paquete no tiene etiqueta, entonces el LSR deberá reenviar el paquete usando el componente de reenvío del enrutamiento convencional.

Cuando el paquete va a salir de la red MPLS, el LSR que recibe el paquete le quitará la etiqueta y lo reenviará al siguiente salto usando el componente de reenvío del enrutamiento convencional. Dicho LSR sabrá que el paquete quiere abandonar la red simplemente porque el siguiente salto no es un LSR.

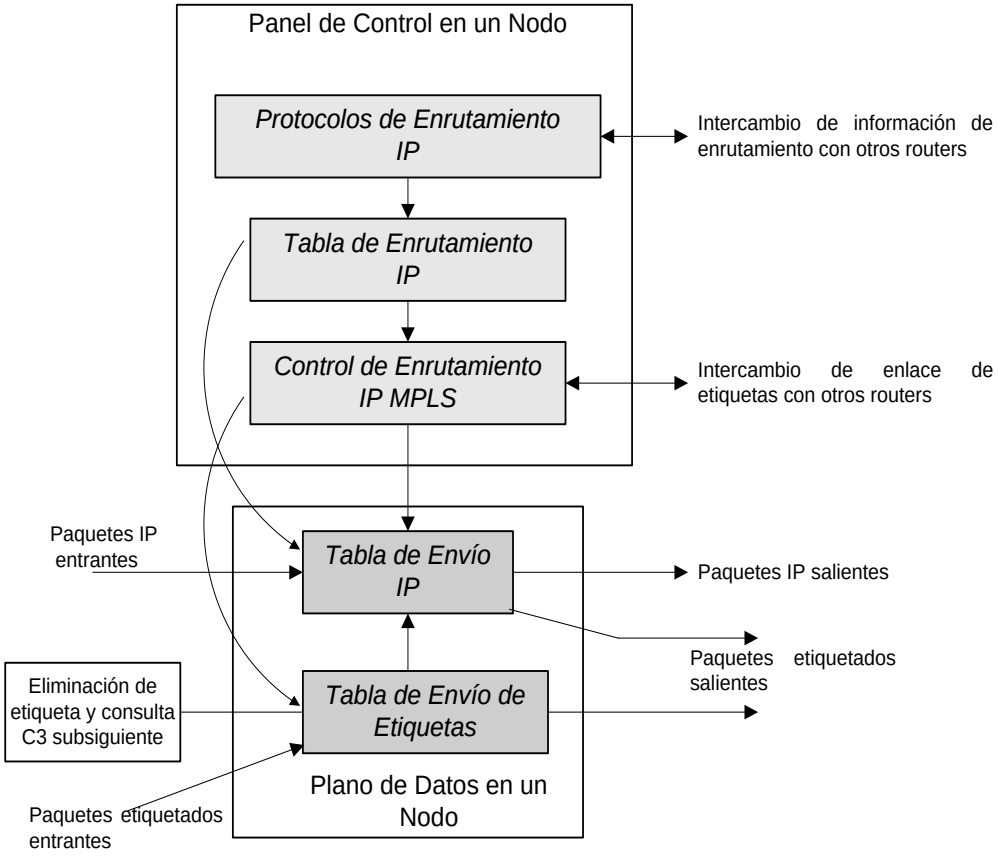


Figura 3.6. Arquitectura de un LSR de frontera

Los tipos de nodos MPLS son:

- LSR de entrada (ingress LSR): LSR que recibe tráfico de usuario (por ejemplo datagramas IP) y lo clasifica en su correspondiente FEC. Genera una cabecera MPLS asignándole una etiqueta y encapsula el paquete junto a la cabecera MPLS obteniendo una PDU MPLS (PDU = Protocol Data Unit o unidad de datos del protocolo).

- LSR de salida (egress LSR): LSR que realiza la operación inversa al de entrada, es decir, desencapsula el paquete removiendo la cabecera MPLS.
- LSR intermedio o interior: LSR que realiza el intercambio de etiquetas examinando exclusivamente la cabecera MPLS (obteniendo la etiqueta para poder realizar la búsqueda en la tabla de enrutamiento).

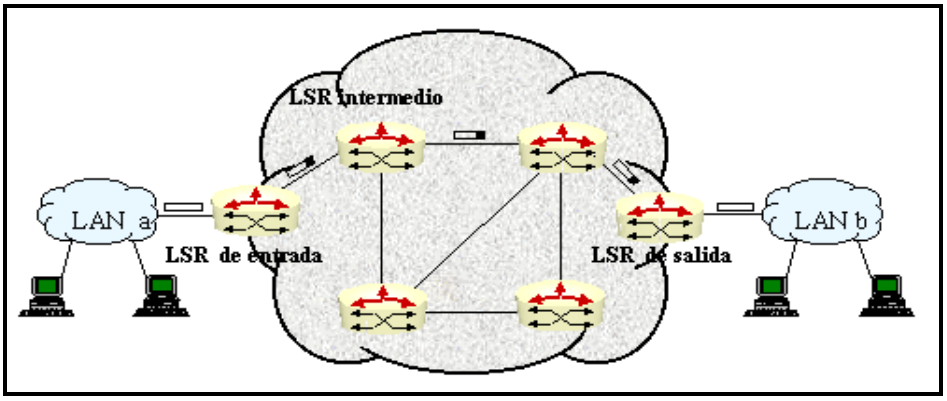


Figura 3.7. Tipos de nodos MPLS

3.2.2. ETIQUETAS

LA CLASE DE EQUIVALENCIA FUNCIONAL: FEC (FUNCTIONAL EQUIVALENCE CLASS)

La clase de equivalencia funcional se usa para describir una asociación de paquetes a una dirección destino, o lo que es lo mismo: Grupo de paquetes IP que se reenvían de la misma manera (ejemplo: Por el mismo camino, con el mismo tratamiento en el reenvío).

También se puede asociar el valor de la FEC a una dirección destino y a una clase de tráfico. La clase de tráfico esta asociada habitualmente a un número de puerto destino.

Uno de los motivos por los que se utiliza la FEC es porque permite agrupar paquetes en clases. Gracias a esta agrupación, el valor de la FEC en el paquete se puede utilizar para establecer prioridades, de tal forma que se da más prioridad a unos FECs sobre otros. Se pueden usar las FECs para dar soporte a operaciones eficientes de QoS (calidad de servicio). Por ejemplo, se pueden asociar FECs de alta prioridad a tráfico de voz en tiempo real, de baja prioridad a correo, etc.

MPLS, para establecer la relación entre una FEC y un paquete, usa la etiqueta. Dicha etiqueta identifica una FEC específica. Para diferentes clases de servicio se utilizarán diferentes FECs y sus etiquetas asociadas.

Una parte esencial de la tabla de enrutamiento mantenida por un router es la dirección del siguiente router. Un paquete perteneciente a una FEC asociado a una determinada entrada de la tabla se reenviará al siguiente router según esté especificado en dicha tabla.

Escalabilidad y grado de granulado:

Un aspecto importante de una FEC es su grado de granulado.

Si consideráramos una FEC en la que se incluyeran todos los paquetes en los que la dirección destino del nivel de red coincidiera con un determinado prefijo de dirección, tendríamos un granulado grueso. Como contrapartida, el sistema sería muy escalable. El inconveniente es que con un granulado grueso no podríamos diferenciar diferentes tipos de tráfico y por tanto no permitiría clases de tráfico ni operaciones de QoS.

En el otro extremo tendríamos el granulado fino, en la que una FEC podría incluir sólo los paquetes pertenecientes a una aplicación entre dos ordenadores, es decir, paquetes que tengan las mismas direcciones origen y destino, los mismos puertos e incluso la misma clase de servicio. En este caso tendremos más clasificaciones de tráfico, más FECs, más etiquetas y una tabla de enrutamiento más grande.

En consecuencia, una red de conmutación de etiquetas permite distintos grados de granulado de la FEC.

FUNCIONES DE CONTROL Y REENVÍO:

Podemos distinguir claramente dos componentes: El componente de control y el componente de reenvío.

El componente de control utiliza los protocolos estándar de enrutamiento, como OSPF y BGP. Utilizando estos protocolos los routers intercambian información de enrutamiento para construir y mantener las tablas de enrutamiento. Además el componente de control debe crear las asociaciones entre etiquetas y FECs y distribuir esta información.

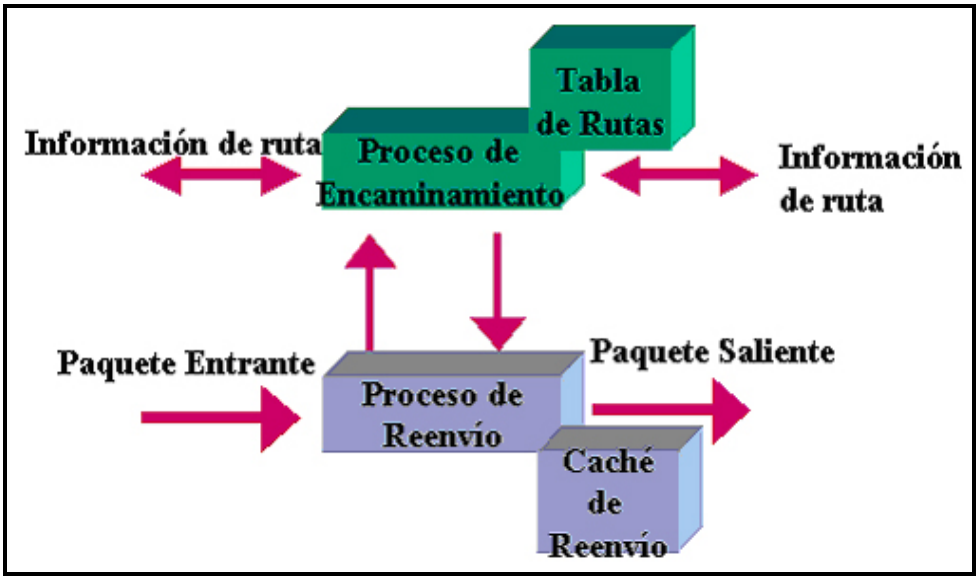


Figura 3.8. Funciones de reenvió y Enrutamiento

El componente de reenvío envía los paquetes desde la entrada hacia la salida. Para reenviar los paquetes, el componente de reenvío examina la información de la cabecera del paquete, busca en la tabla de enrutamiento la entrada correspondiente y reenvía el paquete. Por tanto, el componente de reenvío consiste en el conjunto de procedimientos que usa el router para tomar la decisión sobre el

reenvío de un paquete. Estos algoritmos definen la información del paquete que utiliza el router para encontrar una entrada en la tabla de enrutamiento, así como los procedimientos exactos que el router utiliza para encontrar la entrada.

Cada router de la red implementa ambos componentes. Podríamos ver el enrutamiento del nivel de red como una composición de ambos componentes (control y reenvío) implementada de una manera distribuida por el conjunto de routers que conforman la red.

La ventaja fundamental de separar ambos componentes es la posibilidad de modificar uno de ellos sin modificar el otro.

ALTERNATIVAS PARA EL TRANSPORTE DE LA ETIQUETA:

La decisión del reenvío se basa en uno o más campos del paquete.

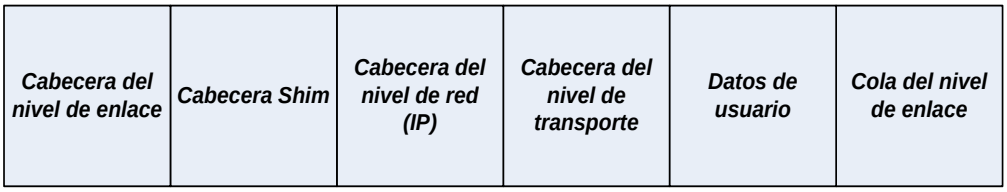


Figura 3.9. Inserción de Etiqueta genérica

El protocolo IP y los números de puerto se usan en la FEC y en las decisiones de reenvío. Estos campos identifican el tipo de tráfico que reside en la parte de datos del datagrama IP, por lo que son muy

importantes en redes que admiten diferentes servicios de QoS para diferentes tipos de tráfico.

ATM y Frame Relay (tecnologías del nivel de enlace) llevan la etiqueta en la cabecera del paquete. ATM puede llevar la etiqueta en el campo VCI o en el VPI de la cabecera, mientras que en Frame Relay estará en el campo DLCI de la cabecera. En DWDM la etiqueta puede asociarse con una longitud de onda en la fibra.

Si esta fuera la única opción, en tecnologías como ethernet que no disponen de un campo para poder llevar la etiqueta en la cabecera del nivel de enlace, no se podría emplear la conmutación de etiquetas. La solución a este problema consiste en transportar la etiqueta en un campo específico para la etiqueta, que se inserta entre la cabecera del nivel de enlace y la cabecera del nivel de red. Esta cabecera se denomina "cabecera shim" (algo así como cabecera de relleno). De este modo se permite cualquier tecnología o combinación de tecnologías del nivel de enlace. Ej: Conmutación de etiquetas en redes ethernet.

El hecho de llevar la etiqueta en el campo VCI de las celdas ATM permite que un conmutador ATM funcione como un LSR siempre que tenga el software de control apropiado.

La cabecera shim está situada en una posición donde la mayoría de los routers pueden procesarla por software, por lo que los routers convencionales pueden convertirse en LSRs siempre que tengan el software apropiado.

LA TABLA DE ENRUTAMIENTO

Una tabla de enrutamiento está constituida por múltiples entradas. Cada entrada consta de:

- Etiqueta de entrada
- Una o más subentradas:
    - Etiqueta de salida
    - Interfaz de salida
    - Dirección del siguiente salto

Etiqueta de entrada	***Etiqueta de salida Interfaz de salida Dirección del próximo salto***	***Etiqueta de salida Interfaz de salida Dirección del próximo salto***	***……***

Figura 3.10. Multiples Entradas de Tabla de Enrutamiento

Puede haber más de una subentrada, puesto que hay que tratar los paquetes de difusión. De esta forma se puede enviar un paquete por múltiples interfaces de salida. Puede existir una tabla de enrutamiento única o por interfaz, en cuyo caso a la hora de encaminar un paquete habrá que saber la interfaz por donde ha entrado el paquete.

La tabla está indexada por el valor de la etiqueta, de tal forma que la búsqueda en la tabla es inmediata. Necesitaremos un solo acceso a memoria, lo que se traduce en un acceso rápido.

La tabla o tablas de enrutamiento son mantenidas por el LSR.

ETIQUETAS LIBRES:

Un LSR mantiene un repositorio de etiquetas libres. Cuando inicia un LSR el repositorio contiene todas las etiquetas que el LSR puede usar para asociaciones locales. Cuando un LSR crea una asociación coge una etiqueta del repositorio y cuando la destruye la vuelve a depositar en el repositorio.

Si el LSR tiene una tabla de enrutamiento por interfaz, tendrá que tener un repositorio con etiquetas por interfaz.

ASOCIACIÓN DE ETIQUETAS A FECS

Asociación local y asociación remota.

- Asociación local: El router local establece la asociación entre la etiqueta y la FEC. Por tanto, la etiqueta pertenecerá al router.
- Asociación remota: Un router vecino será el que establezca la asociación, por lo que el router local recibirá la asociación de la etiqueta.

El componente de control usa ambos tipos de asociaciones para poblar su tabla de enrutamiento con etiquetas de entrada y salida.

Asociación de etiquetas Downstream:

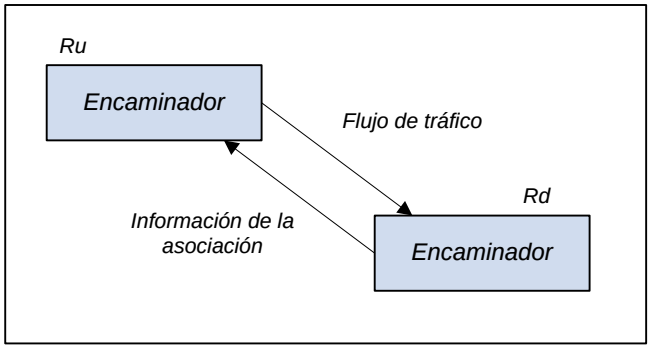


Figura 3.11. Asociación de Etiquetas Downstream

La asociación de la etiqueta a la FEC la realiza el router que está downstream (Rd) respecto al flujo de paquetes. Por tanto, en la tabla de enrutamiento de Ru tendremos como etiquetas de salida las etiquetas de la asociación remota (puesto que las ha elegido el router que está downstream) y como etiquetas de entrada las de la asociación local.

Ejemplo: Ru le manda un paquete a Rd. Este paquete habrá sido identificado con anterioridad como perteneciente a una FEC y tendrá una etiqueta (E) asociada a ese FEC. Por tanto Ru le habrá puesto al paquete como etiqueta de salida E.

Asociación de etiquetas Upstream:

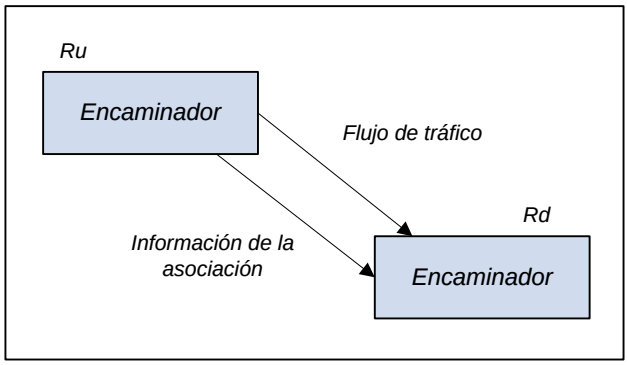


Figura 3.12. Asociación de Etiquetas Upstream

La asociación de la etiqueta a la FEC la realiza el router que está upstream (Ru) respecto al flujo de paquetes. Por tanto, en la tabla de enrutamiento de Ru tendremos como etiquetas de salida las etiquetas de la asociación local (puesto que es éste router el que las ha elegido) y como etiquetas de entrada las de la asociación remota. En MPLS sólo se utiliza la asociación de etiquetas upstream.

Asociación de etiquetas dirigida por control o por datos:

Un LSR crea o destruye asociaciones entre etiquetas y FECs en respuesta a un evento. Este evento puede deberse a que recibe información de control o a que debe reenviar paquetes.

La asociación de etiquetas a FECs dirigida por control se establece de antemano. La asociación de etiquetas a FECs dirigida por los datos

ocurre dinámicamente, a medida que fluyen los paquetes. Normalmente, ambos tipos de asociaciones se usan conjuntamente.

LABEL SWAPPING: INTERCAMBIO DE ETIQUETAS

El algoritmo empleado por el componente de reenvío se basa en el intercambio de etiquetas. Cuando un LSR recibe un paquete extrae el valor de la etiqueta y accede con él a la tabla de enrutamiento. En dicha tabla de enrutamiento encontrará el nuevo valor de la etiqueta que ha de ponerle al paquete antes de reenviarlo, así como la interfaz de salida por donde ha de mandarlo. También podrá encontrar información sobre si debe o no encolar el mensaje.

El algoritmo de reenvío se suele implementar en hardware por su sencillez. Esto repercute favorablemente en el rendimiento del LSR.

Veamos un ejemplo:

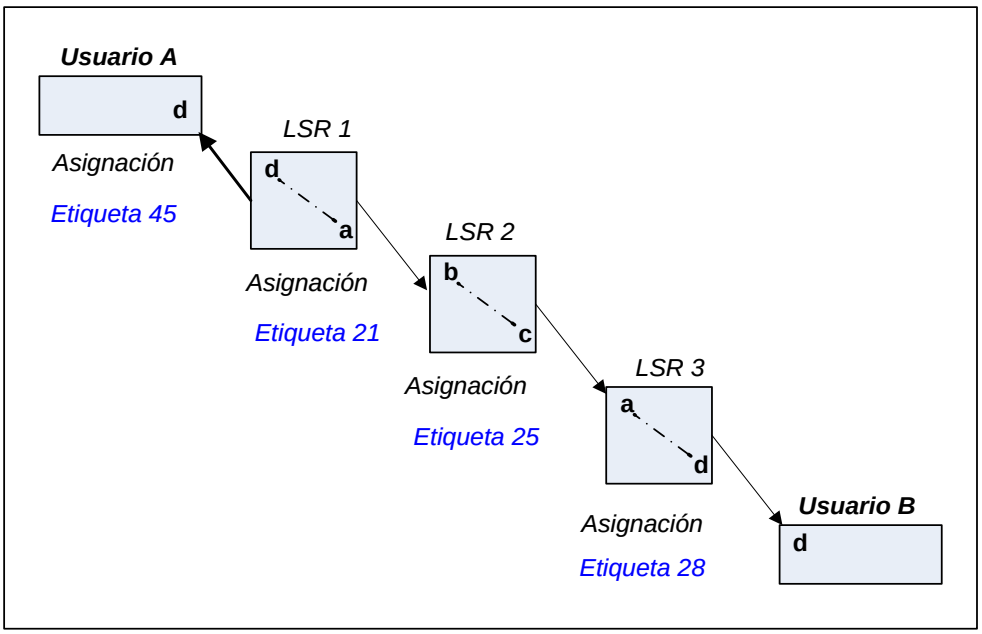


Figura 3.13. Intercambio de Etiquetas

- La etiqueta 45 identifica el LSP entre el usuario A y el LSR 1.
- La etiqueta 21 identifica el LSP entre el LSR 1 y el LSR 2.
- La etiqueta 25 identifica el LSP entre el LSR 2 y el LSR 3.
- La etiqueta 28 identifica el LSP entre el LSR 3 y el usuario B.

FORMATO DE LAS ETIQUETAS:

Una etiqueta MPLS tiene 32 bits. Se sitúa entre la cabecera de nivel 2 y la de nivel 3.

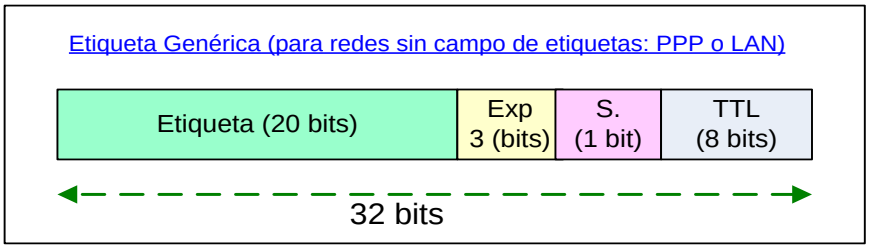


Figura 3.14. Formato de Etiquetas

- Etiqueta: Valor de la etiqueta
- Exp: Uso experimental. No está definido totalmente. Algunos artículos sobre servicios diferenciados (DiffServ) discuten su uso.
- S: Bit de apilamiento (Stacking bit). Se usa para apilar etiquetas.
- TTL: Tiempo de vida (Time To Live). Número de nodos (saltos) que puede atravesar el paquete MPLS. Se necesita porque los LSRs intermedios no analizan el campo IP TTL.

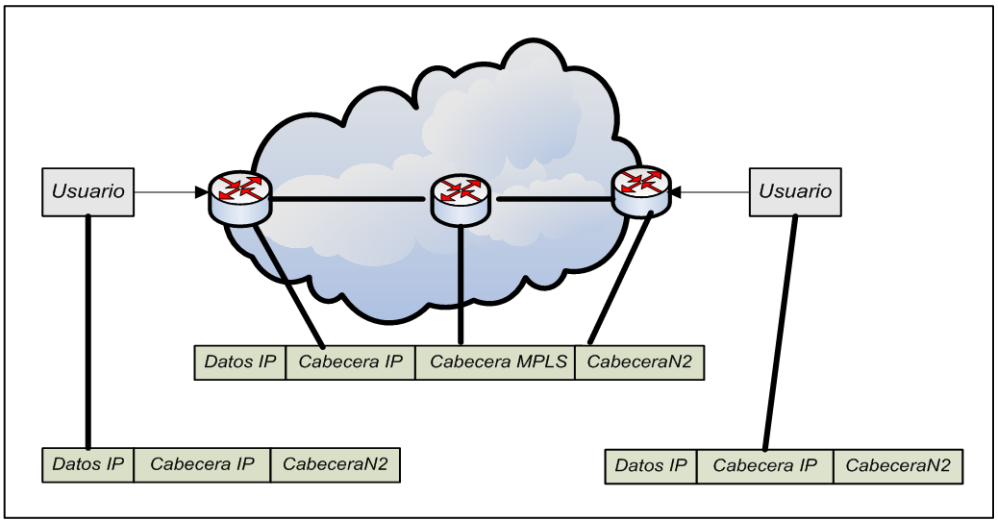


Figura 3.15. Etiquetado MPLS en el Backbone

LA PILA DE ETIQUETAS:

En MPLS un paquete puede tener más de una etiqueta, organizadas éstas a modo de pila (FIFO). A esto se le conoce como pila de etiquetas.

Aunque MPLS soporte una jerarquía gracias a la pila de etiquetas, el procesamiento de un paquete etiquetado es completamente independiente del nivel de la jerarquía. Siempre que se procese una etiqueta, ésta será la de la cima, sin importar cuántas etiquetas pueda haber debajo.

Se puede considerar a un paquete no etiquetado como un paquete con una pila de etiquetas vacía.

Si la profundidad de la pila de etiquetas de un paquete es m, a la etiqueta que está al fondo de la pila se le llama etiqueta de nivel 1, a la que está encima etiqueta de nivel 2, y así sucesivamente.

En la figura 3.16 tenemos tres dominios. Supongamos que el dominio 2 es un dominio de tránsito. En dicho dominio no se originan paquetes. Tampoco hay paquetes destinados a él. Para anunciar las direcciones del dominio 3 el LSR F le distribuye la información al LSR E. El LSR E le distribuye la información al LSR B y este al LSR A. No se distribuye la información a los LSRs C y D porque son LSRs interiores.

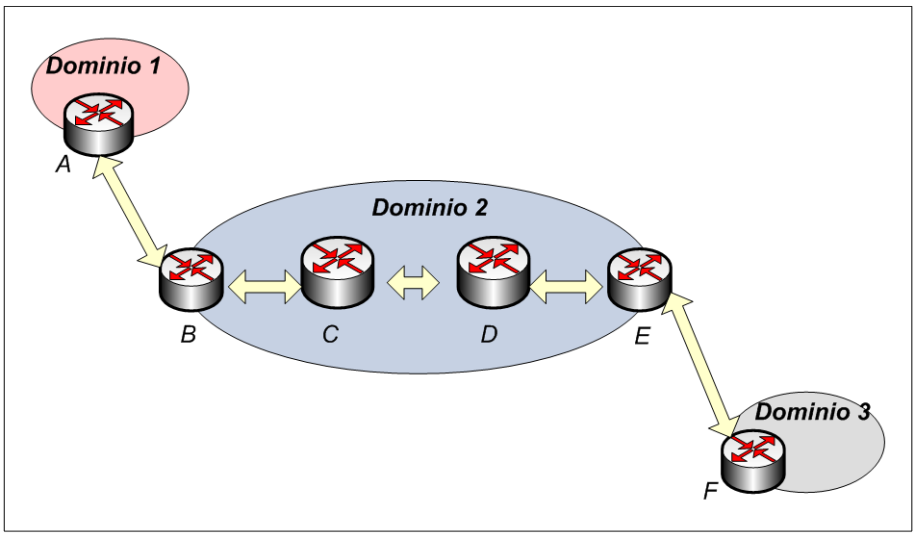


Figura 3.16. Distribución de Etiquetas en dominios

Se usan dos niveles de etiquetas. Cuando el tráfico entra en el segundo dominio se apila una nueva etiqueta en la cima de la pila, por lo que las etiquetas que hubiera en la pila descienden un nivel.

CAMINO DE CONMUTACIÓN DE ETIQUETAS (LSP): REGLAS DE APILAMIENTO

Un LSP de nivel m para un paquete P es una secuencia de ROUTERS <R1,...,Rn> con las siguientes propiedades:

1. R1, el LSR de entrada, es un LSR que apila una etiqueta en la pila de etiquetas de P, resultando una pila de etiquetas de profundidad m.
2. Para todo i, 1<i<n, P tendrá una pila de etiquetas de profundidad m cuando lo reciba el LSR Ri.

3. Mientras P se encuentre entre R1 y Rn-1 su pila de etiquetas nunca tendrá una profundidad menor que m.
4. Para toda i, 1<i<n: P es transmitido desde Ri hasta Ri+1 por medio de MPLS, por ejemplo usando la etiqueta de la cima de la pila como índice de una ILM (Incoming Label Map).
5. Para todo i, 1<i<n: Si un sistema S recibe y reenvía P después de que P sea transmitido por Ri pero antes de que P sea recibido por Ri+1 (por ejemplo, Ri y Ri+1 pueden estar conectados vía una subred conmutada de enlace de datos, y S puede ser un conmutador de enlace de datos), entonces la decisión del reenvío de S no está basado en la etiqueta de nivel m, o en la cabecera del nivel de red. Esto puede ser debido a que:
    - La decisión no se basa en absoluto en la pila de etiquetas o en la cabecera del nivel de red.
    - La decisión se basa en una pila de etiquetas en la que se han apilado etiquetas adicionales (ejemplo: En un nivel de etiquetas m+k con k>0).

En resumen, cuando un LSR etiqueta un paquete que anteriormente fue etiquetado, la nueva etiqueta corresponde a una FEC cuyo LSR de salida es el LSR que asignó la etiqueta que ahora está en la segunda posición en la pila.

Consideremos el conjunto de nodos que pudieran ser el LSP de entrada para una FEC F. Entonces hay un LSP para la FEC F que empieza con cada uno de esos nodos. Si alguno de esos LSPs tiene el mismo LSP de salida, entonces podríamos considerar que el conjunto de esos LSPs forma un árbol, cuya raíz es el LSP de salida. Podríamos entonces hablar de un árbol LSP para una FEC F.

Extracción en el Penúltimo Salto:

Si <R1,..., Rn> es un LSP de nivel m para el paquete P, P puede ser transmitido desde Rn-1 a Rn con una pila de etiquetas de profundidad m-1. Se puede extraer de la pila de etiquetas en el penúltimo LSR del LSP, en vez de en el LSP de salida.

Desde una perspectiva arquitectónica, esto es apropiado. El propósito de la etiqueta de nivel m es hacer llegar el paquete a Rn. Una vez que Rn-1 ha decidido mandar el paquete a Rn, la etiqueta no tiene ninguna funcionalidad y por tanto no es necesario transportarla.

La extracción en el penúltimo salto tiene una ventaja: Si no se hace, cuando el LSP de salida reciba el paquete, éste mirará la etiqueta de la cima de la pila y determinará que es el LSP de salida. Entonces deberá hacer una extracción de la pila y examinar lo que quede del paquete. Si hubiera otra etiqueta en la pila, el LSP de salida miraría

esta etiqueta y reenviaría el paquete basándose en la información que ha obtenido. (En este caso, el LSP de salida para el paquete del LSP de nivel m es también un nodo intermedio para un LSP de nivel m-1). Si no hubiera etiquetas en la pila, entonces se reenviaría el paquete utilizando la dirección de destino del nivel de red. Esto obliga a que el LSR de salida haga dos consultas: Bien dos consultas de etiquetas o una consulta de etiqueta seguida de una consulta de dirección.

Con esta técnica, el LSR de salida sólo tiene que hacer una consulta y requiere que el penúltimo nodo haga una consulta.

La creación del "camino rápido" del reenvío en un producto de conmutación de etiquetas puede ser muy favorecedor si se sabe que sólo requerirá una consulta:

- Se puede simplificar el código si se asume que sólo se necesitará una consulta.
- Se puede basar el código en un "presupuesto de tiempo" que asuma que sólo se necesitará una consulta.

De hecho, cuando se usa la extracción en el penúltimo salto, el LSP de salida puede incluso no ser un LSR.

No obstante, algunos motores hardware de conmutación pueden no ser capaces de extraer de la pila de etiquetas, por lo que esto no puede ser requerido universalmente.

También puede haber situaciones en las que no es deseable la extracción en el penúltimo salto. Por tanto, el penúltimo nodo extraerá la etiqueta de la pila de etiquetas si el LSR de salida se lo pide explícitamente, o si el siguiente nodo en el LSP no soporta MPLS. (Si el siguiente nodo en el LSP no soporta MPLS, y no hace tal petición, el penúltimo nodo no tendrá manera de saber que es el penúltimo nodo).

Un LSR que es capaz de extraer de la pila de etiquetas deberá realizar la extracción en el penúltimo salto cuando se lo pida el LSR del mismo nivel (su "igual" o peer) que está downstream.

Las negociaciones iniciales del protocolo de distribución de etiquetas deben permitir a cada LSR determinar si sus LSRs vecinos son capaces de extraer de la pila de etiquetas. Un LSR no le debe pedir a su "igual" de distribución de etiquetas que extraiga de la pila de etiquetas a no ser que sea capaz de hacerlo.

Un nodo de salida siempre podrá interpretar la etiqueta de la cima de un paquete recibido cuando se utiliza la extracción en el penúltimo

salto si se cumplen las reglas de alcance y unicidad expuestas en el apartado anterior.

Ejemplo: Doble consulta en el LSR F

En la figura 3.17 se puede apreciar que el LSR F realiza una doble consulta, lo que repercute en el rendimiento de dicho nodo. Para mejorar el rendimiento se usa la extracción en el penúltimo salto.

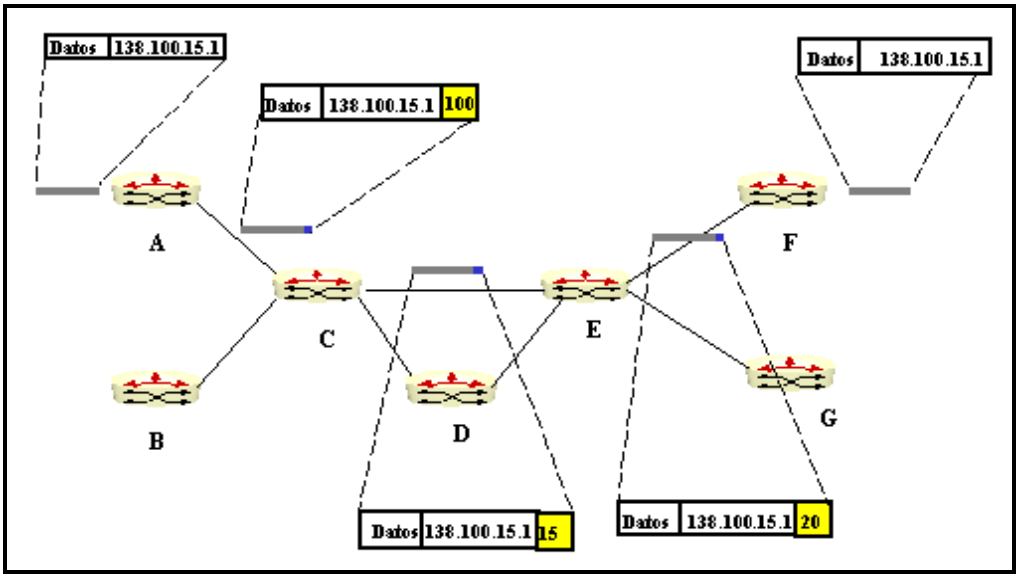


Figura 3.17. LSR realizando una doble consulta

Pasos:

- Primero: Llega un paquete IP al router A.
- Segundo: El router etiqueta el paquete y se lo reenvía al router C.
- Tercero: El router C realiza una búsqueda en la tabla, intercambia la etiqueta y reenvía el paquete al router E.

- Cuarto: El router E realiza una búsqueda en la tabla, intercambia la etiqueta y reenvía el paquete la router F.
- Quinto: El router F realiza una búsqueda en la tabla, extrae la etiqueta, realiza una búsqueda de nivel 3 y reenvía el paquete hacia un router externo.

Ejemplo: Extracción en el penúltimo salto

En la figura 3.18 podemos apreciar que el LSR F realiza una consulta menos que en el caso anterior.

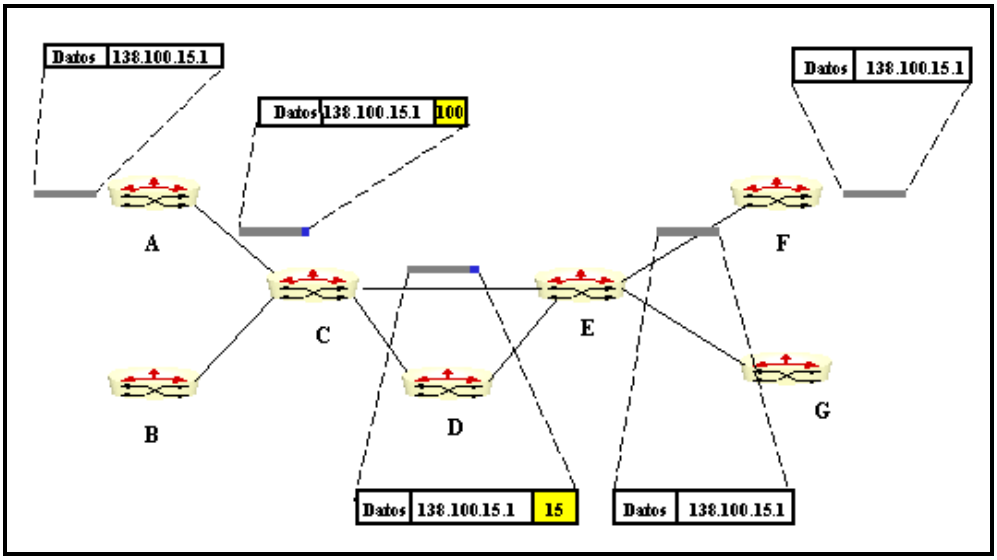


Figura 3.18. Extracción en el penúltimo salto

Pasos

- Primero: Llega un paquete IP al router A.
- Segundo: El router etiqueta el paquete y se lo reenvía al router C.

- Tercero: El router C realiza una búsqueda en la tabla, intercambia la etiqueta y reenvía el paquete al router E.
- Cuarto: El router E realiza una búsqueda en la tabla, extrae la etiqueta y reenvía un paquete IP puro al router F.
- Quinto: El router F realiza únicamente una búsqueda de nivel 3 y reenvía el paquete hacia un router externo.

Ejemplo: LSPs jerárquicos

Ocurre cuando se crea un nuevo LSP dentro de un túnel de un LSP de orden superior. En el siguiente ejemplo se muestra cómo los LSPs de orden inferior disparan la formación de un LSP de orden superior. Los nodos en el borde de dos regiones con respecto a las características de multiplexado, son los responsables de la agregación de los LSPs.

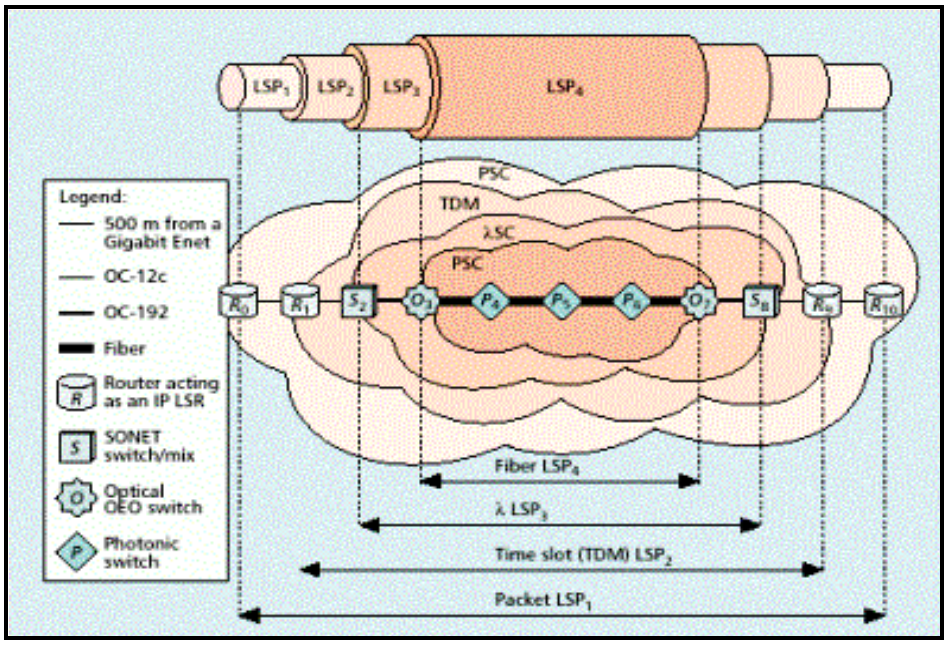


Figura 3.19. LSPs Jerárquicos

- R0, R1, R9 y R10 manejan paquetes.
- S0 y S8 son conmutadores SONET/SDH.
- O3 y O7 son conmutadores electro-ópticos.
- P4, P5 y P6 son conmutadores ópticos.
- Entre R0-R1 y R9-R10 hay enlaces de 500 Mbps.
- Entre R1-S2 y S8-R9 hay un enlace de OC-12 (mayor capacidad que el anterior).
- Entre S2-O3 y O7-S8 hay un enlace de OC-192 (mayor capacidad que el anterior).
- Entre O3-O7 hay un enlace de fibra.
- LSP1 está configurado de R0 a R10 con ancho de banda de 500 Mbps.
- LSP1 está anidado dentro de LSP2, 3, 4 que son LSPs de orden superior.
    - Los nodos en el borde de dos regiones con respecto a las características de multiplexado, son responsables de la formación de LSPs de orden superior o de agregar los LSPs de nivel inferior.

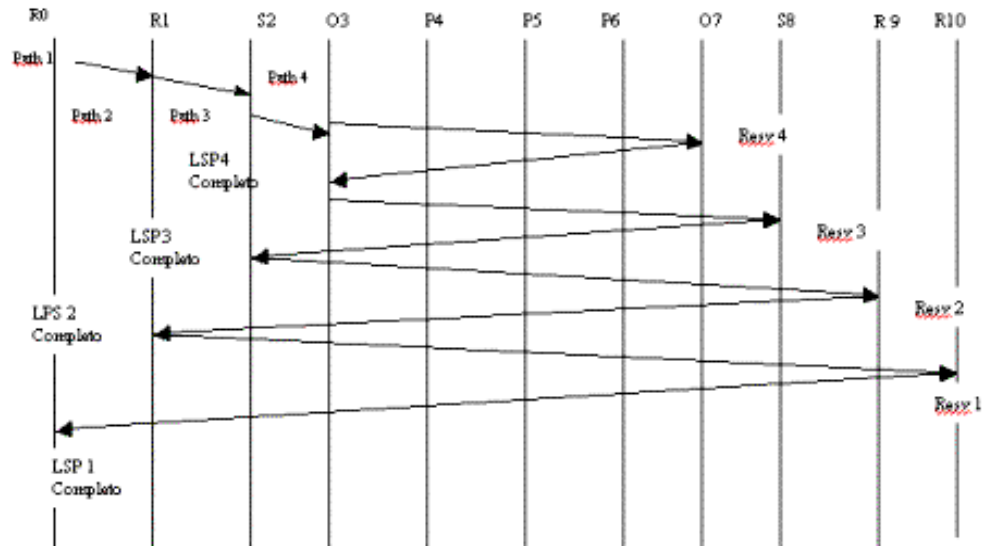


Figura 3.20. Proceso de formación del LSP

La formación del LSP1 dispara la formación de los LSPs 2, 3 y 4. R0 manda una petición de camino (Path) a R1. La llegada de dicha petición a R1 dispara la formación del LSP1 de R1 a R9 y así sucesivamente hasta que se dispare la formación del LSP4 en O3. Una vez establecido el LSP4, el mensaje tercero de Path se manda a través del LSP4 (o sea, por el túnel). Este proceso continua hasta que se cree el primer LSP y se forme la jerarquía.

CONTROL DE ETIQUETAS INDEPENDIENTE Y ORDENADO:

Antes de continuar conviene aclarar lo que es un prefijo de dirección. En vez de utilizar la máscara de subred se puede utilizar un valor llamado valor de prefijo. El valor de prefijo describe cuántos

bits se deben usar como máscara. Ejemplo: La dirección IP 138.100.15.1/24

El número 24 es el valor prefijo e indica que la máscara de subred son 24 bits, dejando los restantes 8 bits para identificar a los hosts.

En MPLS existen dos formas para asignar etiquetas a FECs: Independiente y ordenado.

Control Independiente

Cuando un LSR reconoce una FEC realizará una asociación de forma independiente de una etiqueta a esa FEC. Una vez hecho esto informará de dicha asociación a los LSRs vecinos.

Esta es la forma de trabajar en el enrutamiento IP convencional: Cada nodo encamina los paquetes de forma independiente, apoyándose en que el algoritmo de enrutamiento converge rápidamente garantizando de esta forma que los datagramas son entregados de forma correcta.
Ejemplo:

1. Figura 3.21: El LSR A utiliza OSPF para informarle al LSR C el prefijo de dirección 192.165/16
2. Figura 3.22: Cuando C recibe el prefijo, asigna de forma independiente una etiqueta a esta FEC e informa de dicha asociación a los LSRs vecinos.

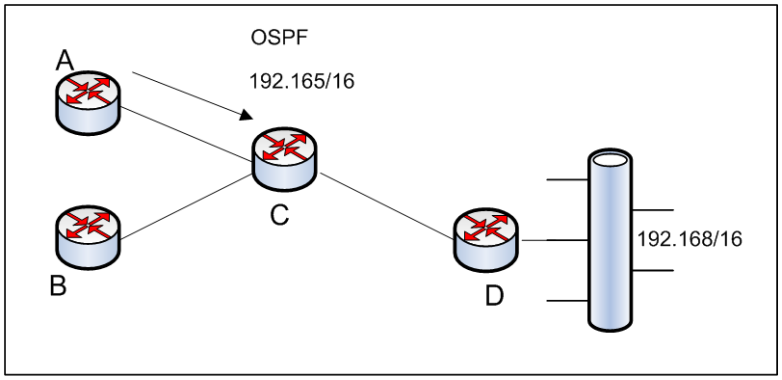


Figura 3.21. Control Independiente: Informa el prefijo al LSR

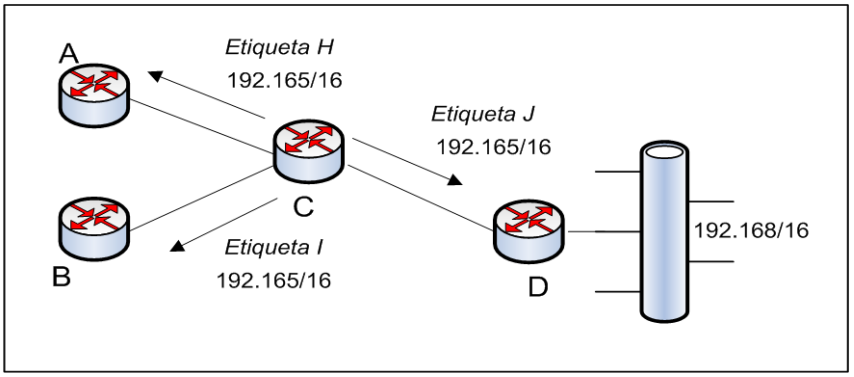


Figura 3.22. Control Independiente: Asignación de etiquetas FEC a los vecinos LSR

Control Ordenado

La asignación de etiquetas ocurre de forma ordenada desde un extremo del LSP hacia el otro. El establecimiento del LSP puede iniciarse por el LSR de entrada o por el LSR de salida del LSP.

Ejemplo: Supongamos que el establecimiento del LSP lo inicia el LSR de salida.

1. Figura 3.23: El nodo D se da cuenta que es el LSR de salida para el prefijo de dirección 192.168/16. Dicho nodo asigna una etiqueta a esta FEC e informa de dicha asociación a su vecino.
2. Figura 3.24: Cuando el LSR C recibe dicha información, asigna una etiqueta e informa de dicha asociación a sus LSRs vecinos. De esta forma, el establecimiento del LSP se hace de forma ordenada desde el LSR de salida al LSR de entrada.

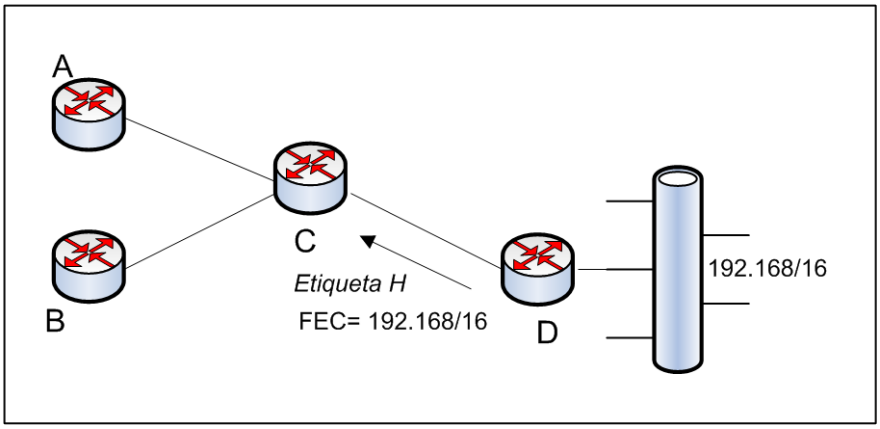


Figura 3.23. Control Ordenado: Asignación de etiquetas a FEC

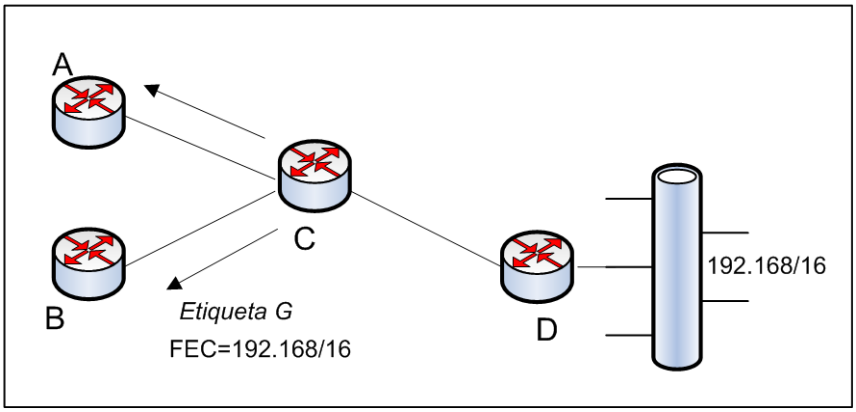


Figura 3.24. Control Ordenado: Asignación de etiquetas a vecinos

Si se pretende garantizar que el tráfico de una FEC particular sigue un camino que tiene una serie de propiedades, se debe usar el control ordenado.

MPLS permite tanto el control independiente como el control ordenado. Un LSR sólo necesita implementar uno u otro.

Un inconveniente del control independiente ocurre cuando dos vecinos no están de acuerdo en las FECs que van a usar. Cuando esto ocurre algunas FECs no tendrán LSPs asociadas a ellas.

El control ordenado facilita la prevención de bucles. También permite a los administradores de la red controlar cómo se establecen los LSPs. Un inconveniente es que se tarda más tiempo en establecer un LSP que con el control independiente, debido a que las asociaciones deben propagarse a través de una región entera antes de que se establezca el LSP.

Si se quiere que el control ordenado sea efectivo, se deberá implementar en todos los LSRs.

3.3. PROTOCOLOS DE DISTRIBUCION DE ETIQUETAS

Un protocolo de distribución de etiquetas es un conjunto de procedimientos por los que un LSR le informa a otro de las asociaciones de etiquetas a FECs que ha hecho.

A dos LSRs que utilizan un protocolo de distribución de etiquetas para intercambiar información de asociaciones de etiquetas a FECs se les conoce como un par de distribución de etiquetas (Label distribution peers) respecto a la información de las asociaciones que intercambian.

MPLS no asume que haya sólo un protocolo de distribución de etiquetas. De hecho, se están normalizando distintos protocolos de distribución de etiquetas. También se están definiendo nuevos protocolos como el LDP (Label Distribution Protocol).

3.3.1. LDP

El protocolo de distribución de etiquetas LDP (Label Distribution Protocol) se ejecuta sobre TCP y, por tanto, es un protocolo de estado duro. Dado que se ejecuta sobre TCP, éste le proveerá de fiabilidad en el envío de mensajes. Posteriormente se verá que la única excepción la encontramos en los mensajes de anuncio que se ejecutan sobre UDP.

La definición según [RFC3036] es la siguiente: El protocolo de distribución de etiquetas es el conjunto de procedimientos mediante los cuales un LSR se comunica con otro para notificarle el significado de las etiquetas para reenviar el tráfico entre ellos.

El uso más sencillo de LDP consiste en establecer enlaces unitarios de LSPs. Para hacer esto se puede usar la distribución de etiquetas downstream no solicitado o downstream por demanda y es compatible con el control ordenado y con el control independiente. Se podrá usar el modo de retención de etiquetas conservador o el liberal. Pero habrá combinaciones no factibles. Veámoslo con un par de ejemplos:

- Si los LSRs vecinos utilizan la distribución de etiquetas downstream no solicitado y el LSR local utiliza el modo conservador de retención de etiquetas, habrá mucho tráfico de liberación de etiquetas.
- Si los LSRs vecinos utilizan la distribución de etiquetas downstream por demanda y el LSR local utiliza el modo liberal de retención de etiquetas habrá mucho tráfico de petición de etiquetas.

LDP es un protocolo muy útil para los casos en los que se desea establecer un LSP a través de LSRs que no soporten piggybacking (básicamente esta es la única ventaja de LDP). LDP es bidireccional y podrá operar entre LSRs adyacentes o no adyacentes.

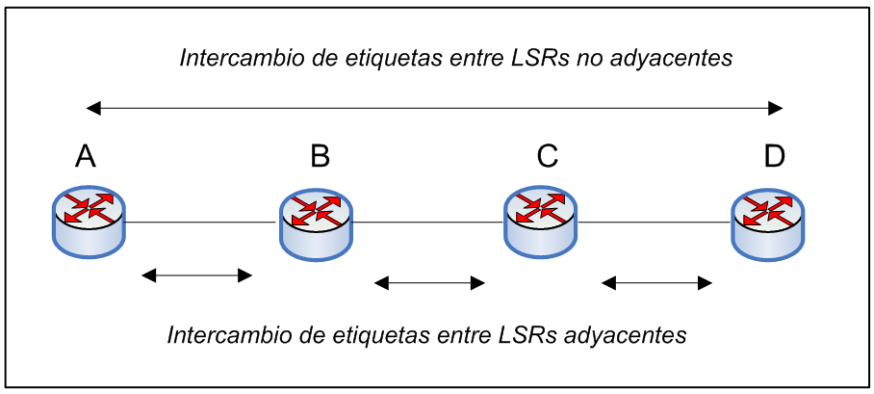


Figura 3.25. Intercambio de Etiquetas entre LSR

El protocolo de distribución de etiquetas asocia una FEC con cada LSP que crea. Dos LDPs serán pares LDP (LDP peers) cuando ambos LSRs intercambien información de asociaciones de etiquetas y FECs. Para intercambiar dicha información establecerán una sesión LDP.

Mensajes LDP

Los pares LDP se podrán intercambiar cuatro clases de mensajes:

1. Mensajes de descubrimiento (discovery messages): Se usan para anunciar y mantener la presencia de un LSR en la red. Un LSR mandará periódicamente por la red mensajes HELLO a través de un puerto UDP con la dirección multicast "todos los routers de esta subred".
2. Mensajes de sesión: Se utilizan para establecer, mantener y terminar sesiones entre pares LDP. Cuando un LSR descubre a

otro por medio de mensajes HELLO utilizará un procedimiento de iniciación LDP por medio de TCP.

3. Mensajes de anuncio (advertisement messages): Se usan para crear, modificar y eliminar asociaciones de etiquetas a FECs. Se transportan vía TCP. Cuando se haya establecido la asociación los pares LDP podrán intercambiarse este tipo de mensajes.
4. Mensajes de notificación: Los mensajes de notificación también se transportan vía TCP. Hay dos tipos de mensajes de notificación: Notificaciones de error y notificaciones de aviso. El primer tipo se utiliza para notificar errores fatales, en cuyo caso terminará la sesión y se descartarán todas las asociaciones de etiquetas aprendidas en dicha sesión. El segundo tipo se utiliza para pasarle a un LSR información de la sesión LDP o el estado de algún mensaje anterior.

FECs e Identificadores

Una FEC identificará a un conjunto de paquetes IP que podrán ser enviados a través de un LSP. LDP define dos tipos de FECs:

- Prefijo de dirección
- Dirección de host

Habrá una correspondencia entre una dirección particular y un prefijo de dirección si la dirección comienza con el prefijo. Habrá una correspondencia entre un paquete y un LSP si existe una correspondencia entre el prefijo de dirección del LSP y la dirección de destino del paquete.

El procedimiento para correlacionar un paquete a un LSP está formado por una serie de reglas. Estas reglas se aplicarán hasta que el paquete pueda ser correlacionado a un LSP. Las reglas son:

- Si hay exactamente un LSP con un elemento FEC de dirección host con la misma dirección destino que el paquete, entonces el paquete se correlacionará con ese LSP.
- Si hay varios LSPs, cada uno con un elemento FEC de dirección host idéntica a la dirección destino del paquete, entonces el paquete se correlacionará con uno de esos LSPs.
- Si hay una única equivalencia entre un paquete y un LSP, entonces el paquete se correlacionará con ese LSP.
- Si hay múltiples equivalencias entre un paquete y varios LSPs, entonces el paquete se correlacionará con el LSP que tenga mayor porcentaje de igualdad en el prefijo (es decir, el más largo).

- Si un paquete debe atravesar un router frontera, y existe un LSP con un elemento FEC de prefijo de dirección que es una dirección de ese router, entonces el paquete se correlacionará con ese LSP.

Identificadores LDP

Un identificador LDP se utiliza para identificar el espacio de etiquetas de un LSR. Se compone de seis octetos, los cuatro primeros identifican al LSR y los dos últimos identifican el espacio de etiquetas de dicho LSR. El espacio de etiquetas puede ser por interfaz o por plataforma. Si los dos últimos octetos tienen un valor de cero el espacio de etiquetas será por plataforma.

La especificación de LDP utiliza la siguiente nomenclatura para representar un identificador LDP:

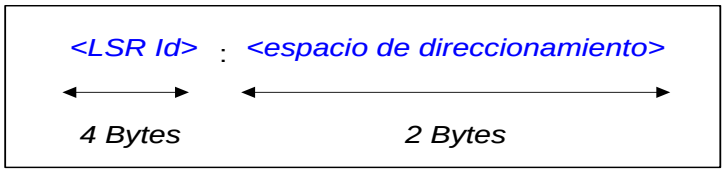


Figura 3.26. Representación de identificadores LDP

Sesión LDP

Cuando un LSR utiliza LDP para anunciar más de un espacio de etiquetas a otro LSR, utilizará diferentes sesiones LDP para cada

espacio de etiquetas. Como se comentó anteriormente, LDP utiliza TCP. Cuando dos LSRs requieren múltiples sesiones LDP, se establecerán sesiones TCP distintas para cada sesión LDP.

En la especificación del protocolo se definen dos fases para el establecimiento de la sesión LDP:

- Descubrimiento
- Establecimiento y mantenimiento de sesiones LDP

Descubrimiento

El protocolo de descubrimiento de LDP utiliza UDP como protocolo de transporte. Existen dos modalidades de descubrimiento: Básica y extendida.

En la modalidad básica el LSR envía periódicamente mensajes HELLO a un puerto bien conocido con la dirección multicast "todos los routers de esta red". Los routers están escuchando continuamente en este puerto a la espera de recibir mensajes HELLO. Por tanto, llegará un momento en el que el LSR conocerá todos los LSRs con los que tiene una conexión directa. Por tanto este mecanismo se utiliza si los LSRs están conectados directamente por medio de un enlace.

Los mensajes HELLO transportarán el identificador LDP con el espacio de etiquetas que LSR pretende usar en esa interfaz, además de otro tipo de información.

Con la modalidad extendida se permite que dos LSRs que no están conectados directamente establezcan una sesión LDP. Con esta modalidad, un LSR emite periódicamente mensajes HELLO a un puerto (UDP) bien conocido y con una dirección específica, que habrá aprendido de algún modo (por ejemplo, por configuración). Los mensajes HELLO transportarán el identificador LDP con el espacio de etiquetas que LSR pretende usar, además de otro tipo de información. El LSR al que se le están enviando los mensajes HELLO podrá responder o ignorar dicho mensaje. Si decide responder a dicho mensaje deberá mandar periódicamente mensajes HELLO al LSR que inició el proceso.

La modalidad extendida es útil cuando se ha configurado un LSP entre dos LSRs por ingeniería de tráfico, deseando mandar paquetes anteriormente etiquetados a través de ese LSP. El LSR situado al principio del LSP necesitará saber como etiquetar los paquetes que le enviará la LSR situado al final del LSP.

Establecimiento y mantenimiento de sesiones LDP

Una vez conocidos los vecinos se podrá establecer la sesión. Cada uno de los LSRs implicados puede jugar un papel activo o pasivo. El establecimiento de una sesión consta de dos fases:

Establecimiento de la Conexión de Transporte

Esta fase consiste en el establecimiento de una conexión TCP entre los LSRs implicados, para una nueva sesión LDP.

Inicio de la Sesión

Una vez establecida la conexión TCP los LSRs deben negociar los parámetros de la sesión. Esto se hace intercambiando mensajes de iniciación. Estos parámetros incluyen la versión del protocolo LDP, el método de distribución de etiquetas, valor de los temporizadores, etc.

Si el LSRa juega el papel activo, éste iniciará la negociación de los parámetros de la sesión enviando un mensaje de iniciación al LSRb. Este mensaje contendrá tanto el identificador LDP del LSRa como el identificador del LSRb.

Cuando un LSR recibe un mensaje de iniciación, mirará dicho mensaje para determinar si los parámetros son aceptables. Si lo son, responderá con su propio mensaje de iniciación proponiendo los parámetros que desea usar y un mensaje de mantenimiento

(KeepAlive) para notificar al otro LSR que acepta los parámetros. Si los parámetros no son aceptables, responderá con un mensaje de notificación de error de parámetros rechazados.

Máquina de estado de la Negociación de la Sesión LDP

A continuación se muestra la Tabla 3.1de transición, y el diagrama de transición de estado de inicialización de la sesión.

ESTADO	EVENTO	NUEVO ESTADO
No Existente	Conexión TCP de sesión establecida	Inicializado
Inicializado	Transmitir mensaje de inicio(papel activo)	Opensent
Inicializado	Recibir mensaje de inicio aceptable (papel pasivo). Acción: Transmitir mensajes de inicio y mantenimiento.	Openrec
Inicializado	Recibir cualquier otro mensaje LDP. Acción: Transmitir mensaje de notificación de error (NAK) y cerrar la conexión de transporte	No Existente
Openrec	Recibir mensaje de mantenimiento	Operacional
Openrec	Recibir cualquier otro mensaje LDP. Acción: Transmitir mensaje de notificación de error (NAK) y cerrar la conexión de transporte.	No Existente
Opensent	Recibir un mensaje de iniciación aceptable. Acción: Transmitir un mensaje de mantenimiento.	Openrec
Opensent	Recibir cualquier otro mensaje LDP. Acción: Transmitir mensaje de notificación de error (NAK) y cerrar la conexión de transporte.	No Existente

Operacional	Recibir mensaje de finalización. Acción: Transmitir mensaje de finalización y cerrar la conexión de transporte.	No Existente
Operacional	Recibir cualquier otro mensaje LDP	Operacional
Operacional	Intervalo de tiempo sobrepasado. Acción: Transmitir mensaje de finalización y cerrar la conexión de transporte.	No Existente

Tabla 3.1. Tabla de Transición

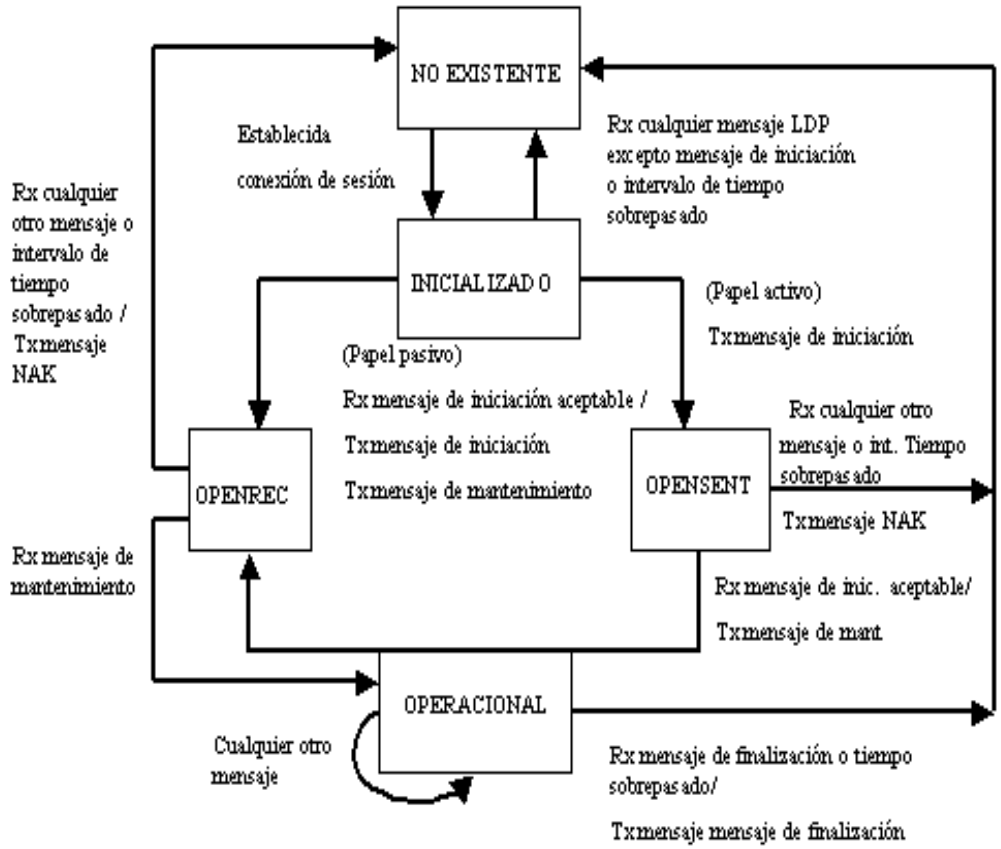


Figura 3.27. Diagrama de Transición de Estado de Inició de Sesión LDP

Formato de los mensajes

PDUs LDP

El intercambio de mensajes entre LSRs pares se realiza mediante el envío de PDUs (PDU: Protocol Data Unit: Unidad de datos del protocolo) LDP. Cada PDU LDP puede transportar más de un mensaje.

Cada PDU LDP está compuesto por una cabecera seguida de uno o más mensajes LDP.

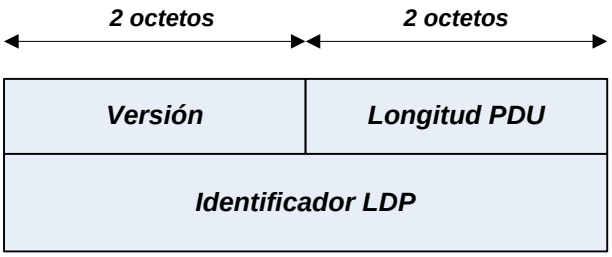


Figura 3.28. Formato de la Cabecera PDU LDP

- Versión: Dos octetos que identifican la versión del protocolo. Actualmente la 1
- Longitud PDU: Dos octetos que especifican la longitud total en octetos de la PDU excluyendo los campos de la Versión y la Longitud de la PDU. La longitud de la PDU es negociable cuando se inicia la sesión LDP. Antes de la negociación, el tamaño máximo admitido es de 4096 octetos.

- Identificador LDP: Campo de 6 octetos definido anteriormente.

Codificación TLV (Type-Length-Value: Tipo-Longitud-Valor)

El protocolo LDP utiliza el esquema de codificación de mensajes conocido como TLV.

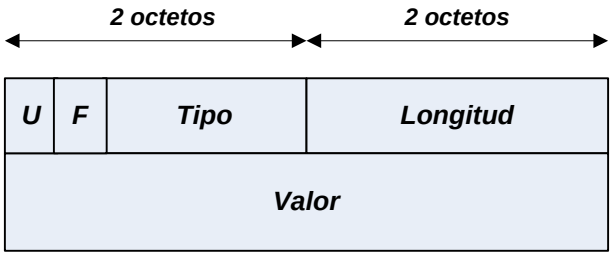


Figura 3.29. Cabecera TLV

- U: Bit de desconocido (Unknown). Si se recibe una TLV desconocida y U = 0, se debe enviar un mensaje de notificación al LSR origen y se ignora el mensaje. Si U = 1 se ignora el mensaje sin notificación.
- F: Bit de reenvío de una TLV desconocida (Forward Unknown). Este campo sólo se utiliza cuando el bit U está activo. Si F = 0 la TLV desconocida no es reenviada. Si F = 1 la TLV desconocida se reenvía.
- Tipo: Campo de 14 bits que define el tipo de mensaje y por tanto indica cómo debe ser procesado el campo Valor.
- Valor: Campo de tamaño variable con la información a ser interpretada como lo especifique el campo Tipo. Este campo puede tener a su vez TLVs.

Codificaciones TLV para los parámetros usados frecuentemente

TLVs definidas en la versión 1 del protocolo:

- FEC: Esta TLV contendrá las FECs que se intercambian los LSRs. Una FEC podrá ser un prefijo de dirección o una dirección completa de un host. El elemento FEC comodín se utiliza exclusivamente en los mensajes de liberación y retiro de etiquetas.
- Etiquetas: Estas TLVs sirven para codificar etiquetas. Las TLVs de etiquetas son transportadas por los mensajes de anuncio, petición liberación y retiro de etiquetas. Tipos de TLVs de etiquetas:
    - Etiqueta genérica: Un LSR utiliza este tipo de TLV para codificar etiquetas que se van a usar en enlaces para los que los valores de las etiquetas son independientes de la tecnología del nivel de enlace subyacente (por ejemplo, PPP y Ethernet).
    - Etiqueta ATM: Un LSR utiliza este tipo de TLV para codificar etiquetas a usar en enlaces ATM. Esta TLV contendrá los valores ATM VPI/VCI.
    - Etiqueta de retransmisión de tramas (Frame Relay): Un LSR utilizará la TLV de etiqueta de retransmisión de

tramas para codificar etiquetas a usar en enlaces Frame Relay. Contendrá los valores DLCI de Frame Relay.

- Lista de direcciones: La TLV de lista de direcciones aparece en los mensajes de dirección y retiro de etiquetas. Actualmente sólo está definido IPv4.
- Cuenta de saltos: Esta TLV aparece como un campo opcional en los mensajes que establecen los LSPs. Calcula el número de saltos LSR a través de un LSP a medida que el LSP se establece. Se puede usar para la detección de bucles.
- Vector camino: Se utiliza conjuntamente con la TLV de cuenta de saltos en los mensajes de petición y asociación de etiquetas para implementar el mecanismo opcional de detección de bucles. Su uso en el mensaje de petición de etiquetas registra el camino de LSRs que ha atravesado la petición. En el mensaje de asociación de etiquetas, registra el camino de LSRs que el mensaje de aviso (Advertisement) ha atravesado para establecer el LSP.
- Estado: Los mensajes de notificación transportan TLVs de estado para especificar los eventos que se están señalizando.
- Estado extendido: Extiende la TLV anterior con información adicional.

- PDU devuelta: Esta TLV puede operar con la TLV de estado. Un LSR la utilizará para devolver parte de la PDU LDP que le envió otro LSR. El valor de esta TLV será la cabecera de la PDU y tantos datos de la PDU como sean necesarios por la condición que marque el mensaje de notificación.
- Mensaje devuelto: Se puede usar conjuntamente con la TLV de estado. Sirve para devolver parte de un mensaje LDP al LSR que lo envió.
- Parámetros HELLO comunes: Esta TLV contiene parámetros comunes para manejar los mensajes HELLO.
- Dirección de transporte IPv4: Esta TLV permite que se use una dirección IPv4 al abrir una conexión TCP para una sesión LSP.
- Número de secuencia de configuración: Identifica el estado de configuración del LSR emisor. Se usa para que el LSR receptor pueda detectar cambios en la configuración.
- Dirección de transporte IPv6: Esta TLV permite que se use una dirección IPv6 al abrir una conexión TCP para una sesión LSP.
- Parámetros comunes de la sesión: Esta TLV tendrá los valores propuestos por el LSR emisor para los parámetros que pretende negociar en una sesión LDP.

- Parámetros de la sesión ATM: Esta TLV contiene las capacidades de un LSR ATM.
- Parámetros de la sesión de retransmisión de tramas: Igual que la anterior, pero para retransmisión de tramas.
- Identificador del mensaje de petición de etiquetas: El valor de este parámetro es el identificador del mensaje de petición de etiquetas.
- Privada de vendedor (propietaria): Usada para transmitir información de privada de vendedor (propietaria).
- Experimental: Para usos experimentales.

Mensajes

Todos los mensajes LDP tienen el siguiente formato:

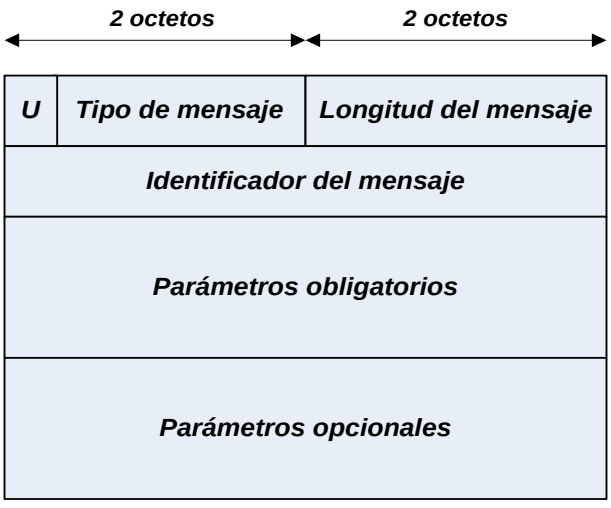


Figura 3.30. Formato de mensajes LDP

- U: Bit de mensaje desconocido. Cuando se reciba un mensaje desconocido, si U = 0 se enviará una notificación al origen del mensaje. Si U = 1 simplemente se ignorará.
- Tipo de mensaje: Identifica el tipo del mensaje.
- Longitud del mensaje: Longitud del identificador del mensaje, de los parámetros obligatorios y de los parámetros opcionales
- Identificador del mensaje: Identificador del mensaje.
- Parámetros obligatorios: Conjunto de todos los parámetros obligatorios de los mensajes. Este campo tiene una longitud variable. Algunos mensajes no tienen parámetros obligatorios.
- Parámetros opcionales: Conjunto de los parámetros opcionales de los mensajes. Este campo también es de longitud variable.
- Todo lo que aparece en un mensaje LDP se podría codificar en una TLV, pero la especificación no utiliza dicha codificación para todos los casos.
- Los tipos de mensajes que define la especificación son los siguientes:
    - Notificación
    - HELLO
    - Iniciación
    - Mantenimiento

- Dirección
- Retiro de dirección
- Asociación de etiqueta
- Petición de etiqueta
- Petición de abandono de etiqueta
- Retiro de etiqueta
- Liberación de etiquetas

A continuación se mostrará el formato de cada uno de estos mensajes.

Mensaje de notificación

Este tipo de mensajes es utilizado por un LSR para notificarle a su par LSR de una condición de error o para suministrarle información de aviso.

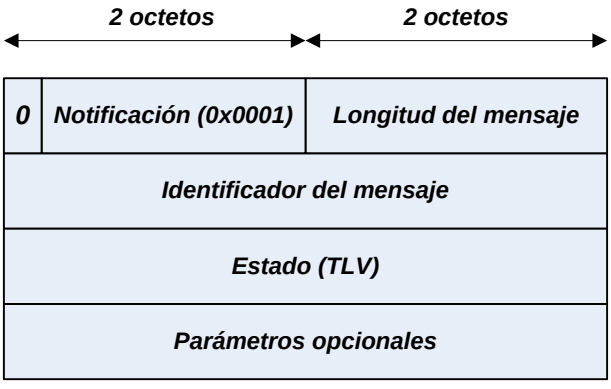


Figura 3.31. Formato del mensaje de notificación de LSR a LSR

- Identificador de mensaje: Valor de 32 bits usado para identificar el mensaje.
- TLV de estado: Indica el evento que está siendo señalizado
- Parámetros opcionales: Campo de longitud variable. Contiene cero o más parámetros, cada uno codificado en una TLV. Los parámetros que pueden aparecer son: Estado extendido, PDU devuelta y mensaje devuelto.

Cuando un LSR recibe un mensaje de notificación que contiene un código de estado que indica un gran error fatal, éste terminará la sesión LDP cerrando conexión TCP de la sesión y descartará todo estado asociado a la sesión, incluyendo todas las asociaciones de etiquetas a FECs aprendidas en dicha sesión LDP.

Clasificación de los eventos que este tipo de mensajes señalizan:

- PDU mal formada o mensaje mal formado.
- TLV desconocida o mensaje desconocido.
- Expiración del temporizador del mantenimiento de la sesión.
- Terminación de la sesión unilateralmente.
- Eventos de mensajes de iniciación.
- Eventos resultantes de otros mensajes
- Errores internos.

- Eventos diversos.

Mensaje HELLO

Este tipo de mensajes son intercambiados entre pares LDPs durante la fase de descubrimiento.

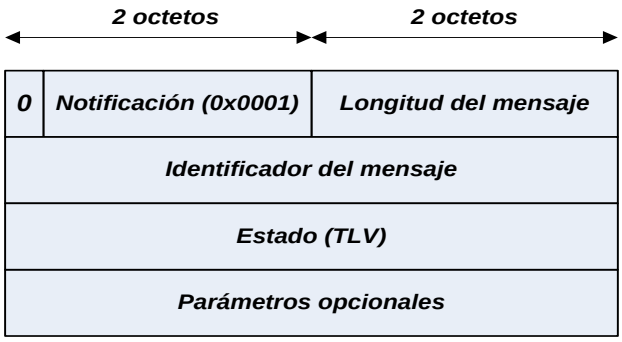


Figura 3.32. Formato del mensaje HELLO

- Identificador del mensaje: Valor de 32 bits usado para identificar el mensaje.
- TLV de parámetros comunes HELLO. Especifica los parámetros comunes de los mensajes HELLO. El formato TLV se puede apreciar en la figura 3.33. Campos:
  - Tiempo de espera: Tiempo de espera en segundos. Un LSR mantiene un registro de los HELLOs recibidos de pares potenciales. Este campo especifica el tiempo que el LSR emisor mantendrá el registro de HELLOs del receptor sin recibir otro HELLO. Los LSRs negocian los tiempos de espera que usarán para los HELLOs de cada

uno. Cada uno propondrá un tiempo y se utilizará el mínimo entre ambos.

- T: HELLO con destino (Targeted HELLO). T = 1 implica que este HELLO es un HELLO con destino. T = 0 implica que es un HELLO de enlace. Recordemos que existían dos modalidades de descubrimiento. La modalidad básica utiliza este último tipo de HELLOs. La extendida utiliza el primer tipo de HELLOs.
- R: Petición de envío de HELLOs con destino. Un valor de uno indica una petición al receptor de mandar periódicamente HELLOs con destino a la fuente. Un valor de cero implica que no hay petición.

- Parámetros opcionales: Campo de longitud variable que contiene cero o más parámetros codificados como TLVs. Los parámetros opcionales son: Dirección de transporte IPv4, configuración del número de secuencia, dirección de transporte IPv6.

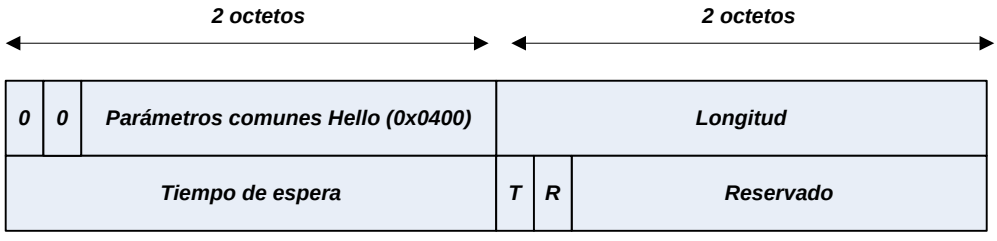


Figura 3.33. Formato TLV con parámetros HELLO

Mensaje de Iniciación

Este mensaje se utiliza cuando dos pares LDP desean establecer una sesión LDP.

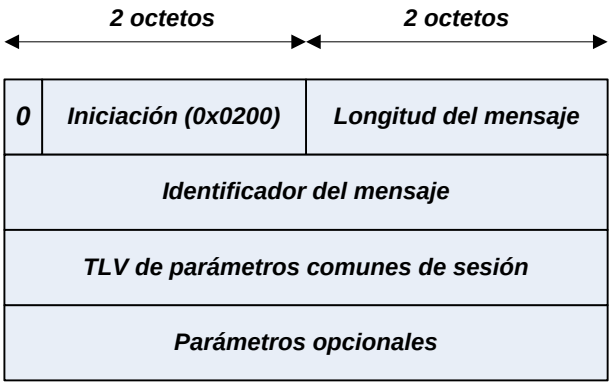


Figura 3.34. Formato del Mensaje de Iniciación entre dos LDP

- Identificador del mensaje: Valor de 32 bits usado para identificar el mensaje.
- TLV de parámetros comunes de sesión: Especifica los parámetros propuestos por el emisor para la negociación de la sesión LDP. Estos parámetros son: Tiempo de mantenimiento, disciplina de anuncio de etiquetas (downstream no solicitado y downstream por demanda), detección de bucles, máximo tamaño del vector camino, longitud máxima de la PDU, etc.
- Parámetros opcionales: Campo de longitud variable que contiene cero o más parámetros codificados en TLVs. Los

parámetros opcionales son: Parámetros de sesión ATM y parámetros de sesión de retransmisión de tramas.

Mensaje de Mantenimiento (KeepAlive)

Estos mensajes los intercambian pares LSRs para monitorizar la integridad de la conexión de transporte de la sesión LDP.

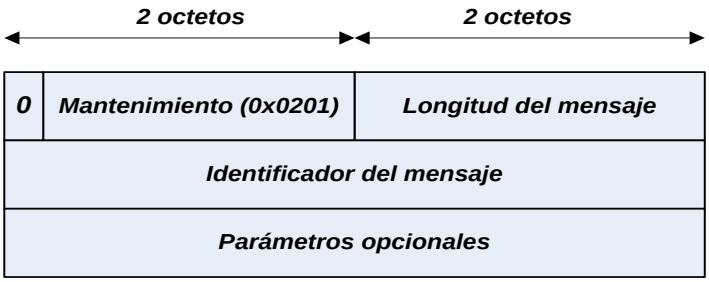


Figura 3.35. Formato del mensaje Keep Alive en sesión LDP

- Identificador del mensaje: Valor de 32 bits usado para identificar el mensaje.
- Parámetros opcionales: No definidos.

Mensaje de Dirección

Este mensaje se lo manda un LSR a su par LSR para notificarle las direcciones de sus interfaces. El LSR que reciba este mensaje utilizará las direcciones aprendidas para actualizar una base de datos para las correlaciones entre los identificadores LDP de los pares y las direcciones de los siguientes saltos.

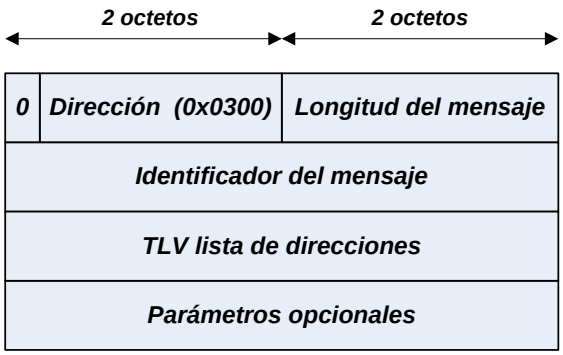


Figura 3.36. Formato del mensaje de Dirección en sesión LDP

- Identificador del mensaje: Valor de 32 bits usado para identificar el mensaje.
- TLV lista de direcciones: Lista de las direcciones de las interfaces que están siendo notificadas por el LSR emisor.
- Parámetros opcionales: No definidos.

Mensaje de Retiro de Direcciones

Este mensaje se utiliza para retirar las direcciones de interfaces notificadas anteriormente.

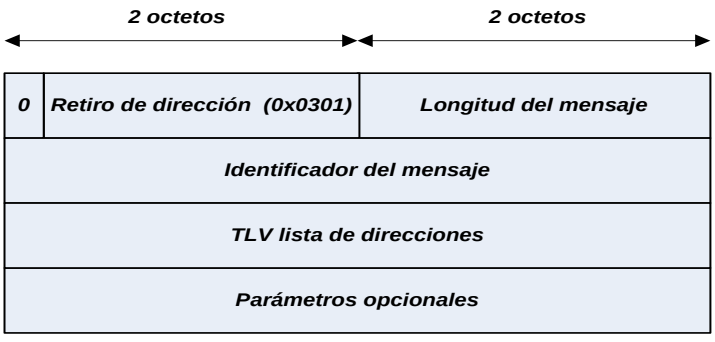


Figura 3.37. Formato del Mensaje de Retiro de Direcciones de sesiones LDP

- Identificador del mensaje: Valor de 32 bits usado para identificar el mensaje.
- TLV lista de direcciones: Lista de las direcciones de los interfaces que se están retirando por el LSR emisor.
- Parámetros opcionales: No definidos.

Mensaje de Asociación de Etiquetas

Este mensaje lo utiliza un LSR para notificarle a su par LSR una asociación de etiquetas.

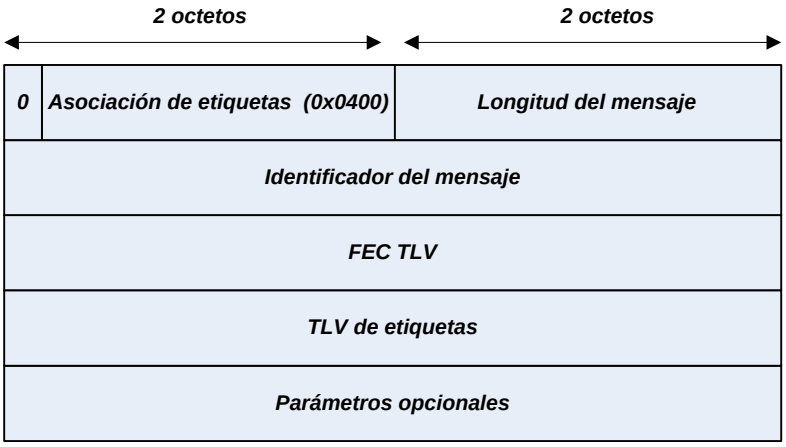


Figura 3.38. Formato del Mensaje de Asociación de etiquetas en sesión LDP

- Identificador del mensaje: Valor de 32 bits usado para identificar el mensaje.
- FEC TLV: Especifica el componente FEC de la asociación de etiquetas que se está notificando.

- TLV de etiquetas: Especifica el componente de etiqueta de la asociación de etiquetas.
- Parámetros opcionales: Campo de longitud variable que contiene cero o más parámetros codificados en TLVs. Los parámetros opcionales son: TLV identificador del mensaje de petición de etiquetas, TLV de cuenta de saltos y TLV de vector camino.

Mensaje de Petición de Etiquetas

Este mensaje se lo manda un LSR a su par LSR cuando quiere solicitarle una asociación de etiquetas.

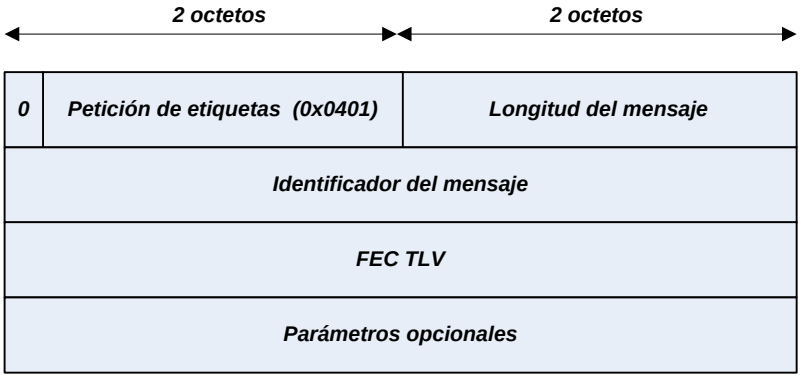


Figura 3.39. Formato del Mensaje de Petición de Etiquetas

- Identificador del mensaje: Valor de 32 bits usado para identificar el mensaje.
- FEC TLV: La FEC para la que se está solicitando la etiqueta.

- Parámetros opcionales: Campo de longitud variable que contiene cero o más parámetros cada uno codificado como una TLV. Los parámetros opcionales son: TLV de cuenta de saltos. TLV de vector camino.

El mensaje de petición de etiquetas lo utiliza un LSR que está upstream para solicitarle explícitamente al LSR que está downstream una asociación de etiquetas.

Un LSR puede enviar un mensaje de petición de etiquetas sí:

1. El LSR reconoce una nueva FEC vía la tabla de reenvío y el siguiente salto es un par LDP, y además el LSR no tiene una asociación del siguiente salto para dicha FEC.
2. El siguiente salto para la FEC cambia y el LSR no tiene todavía la asociación de su siguiente salto para dicha FEC.
3. El LSR recibe una petición de etiquetas para una FEC de su par LDP que está upstream, el siguiente salto de la FEC es un par LDP, y el LSR no tiene la asociación de su siguiente salto.

Mensaje de Petición de Abandono de Etiqueta

Este mensaje abandona una petición de etiquetas pendiente.

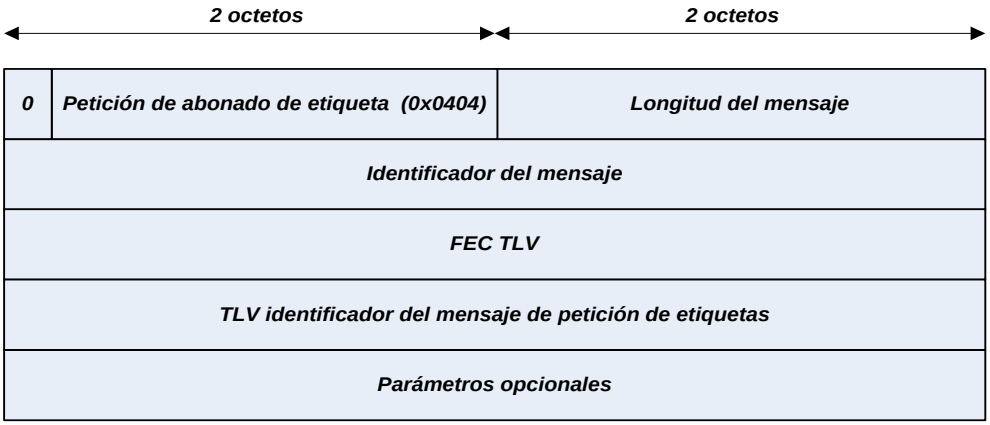


Figura 3.40. Formato del Mensaje de Petición de Abandono de Etiqueta

- Identificador del mensaje: Valor de 32 bits usado para identificar el mensaje.
- FEC TLV: Identifica a la FEC para la que se está abandonando la petición de etiquetas.
- TLV identificador del mensaje de petición de etiquetas: Especifica el identificador del mensaje de petición de etiquetas que se va a abandonar.
- Parámetros opcionales: No definido.

Mensaje de Retiro de Etiquetas

Este mensaje se utiliza para retirar una asociación de etiquetas que está siendo usada. Un LSR le enviará este tipo de mensaje a su par LSR para indicarle que no puede continuar usando la asociación que

previamente anunció. De esta forma se rompen las asociaciones entre etiquetas y FECs.

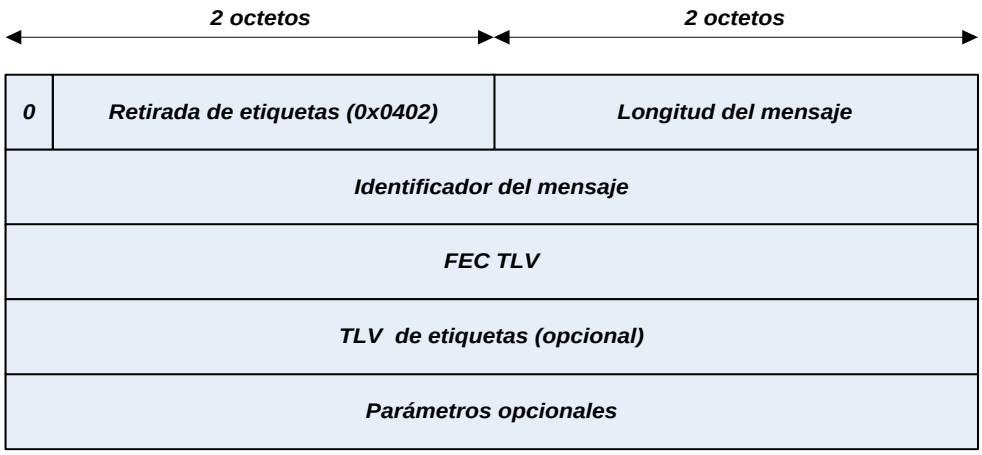


Figura 3.41 Formato del Mensaje de Retiro de Etiquetas

- Identificador del mensaje: Valor de 32 bits usado para identificar el mensaje.
- FEC TLV: Identifica la FEC para la que la asociación de etiquetas está siendo retirada.
- TLV de etiquetas: Campo de longitud variable. Si no aparece este campo, se retirarán todas las etiquetas asociadas a la FEC. En caso de que aparezca, sólo se retirará dicha etiqueta.
- Parámetros opcionales: Campo de longitud variable que contiene cero o más parámetros codificados como TLVs.

Un LSR enviará este tipo de mensajes bajo las siguientes condiciones:

1. El LSR no reconoce una FEC que antes reconocía para la que ha anunciado una etiqueta.
2. El LSR ha decidido unilateralmente (por ejemplo, vía configuración) que no va a realizar la conmutación de etiquetas para la FEC o FECs con la asociación que se va a retirar.

Un LSR que reciba este tipo de mensaje debe responder con un mensaje de liberación de etiquetas.

Mensaje de Liberación de Etiquetas

Este mensaje se utiliza cuando un LSR quiere informar a su par LSR que no necesita una asociación pedida o advertida anteriormente por su par LSR.

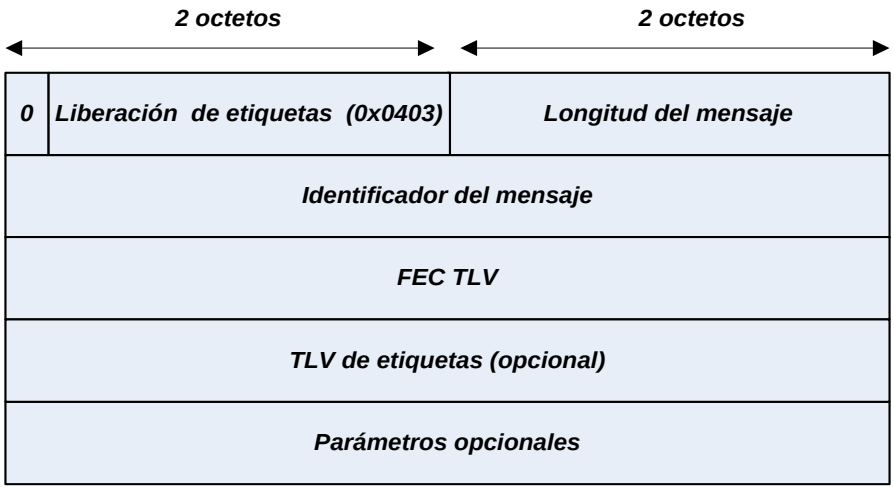


Figura 3.42 Formato del Mensaje de Liberación de Etiquetas

Los campos son iguales que en el mensaje anterior.

Un LSR debe transmitir este mensaje sí:

1. El LSR que mandó la asociación no es el siguiente salto para la FEC asociada y el LSR está configurado para operar en modo conservativo.
2. El LSR recibe una asociación de un LSR que no es el siguiente salto para la FEC, y el LSR está configurado para operar en modo conservativo.

El LSR recibe un mensaje de retiro de etiquetas

3.3.2. RSVP

El Protocolo de Reserva de Recurso (RSVP: Resource reSerVation Protocol) se utiliza para reservar recursos de una sesión en un entorno de red IP. Es un protocolo de estado blando. En la figura 3.43 podemos apreciar que el protocolo RSVP se apoya en IP:

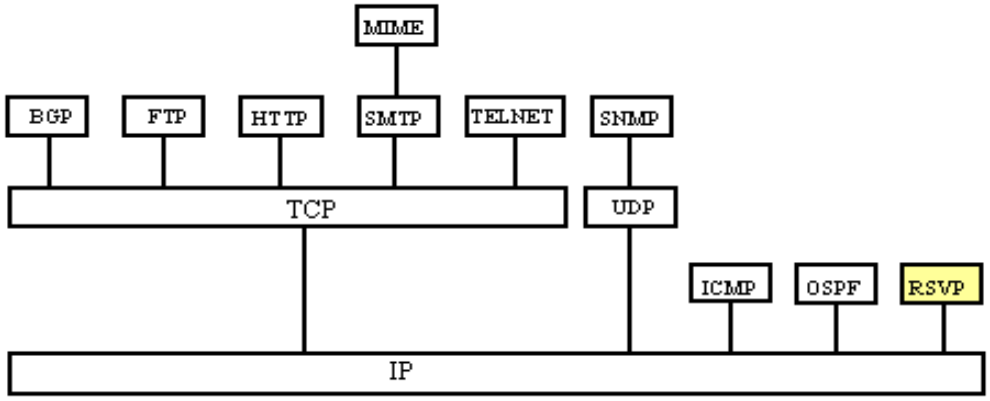


Figura 3.43 Diagrama de Protocolos

RSVP pretende proporcionar calidad de servicio estableciendo una reserva de recursos para un flujo determinado. Un host hace una petición de una calidad de servicio específica sobre una red para un flujo particular de una aplicación.

Características de RSVP

- Protocolo de reserva de recursos.
- Se diseña para trabajar con cualquier servicio de QoS (los objetos propios de la QoS no están definidos por el protocolo).
- Permite Unicast y Multicast. No es un protocolo de enrutamiento, sino que está pensado para trabajar conjuntamente con éstos.
- No transporta datos de usuario.
- Los protocolos de enrutamiento determinan dónde se reenvían los paquetes mientras que RSVP se preocupa por la QoS de los paquetes reenviados de acuerdo con el enrutamiento.
- Es un protocolo simplex: Petición de recursos sólo en una dirección, diferencia entre emisor y receptor. El intercambio entre dos sistemas finales requiere de reservas diferenciadas en ambas direcciones.
- Reserva iniciada por el receptor (protocolo orientado al receptor).

- Mantenimiento del estado de la reserva (estado blando) en los routers. El mantenimiento de la reserva es responsabilidad de los usuarios finales.
- Permite diferentes tipos de reservas.
- Protocolo transparente para los routers no RSVP.
- Soporta IPv4 e IPv6 aunque no sea un protocolo de transporte.
- Existen dos tipos fundamentales de mensajes RSVP:
- Mensajes Path: Son generados por los emisores. Describen el flujo del emisor y proporcionan la información del camino de retorno hacia el emisor. Se establece el camino de la sesión entre emisores. Pueden atravesar routers que no entiendan RSVP puesto que tienen una dirección IP origen y una dirección IP destino.
- Mensaje Resv: Los generan los receptores y sirven para hacer una petición de reserva de recursos. Crean el "estado de la reserva" en los routers. Generalmente, una petición de recursos implicará una reserva de éstos en todos los nodos del camino del flujo de datos. Estos mensajes siguen exactamente el camino inverso al de los datos.
- Por tanto, el mensaje Path es el responsable del inicio de la operación y es mandado a los participantes potenciales de la

sesión. El mensaje Resv se manda en respuesta al mensaje Path.

La figura 3.44 muestra el uso de estos mensajes:

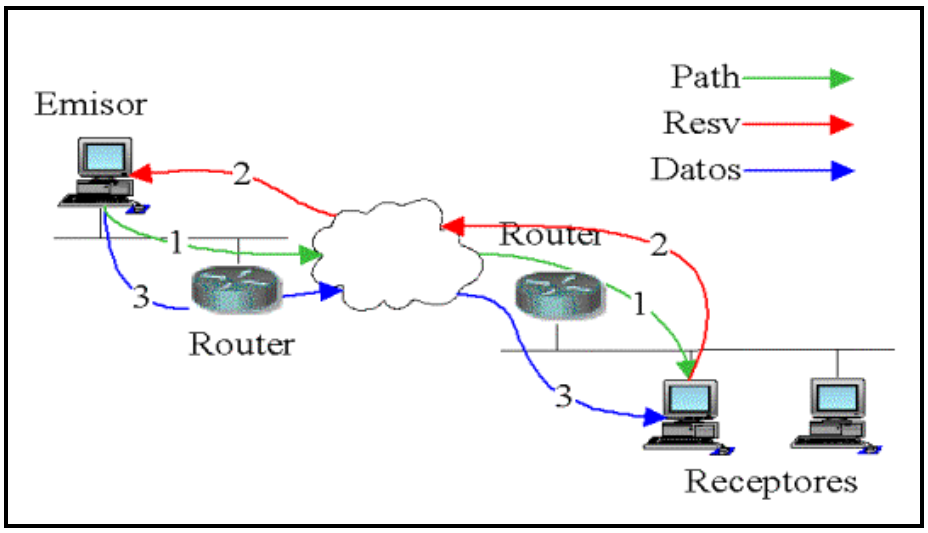


Figura 3.44 Tipos de Mensaje RSVP: Mensaje Path y mensaje Resv

Flujos de datos

Existen tres conceptos básicos asociados con los flujos de datos que maneja el protocolo.

- Sesión RSVP: Es un flujo de datos identificado por su destino y por un protocolo de transporte particular. Sus componentes son:
  - Dirección IP destino: Dirección IP destino de los paquetes (unicast o multicast)

    - Identificador del protocolo IP.
    - Puerto destino (opcional).
- Descriptor de flujo: Se llama así a una petición de reserva realizada por un sistema final. Está compuesto de:
    - Flowspec: Especifica la calidad de servicio deseada. Incluye:
    - Service class: Clase de servicio.
    - Y dos parámetros numéricos: Rspec, que define la QoS deseada (Reserve) y Tspec, que describe el flujo de datos (Traffic)
    - Filter spec: Designa un conjunto arbitrario de paquetes dentro de una sesión a los que aplicar la QoS definida por el flowspec. El formato depende de si se utiliza IPv4 o IPv6, pero básicamente es:
    - Dirección IP fuente + puerto UDP/TCP fuente

Mensajes RSVP

Un mensaje RSVP está formado por una cabecera común, seguida de un número variable de objetos de longitud variable.

Formato de la cabecera

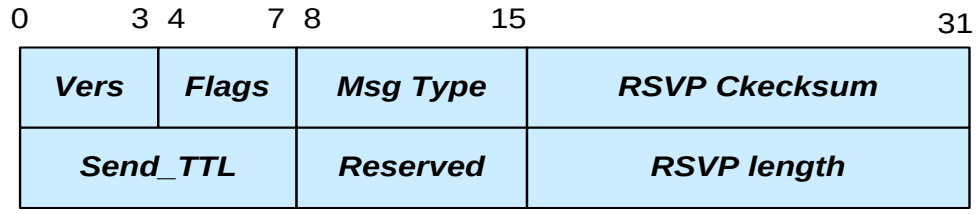


Figura 3.45 Formato de Cabecera de un Mensaje RSVP

Campos de la cabecera

- Vers: Versión del protocolo RSVP. Actualmente la 1.
- Flags: No definido.
- Msg Type: Tipo de mensaje. A continuación se enumeran.
  - Path
  - Resv
  - Path_Err
  - Resv_Err
  - PathTear
  - ResvTear
  - ResvConf
- RSVP Checksum: Campo de verificación.
- Send_TTL: Indica el tiempo de vida (Time To Live) del mensaje.
- RSVP Length: Longitud total del mensaje expresada en bytes, incluyendo la cabecera y el cuerpo.

Formato de los objetos

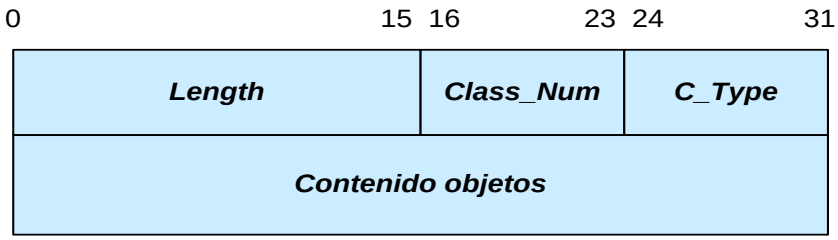


Figura 3.46 Formato de los Objetos de mensajes RSVP

Campos de los objetos

- Length: Longitud total del objeto expresada en bytes. Su valor debe ser siempre múltiplo de cuatro.
- Class_Num: Identifica la clase del objeto. Todas las implementaciones de RSVP reconocen las siguientes clases:
  - NULL
  - SESSION
  - RSVP_HOP
  - TIME_VALUES
  - STYLE
  - FLOWSPEC
  - FILTER_SPEC
  - SENDER_TEMPLATE
  - SENDER_TSPEC
  - ADSPEC

    - ERROR_SPEC
    - POLICY_DATA
    - INTEGRITY
    - SCOPE
    - RESV_CONFIRM
- C_Type: Tipo de objeto. Identifica el tipo de objeto dentro de la clase.

Funcionamiento

La fuente envía un mensaje Path a los destinos. Dicho mensaje se manda a una dirección que es una dirección de sesión. Podrá ser una dirección unicast o multicast. Cuando el destino reciba el mensaje Path podrá enviar un mensaje Resv a la fuente, que viajará justo por el camino inverso al mensaje Path. Dicho mensaje Resv identificará la sesión para la que se quiere hacer la reserva. El mensaje será reenviado hacia la fuente por los routers. Éstos reservarán los recursos necesarios analizando dicho mensaje.

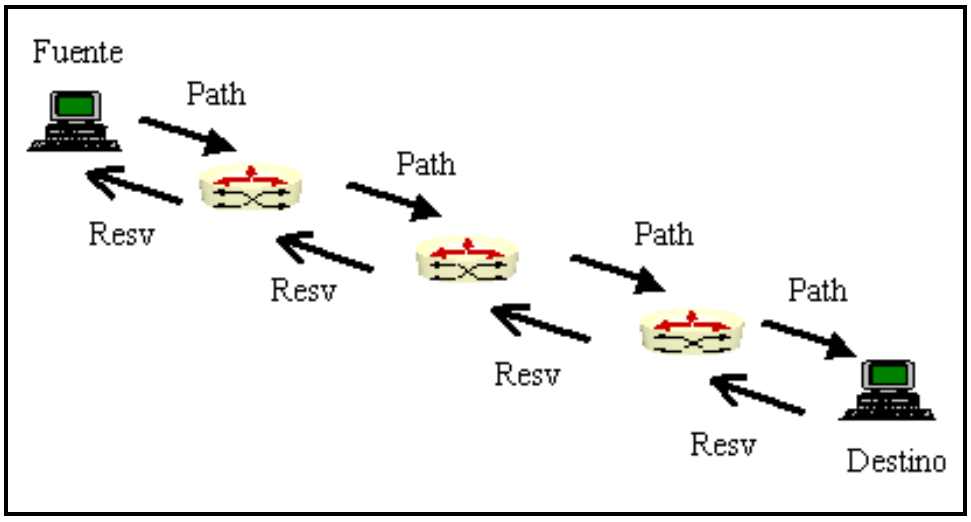


Figura 3.47 Envio de Menajes RSVP

Como vimos anteriormente, RSVP es un protocolo simplex. Los routers reconocerán los paquetes pertenecientes a un flujo examinando la dirección origen y destino, el puerto origen y destino y el número de protocolo (ej: UDP). Puesto que RSVP es un protocolo de estado blando, se deberán mandar periódicamente mensaje Path y Resv para refrescar el estado.

RSVP-TE: EXTENSIONES DE RSVP PARA TÚNELES LSP

RSVP-TE define los siguientes objetos extendidos para poder usarse con RSVP:

- Objeto Etiqueta
- Objeto Petición de etiqueta
- Objeto Ruta Explícita

- Objeto Registrar Ruta
- Objeto Sesión LSP_TUNEL_IPv4
- Objeto Sesión LSP_TUNEL_IPv6
- Objeto Plantilla Emisor LSP_TUNEL_IPv4
- Objeto Plantilla Emisor LSP_TUNEL_IPv6
- Objeto Especificación Filtro LSP_TUNEL_IPv4
- Objeto Especificación Filtro LSP_TUNEL_IPv6
- Objeto Atributo Sesión
- Objetos TSPEC y FLOWSPEC para clases de servicio
- Objetos Hello

Se puede utilizar RSVP para establecer LSPs usando la distribución de etiquetas downstream por demanda. Para establecer un LSP, el LSR de entrada mandará un mensaje Path. Dicho mensaje tendrá un Objeto de petición de etiqueta y un objeto de sesión LSP_TUNEL_IPv4 o LSP_TUNEL_IPv6. Si un nodo no es capaz de realizar una asociación de etiquetas, mandará un mensaje PathErr con un error "Clase de Objeto Desconocido".

Cuando el mensaje Path llegué al LSR de salida, éste responderá con un mensaje Resv. Este mensaje contendrá el Objeto Etiqueta, utilizado como se describe a continuación. El LSR de salida realizará una asociación de etiquetas e incluirá esta etiqueta en el Objeto

Etiqueta. Acto seguido mandará el mensaje upstream. Cuando el siguiente LSR reciba este mensaje sabrá que la etiqueta incluida en el Objeto Etiqueta será la que debe usar como etiqueta de salida para ese flujo. Una vez hecho esto, el LSR asignará una etiqueta (que será la futura etiqueta entrante), la insertará en el Objeto Etiqueta y enviará el mensaje Resv upstream. Este proceso se repetirá hasta que el mensaje llegue a la fuente. En ese momento se podrá decir que se ha establecido el LSP.

La siguiente figura muestra este proceso:

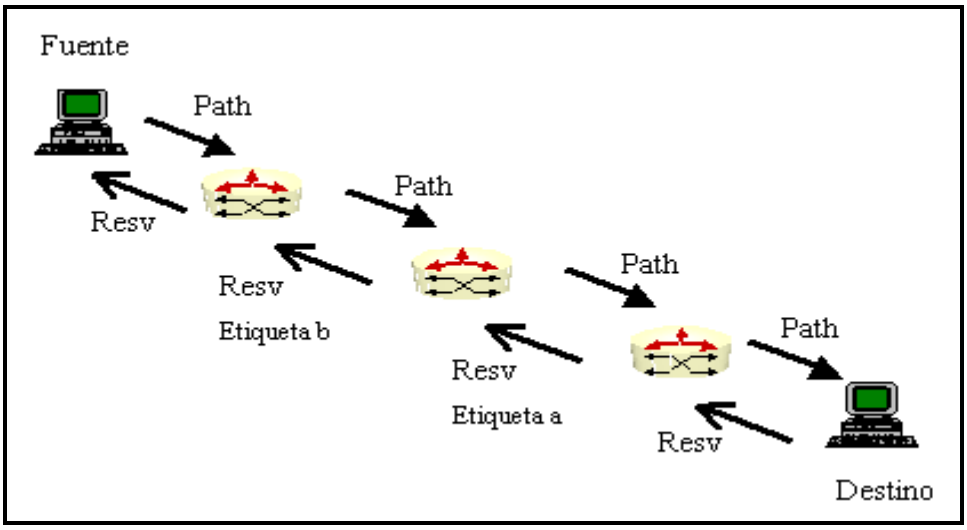


Figura 3.48 Envio de Mensajes RSVP TE con Etiquetas

El último LSR de la figura 3.48 asigna la etiqueta a y la distribuye al LSR del centro. Éste LSR asigna la etiqueta b y la distribuye al LSR de entrada. El LSP para este flujo está creado.

Un LSR de entrada puede crear una ruta explícita. Esto se consigue añadiendo al mensaje Path el Objeto Ruta Explícita. Este objeto encapsula una concatenación de saltos que constituyen el camino explícito. Este camino explícito puede ser especificado por un administrador o puede generarse automáticamente en base a una política determinada y una QoS requerida. Cuando un mensaje Path contiene el Objeto de enrutamiento explícito, cada LSR reenviará el mensaje por el camino que dicho objeto especifique.

Una de las mayores ventajas del hecho de usar RSVP para establecer túneles LSP es que permite la asignación de recursos a través del camino. Pero no es obligatorio realizar la reserva de recursos cuando se establece el LSP. Se puede establecer un LSP sin reservar ningún tipo de recursos.

3.3.3. CR-LDP

Antes de desarrollar CR-LDP (Constraint-based Routing LDP: Enrutamiento basado en restricciones LDP) conviene aclarar lo que se entiende por enrutamiento basado en restricciones.

Enrutamiento Basado en Restricciones

Con el enrutamiento convencional, es decir, con IP, la elección de un camino se basa en algún algoritmo que optimice alguna métrica

escalar. Por ejemplo, con RIP la métrica que se usa es el número de saltos. RIP elige el camino que minimice el número de saltos.

Con el enrutamiento basado en restricciones, entre cada par de nodos se deberán satisfacer una serie de restricciones. Las restricciones entre nodos diferentes podrán ser diferentes. Por supuesto, además de satisfacer dichas restricciones, también existirá una métrica particular como sucedía en el enrutamiento convencional. Una vez establecido el camino, el enrutamiento basado en restricciones será el responsable de establecer y mantener el estado del reenvío a través de dicho camino.

Las restricciones podrán ser de rendimiento, calidad de servicio como demora, variación de demora o tasa de pérdidas, administrativas o una mezcla entre ellas. Ejemplo de restricción de rendimiento puede ser el encontrar un camino que tenga un mínimo ancho de banda, y ejemplo de restricción administrativa sería que determinado tráfico atravesará sólo ciertos enlaces de la red.

CR-LDP

El grupo de trabajo sobre MPLS del IETF ha definido extensiones para que el protocolo LDP soporte el enrutamiento basado en restricciones. A esta extensión del protocolo se le denomina CR-LDP.

Cuando un LSR de entrada decide usar un camino explícito, añadirá la TLV ER (Explicit Route TLV: TLV de camino explícito) al mensaje LDP de petición de etiquetas. El uso de esta TLV para establecer un LSP requiere el uso de la distribución de etiquetas downstream por demanda y el modo de control ordenado.

Cada LSR enviará el mensaje de petición de etiquetas a través del camino especificado en dicha TLV. Cuando el mensaje llegue al LSR de salida, éste responderá con un mensaje de asociación de etiquetas, donde habrá incluido la etiqueta de la asociación.

Estos mensajes se irán enviando upstream hacia el LSR de entrada por el camino inverso por donde se mandaron los mensajes de asociación de etiquetas. Por supuesto, en cada nodo se realizará la correspondiente asociación incluyéndose la etiqueta en el mensaje que se envía upstream.

Cuando al LSR de entrada le llegue un mensaje de asociación de etiquetas para una etiqueta pedida, el LSP estará establecido.

Para poder reservar recursos en el LSP se ha definido un nuevo objeto: El objeto de parámetro de tráfico. Actualmente hay definidos siete parámetros de tráfico:

- Peak data Rate (PDR: Velocidad de pico de datos)

- Peak burst size (PBS: Tamaño de pico de la ráfaga)
- Commited data rate (CDR: Velocidad de datos garantizada)
- Commited burst size (CBS: Tamaño de ráfagas garantizada)
- Excess burst size (EBS: Tamaño de la ráfaga en exceso)
- Frequency (frecuencia)
- Weight (peso)

Con PDR y PBS se define un cubo de tokens con la máxima velocidad de tráfico que se supone que va a ir por el LSP. Con CDR y CBS se define un cubo de tokens con la velocidad media que se supone que va a ir por el LSP. EBS define un cubo goteante que indica cuánto puede sobrepasar la ráfaga a lo pactado.

CR-LDP no requiere actualizaciones periódicas de la información de estado. CR-LDP y RSVP-TE son dos protocolos de señalización que realizan funciones similares en redes MPLS. Actualmente no hay consenso sobre si uno es superior tecnológicamente al otro.

Las limitaciones de CR-LDP en la actualidad son las siguientes:

- Sólo soporta LSPs punto a punto.
- Sólo soporta el establecimiento unidireccional de LSPs.
- Sólo soporta una única etiqueta por LSP.

Lógicamente, se está trabajando para encontrar soluciones a las presentes limitaciones.

3.3.4. BGP

BGP es un protocolo de enrutamiento usado entre sistemas autónomos. Está siendo utilizado ampliamente para conectar grandes redes de proveedores. El protocolo utiliza mensajes que se envían utilizando conexiones TCP. Los distintos tipos de mensajes que maneja este protocolo son:

- Open: Se utiliza para establecer una relación de vecindad con otro Router.
- Actualización (Update): Se utiliza para transmitir información a través de una ruta y/o enumerar múltiples rutas que se van a eliminar.
- Mantenimiento (Keepalive): Utilizado para confirmar un mensaje Open y para confirmar periódicamente la relación de vecindad.
- Notificación: Este tipo de mensajes se envían cuando se detecta una condición de error.

Los procedimientos funcionales de BGP son:

Adquisición de vecinos: Ocurre cuando dos Routers situados en diferentes sistemas autónomos se ponen de acuerdo para

intercambiar información de enrutamiento regularmente. Un Router le enviará a otro un mensaje Open. Si el destino acepta la solicitud le devolverá un mensaje de mantenimiento.

1. Detección de vecino alcanzable: Una vez realizada la adquisición de vecinos se utiliza este procedimiento para mantener la relación. Periódicamente ambos dispositivos de enrutamiento se envían mensajes de mantenimiento para asegurarse que su par sigue existiendo y desea continuar con la relación de vecindad.
2. Detección de red alcanzable: Cada router mantiene una base de datos con las redes que puede alcanzar y la ruta preferida para alcanzar dichas redes. Cuando se realiza un cambio a esta base de datos, el router enviará un mensaje de actualización por difusión. De esta forma el resto de los routers BGP podrán construir y mantener la información de enrutamiento.

MPLS-BGP

En MPLS se puede utilizar BGP para distribuir la información de asociación de etiquetas para cada ruta que se anuncie. Esto es posible gracias a las extensiones multiprotocolo (MPEs: Multiprotocol Extensions) de BGP versión 4.

Para distribuir las etiquetas se utilizan los mensajes de actualización (utilizando piggybacking), los cuales también se utilizan para distribuir la información de las rutas. La etiqueta se codifica en el campo NLRI (Network Layer Reachability Information: información de alcanzabilidad del nivel de red) y para indicar que el campo NLRI contiene una etiqueta, se utiliza el campo SAFI (Subsequent Address Family Identifier: identificador de familias de direcciones consecutivas). Un hablante BGP no podrá utilizar BGP para la distribución de etiquetas hacia un igual a no ser que dicho igual le indique que puede procesar mensajes de actualización con el campo SAFI especificado.

Ventajas de la utilización de MPLS-BGP:

- Si dos LSRs adyacentes también son hermanos BGP (peers), entonces la distribución de etiquetas se puede realizar sin necesidad de tener otro protocolo de distribución de etiquetas.
- Supongamos una red con dos clases de LSRs: LSRs exteriores, que hacen de interfaz con otras redes, y LSRs interiores, que sólo transmiten tráfico entre los LSRs exteriores. Si los LSRs exteriores también son hablantes BGP y distribuyen etiquetas MPLS con la información de encaminamiento, entonces los LSRs interiores no necesitan recibir ninguna de las rutas BGP de los hablantes BGP.

Como se comentó anteriormente, las etiquetas se transportan como parte del campo NRLI en los atributos de extensión multiprotocolo. El AFI indica la familia de direcciones de la ruta asociada. Si el campo NLRI contiene una etiqueta, se le dará un valor de cuatro al campo SAFI para identificar esta situación.

El campo NLRI se codifica en una o más tripletas <longitud, etiqueta, prefijo> de la siguiente forma:

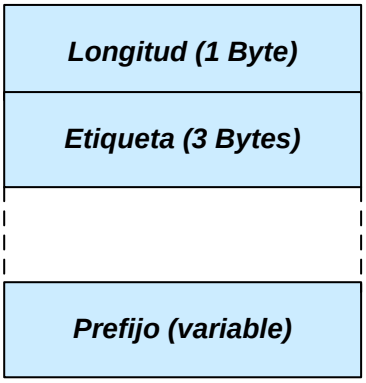


Figura 3.49 Forma del campo NLRI

- Longitud: Este campo se utiliza para indicar la longitud en bits del prefijo de dirección más la etiqueta.
- Etiqueta: El campo de la etiqueta sirve para transportar una o más etiquetas (lo que corresponde a la pila de etiquetas). Cada etiqueta se codifica en 3 Bytes, donde los 20 bits de más peso contienen el valor de la etiqueta y los bits de menos peso contienen la parte baja de la pila.

- Prefijo: Este campo contiene los prefijos de dirección seguidos de bits de relleno para conseguir que el campo ocupe un número exacto de Bytes.

Para retirar una ruta anunciada previamente un hablante BGP podrá:

- Anunciar una nueva ruta (y una etiqueta) con la misma NLRI que la ruta previa.
- Listando la NLRI de la ruta previa en el campo de retirada de rutas (Withdrawn Routes Field) de un mensaje de actualización.

Si se termina una sesión BGP también se retiran todas las rutas anunciadas previamente.

Anuncio de Múltiples Rutas a un Destino

Un hablante BGP puede mantener (y anunciar a sus hermanos) más de una ruta hacia un mismo destino siempre que cada ruta tenga sus propias etiquetas.

La codificación mencionada previamente permite que un solo mensaje de actualización contenga múltiples rutas, cada una con su(s) propia(s) etiqueta(s).

Para el caso en el que un hablante BGP anuncie múltiples rutas a un destino, si la ruta es retirada y la etiqueta(s) se especifica a la vez que la retirada, sólo dicha ruta con su correspondiente etiqueta es retirada.

Si la ruta se retira y no se especifica etiqueta, entonces sólo la ruta sin etiquetar correspondiente se retira y se mantienen las rutas etiquetadas.

Hermanos BGP que no son adyacentes

Veámoslo con un ejemplo:

Figura 3.50 Routers BGP adyacentes

D le distribuye a A la etiqueta L. A no podrá simplemente apilar L en la pila de etiquetas del paquete y enviar dicho paquete hacia B. D debe ser el único LSR que vea L en la cima de la pila. Antes de que A le envíe el paquete deberá apilar otra etiqueta que habrá obtenido previamente de B. B remplazará esta etiqueta con otra que obtuvo de C. Dicho de otra forma, de haber un LSP entre A y D. Si no existiera dicho LSP, A no podría usar la etiqueta L. Esto siempre será cierto cuando las etiquetas se distribuyan entre LSRs que no son adyacentes, no importando si la distribución se hace por BGP o por cualquier otro método.

3.4. APLICACIONES

Las principales aplicaciones que hoy en día tiene MPLS son:

- Ingeniería de tráfico
- Diferenciación de niveles de servicio mediante clases (CoS) y calidad de servicio (QoS)
- 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.

3.4.1. INGENIERIA 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 congestionados, a otros enlaces menos congestionados, aunque estén fuera de la ruta más corta (con menos saltos). En el esquema de la figura 3.51 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

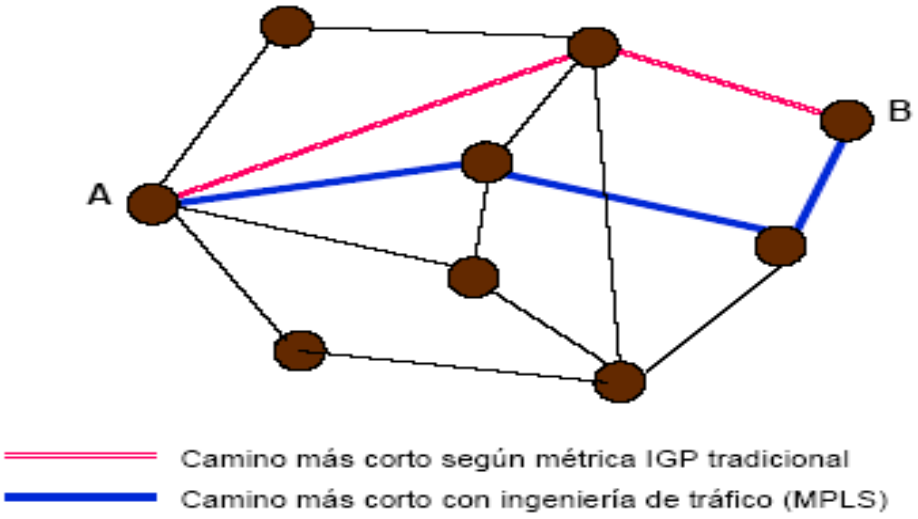


Figura 3.51 La Ruta mas corta según IGP o MPLS

El camino más corto 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 haga aconsejable la utilización del camino alternativo indicado con un salto más.

MPLS es una herramienta efectiva para esta aplicación en grandes *Backbones*, porque:

- 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 "enrutamiento 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 mas flexibles y menores costes de planificación y gestión para el administrador y con mayor calidad de servicio para todos los clientes.

3.4.2. DIFERENCIACION DE NIVELES MEDIANTE CLASE Y CALIDAD DE SERVICIO

MPLS soporta diferentes clases de servicio para cada LSP. Como caso particular, puede soportar servicios diferenciados en el mismo LSP.

Históricamente, Internet ha ofrecido un solo nivel de servicio: "Best effort". Con la aparición de aplicaciones multimedia y aplicaciones en tiempo real, surgió la necesidad de la diferenciación de servicios en Internet. De esta forma se podrán diferenciar servicios como el correo electrónico de otros que dependen mucho más del retardo y de la variación del mismo como el video y la voz interactiva.

El modelo de los servicios diferenciados define los mecanismos para poder clasificar el tráfico en clases de servicio con diferentes prioridades. Para clasificar el tráfico se emplea el campo ToS (Type of Service: Tipo de Servicio). A este campo se le llama DS en DiffServ. Una vez clasificados los paquetes en la frontera de la red, los paquetes se reenvían basándose en el campo DS. El reenvío se realiza por salto, es decir, el nodo decide por sí solo como se deberá realizar el reenvío. A este concepto se le denomina comportamiento por salto (PHB: Per-Hop Behavior).

MPLS se adapta bien a este modelo, porque las etiquetas MPLS tienen el campo Exp para poder propagar la clase de servicio CoS en el correspondiente LSP. Por tanto, una red MPLS puede transportar distintas clases de tráfico. Entre cada par de LSRs exteriores se pueden tener distintos LSPs con distintas prestaciones y distintos anchos de banda.

3.4.3. SERVICIOS DE REDES PRIVADAS VIRTUALES

Una de las principales razones del despliegue de MPLS en proveedores de servicios y redes empresariales son los servicios de VPNs.

Una red privada virtual se puede definir como una red en la que la conectividad entre múltiples lugares se realiza a través de una infraestructura compartida con las mismas políticas de acceso y seguridad que en una red privada. Una compañía en la que su Intranet corra encima de un servicio de VPN tendrá la misma seguridad, fiabilidad, etc., que el resto de sus redes privadas. Por tanto, el objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables.

Las dos características más importantes de una VPN desde el punto de vista del usuario son la seguridad y la privacidad.

Las primeras WANs usaban líneas dedicadas y alquiladas para realizar sus conexiones. Estas redes tienen el inconveniente de ser caras, debido a la necesidad del alquiler de las líneas.

Posteriormente, con la introducción de las VPNs, se pueden conectar múltiples sitios usando el Backbone de un proveedor de servicios. Dicho proveedor ofrecerá servicios VPN a un precio inferior que con líneas dedicadas porque el proveedor de servicios podrá utilizar los recursos de su Backbone de forma compartida para múltiples clientes.

Debido a que las soluciones existentes de aquel entonces no eran compatibles surgió un gran interés por las redes privadas virtuales basadas en IP que funcionaran en la red de redes (Internet) y que utilizaran estándares que funcionaran a través de múltiples proveedores de servicios. De esta forma se consigue una mayor flexibilidad en el diseño e implantación con unos menores costos de gestión y provisión del servicio. La forma de conseguir VPNs IP es construyendo túneles IP de diversos modos. El objetivo de un túnel IP es crear una asociación permanente entre dos extremos de modo que funcionalmente parezcan conectados. Se está utilizando una estructura no orientada a conexión para simular dichas conexiones.

El inconveniente de este tipo de soluciones es que:

- Están basadas en conexiones punto a punto.
- La configuración es manual: Una nueva conexión supone alterar todas las configuraciones.
- Plantean problemas de crecimiento.
- La gestión de la QoS es posible pero costosa.

El problema que plantean las VPNs IP es que están basadas en el modelo superpuesto, por lo que el número de adyacencias es elevado y la escalabilidad limitada. Con MPLS se solucionan estos problemas, puesto que tendremos un modelo acoplado. MPLS reenvía los datos sirviéndose de las etiquetas que tienen los paquetes. Los nodos intermedios no tienen que analizar los datos del paquete. Como no se miran las direcciones IP de los paquetes, MPLS ofrece un mecanismo de encapsulado eficiente para el tráfico privado que atraviesa la red del proveedor de servicios.

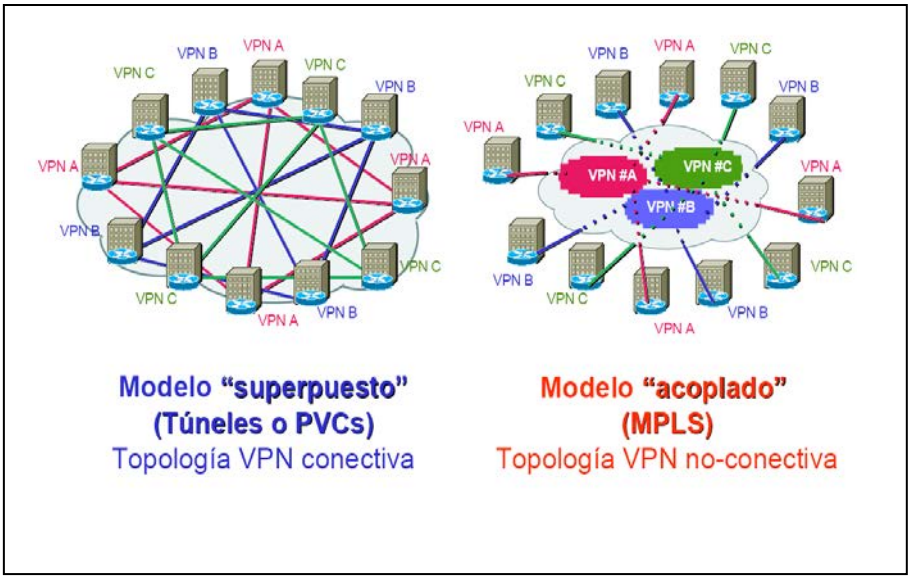


Figura 3.52 Comparación entre Túneles o PVCs y MPLS

Las VPNs MPLS se basan en el uso de túneles LSP para el reenvío de los datos entre los routers frontera de un proveedor de servicios. Al etiquetar los datos que entran en la VPN, un LSR podrá separar los flujos VPN del resto de los datos que fluyen por el Backbone del proveedor de servicios.

Las ventajas que ofrece MPLS para VPNs IP son las siguientes:

- Modelo acoplado frente al superpuesto.
- La provisión del servicio es sencilla.
- Es más fácilmente escalable.
- Se puede garantizar la QoS de los datos que entran en la VPN reservando los recursos necesarios para el túnel LSP.

- Permite aprovechar las posibilidades de la ingeniería de tráfico de tal forma que se pueda garantizar la respuesta global de la red (ancho de banda, retardo, etc.)

CAPITULO 4

APLICACIONES DE LA TECNOLOGIA IP/MPLS EN ETAPA

4.1. SERVICIOS DE VALOR AGREGADO

Las empresas pueden incrementar su productividad y la eficacia de las comunicaciones si su VPN IP utiliza la Tecnología MPLS.

La tecnología MPLS permite dar prioridad a las aplicaciones empresariales críticas y sensibles al tiempo, respecto al tráfico menos importante, como el correo electrónico y la navegación por Internet. De este modo, las empresas no tienen que adquirir ancho de banda adicional para poder gestionar los picos de tráfico, al mismo tiempo, mejorar el rendimiento de las aplicaciones empresariales críticas. Así mismo, las Redes VPN IP ofrecen una plataforma de convergencia para las aplicaciones de Voz y Datos, y admiten aplicaciones multimedia, como las Videoconferencias.

ETAPA con su backbone IP/MPLS puede ofrecer distintos tipos de servicios a sus clientes como:

- Internet de banda ancha
- Internet Inalámbrica de banda ancha
- Servicio de xDSL: ADSL, SDSL
- Servicio de videoconferencias de muy alta calidad, gracias la baja latencia que proporciona su Backbone
- Servicios de VOZ IP
- Servicio de Carrier, gracias a la gran capacidad de su Backbone
- Ingeniería de trafico en sus enlaces, permitiendo a las aplicaciones y a los usuarios pedir y recibir un nivel de servicio previsible para cada tipo de trafico
- Conectividad con cualquier red, esto es Frame Relay, ATM, IP, etc
- Ofrecemos a los usuarios clases de servicios diferenciadas, los mismos que los hemos clasificado en cuatro tipos:

Clase de Tráfico	*Tipo de Tráfico*	*Ejemplos*
Cos 1	*Voz*	*Voz sobre IP*
Cos 2	*Aplicaciónes de gestión muy solicitadas*	*Aplicaciónes transaccionales*
Cos 3	*Aplicaciónes de gestión criticas*	*Aplicaciónes con BBDD, aplicación de gestion comercial*
Cos 4	*Aplicaciónes de gestión estándar*	*Trnasferecia de fichero Transferencia en batch, email navegacion por la web y replicacion de base de datos*

Tabla 4.1 Clases de Servicios Diferenciados

VPNs EN LAS SIGUIENTES MODALIDADES:

Host to LAN

Donde los usuarios remotos de una empresa se pueden conectar a la misma y acceder a datos corporativos, aplicaciones, impresoras, etc. Tienen esta necesidad empresas con gran número de trabajadores que se desplazan geográficamente en su trabajo habitual y que necesitan conectarse con la Central, o empresas con teletrabajadores.

Como por ejemplo: Utilizando túneles PPTP para conectar un Host remoto con una estación de trabajo en una compañía cualquiera.

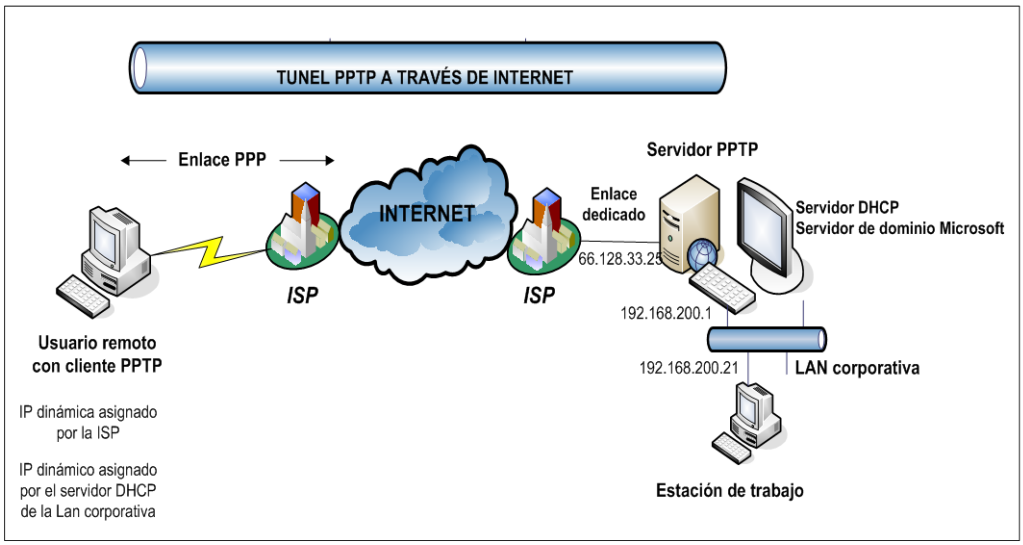


Figura 4.1 Red VPN de Host to Lan

Para esto necesitaremos los siguientes equipos:

- Un computador P4 1.8Ghz, 384MB RAM, 40GB. Actuando como servidor de dominio principal bajo Windows 2000 Server, DHCP Server, WINS Server, PPTP Server (PNS).
- Un computador genérico, P2 350Mhz, 192MB RAM, 12GB, actuando como estación de trabajo Windows2000 dentro del dominio principal.
- Un computador genérico Celeron 1.0GHz, 192MB, 40GB, con Windows XP Home Edition, actuando como cliente PPTP nativo.

LAN to LAN

Esta solución es la ideal para medianas y grandes empresas que tienen la necesidad de conectar las redes locales de sus agencias, que se encuentran separadas geográficamente con su Matriz. Con esta solución se puede ahorrar costes en comunicaciones como licencias de aplicaciones, tiempo, etc.; al poder acceder a los recursos de todas las redes conectadas en forma transparente.

Como por ejemplo: Utilizando túneles IPSec para conectar dos redes LAN separadas geográficamente.

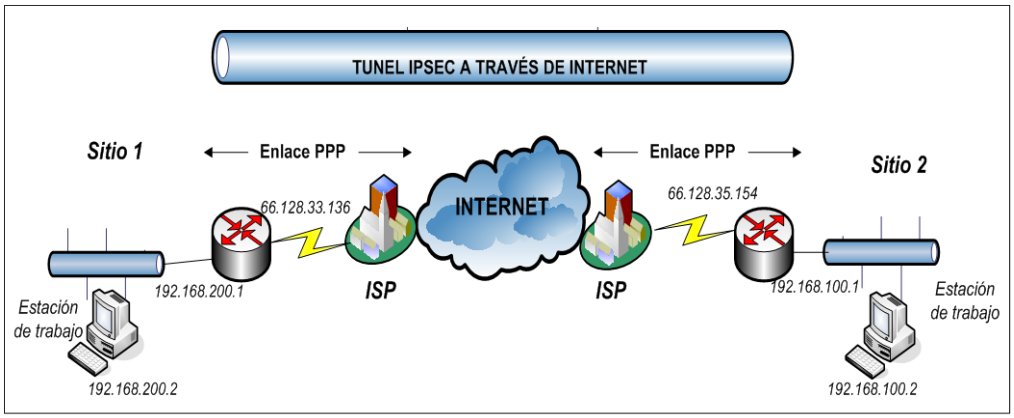


Figura 4.2 Red VPN de LAN to LAN

Para esto necesitaremos los siguientes equipos:

- Dos routers Cisco 1760, con interfaces WIC-1B S/T (puerto ISDN BRI), e IOS C1700-K9SV3Y7-M, Versión 12.2(11)T con cifrado DES.

- Un computador P4 1.8Ghz, 384MB RAM, 40GB, actuando como estación de trabajo en la LAN corporativa Sitio1.
- Un computador genérico Celeron 1.0GHz, 192MB, 40GB, actuando como estación de trabajo en la LAN corporativa Sitio2.

4.2. COMERCIO ELECTRONICO

El término “comercio electrónico” se refiere a la venta de productos y servicios por Internet. Actualmente, este segmento presenta el crecimiento más acelerado de la economía. Gracias al costo mínimo que engloba, hasta la empresa más pequeña puede llegar a clientes de todo el mundo con sus productos y mensajes que hace muchos años era imposible, ahora se tiene la posibilidad de comprar y vender en línea.

Es muy común referirse al comercio electrónico con el término *e-commerce*, pero existen variantes de comercio electrónico que dependen de la modalidad o naturaleza de la transacción.

Dichas variantes son identificadas como:

- B2B.- Business to Business (Negocio a Negocio). Es la modalidad de comercio electrónico destinado al comercio de mayoreo. Se caracteriza por el manejo de grandes volúmenes

de mercancía, un mayor flujo de datos y enormes cantidades monetarias; todo aquello que precisamente se encontraría cuando las empresas hacen negocio con las empresas. Se manejan precios especiales por volumen, e inclusive por cliente (precios negociados). Puede o no recurrirse a un método de pago en línea y el proceso puede ser llevado automáticamente o involucrando personal. El proveedor de este servicio de comercio electrónico actúa más como un medio de transacción que como una tienda.

- B2C.- Business to Consumer (Negocio a Consumidor). Es el más común para la mayoría de los usuarios de la Internet. Los precios son usualmente menores que los que se encuentran en la calle pero no son de mayoreo. Está enfocado a la venta en menudeo y para personas físicas. Los métodos de pago en línea están convirtiéndose en obligados en la actualidad.
- B2G.- Business to Government (Negocio a Gobierno). Únicamente ventas a gobiernos locales, municipales y estatales es lo que contempla. Aplica reglas muy particulares para la licitación de contratos o la enajenación de bienes y servicios. El volumen y monto de ventas es el principal atractivo. Usualmente no hay pago en línea, pero la tendencia es incorporarlo.

- B2E.- Business to Employee (Negocio a Empleado). Esta modalidad está vista como un medio para el ofrecimiento de prestaciones y beneficios que la compañía puede ofrecer a sus empleados. Usualmente son tiendas virtuales que sólo pueden ser vistas en la Intranet de la organización. Formas de pago on-line están disponibles junto con la posibilidad de descuentos por nómina u otros esquemas.

Las empresas centradas en el comercio electrónico comenzaron hace más de dos décadas con la introducción del intercambio electrónico de datos (EDI) entre firmas comerciales (envío y recibo de pedidos, información de reparto y pago, etc.) Incluso el comercio electrónico orientado al consumidor tiene también una larga historia: cada vez que utiliza un cajero automático o presenta una tarjeta de crédito, está efectuando una transacción electrónica. EDI y ATM, sin embargo, operan en un sistema cerrado; son un medio de comunicación más conveniente, estrictamente entre las partes involucradas. Mediante las VPN IP/MPLS se puede brindar este tipo de transacciones a nivel de toda la red de ETAPA otorgando seguridad desde el router de la empresa proveedora de Internet (ETAPA) hasta el servidor Web de la empresa que da el servicio de comercio electrónico.

En el comercio electrónico se deben plantear cuestiones que van, desde

la validez legal de las transacciones y contratos sin papel, la necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio, el control de las transacciones internacionales, incluido el cobro de impuestos; la protección de los derechos de propiedad intelectual, la protección de los consumidores en cuanto a publicidad engañosa o no deseada, fraude, contenidos ilegales y uso abusivo de datos personales, hasta otros provocados por la dificultad de encontrar información en Internet, comparar ofertas y evaluar la fiabilidad del vendedor y del comprador en una relación electrónica, la falta de seguridad de las transacciones y medios de pago electrónicos, la falta de estándares consolidados, la proliferación de aplicaciones y protocolos de comercio electrónico incompatibles y la congestión de Internet.

Privacidad y seguridad: La mayoría de los usuarios no confía en el Internet como canal de pago. En la actualidad, las compras se realizan utilizando el número de la tarjeta de crédito, pero aún no es seguro introducirlo en Internet sin conocimiento alguno. Cualquiera que transfiera datos de una tarjeta de crédito mediante el Web, no puede estar seguro de la identidad del vendedor. Análogamente, éste no lo está sobre la del comprador. Quien paga no puede asegurarse de que su número de tarjeta de crédito no sea recogido y sea utilizado para algún propósito malicioso; por otra parte, el vendedor no puede

asegurar que el dueño de la tarjeta de crédito rechace la adquisición. Resulta irónico que existan y funcionen correctamente los sistemas de pago electrónico para las grandes operaciones comerciales, mientras que los problemas se centren en las operaciones pequeñas, que son mucho más frecuentes.

Por tales motivos se han desarrollado sistemas de seguridad para transacciones por Internet: Encriptación, Firma Digital y Certificado de Calidad, que garantizan la confidencialidad, integridad y autenticidad respectivamente.

Con la encriptación la información transferida solo es accesible por las partes que intervienen (comprador, vendedor y sus dos bancos).

La firma digital, evita que la transacción sea alterada por terceras personas sin saberlo.

El certificado digital, que es emitido por un tercero, garantiza la identidad de las partes.

Lo que hacen las VPN es asegurar que la información que viaja a través de Internet no sea fácilmente detectada y leída,

Cuestiones legales, políticas y sociales: Existen algunos aspectos abiertos en torno al comercio electrónico: validez de la firma electrónica,

no repudio, legalidad de un contrato electrónico, violaciones de marcas y derechos de autor, pérdida de derechos sobre las marcas, pérdida de derechos sobre secretos comerciales y responsabilidades. Por otra parte, deben considerarse las leyes, políticas económicas y censura gubernamentales

CAPITULO 5

DISEÑO DE UNA RED VPN IP/MPLS

5.1. DISEÑO DE LA RED

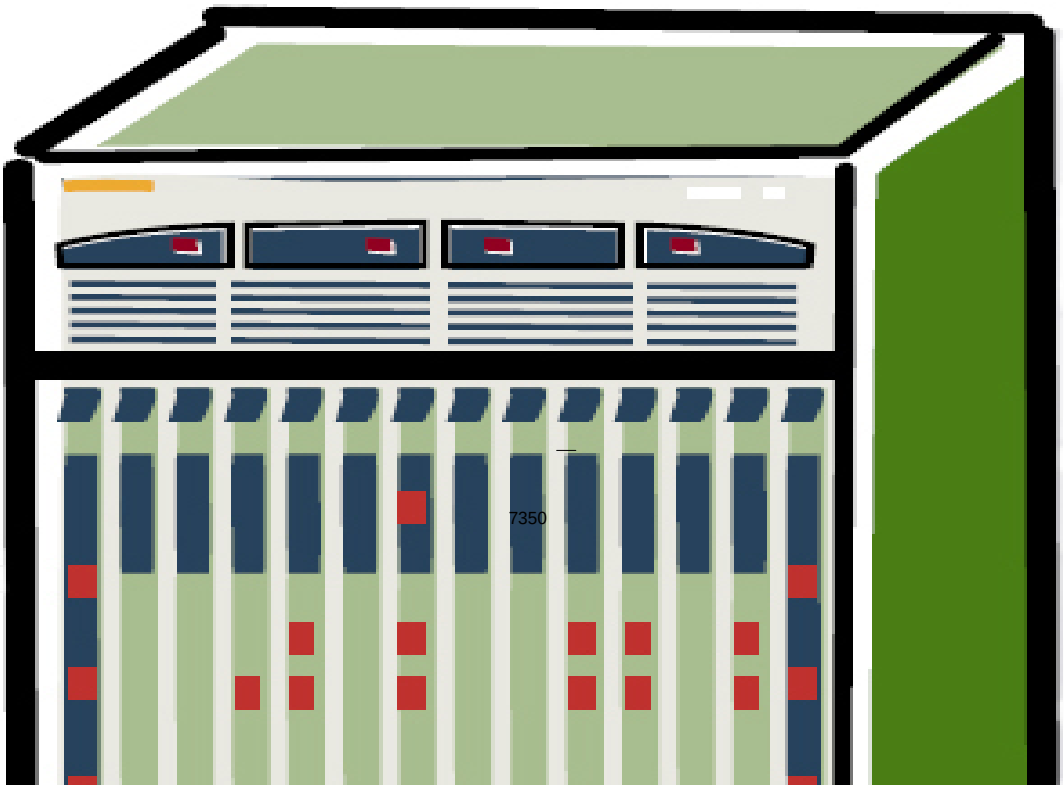
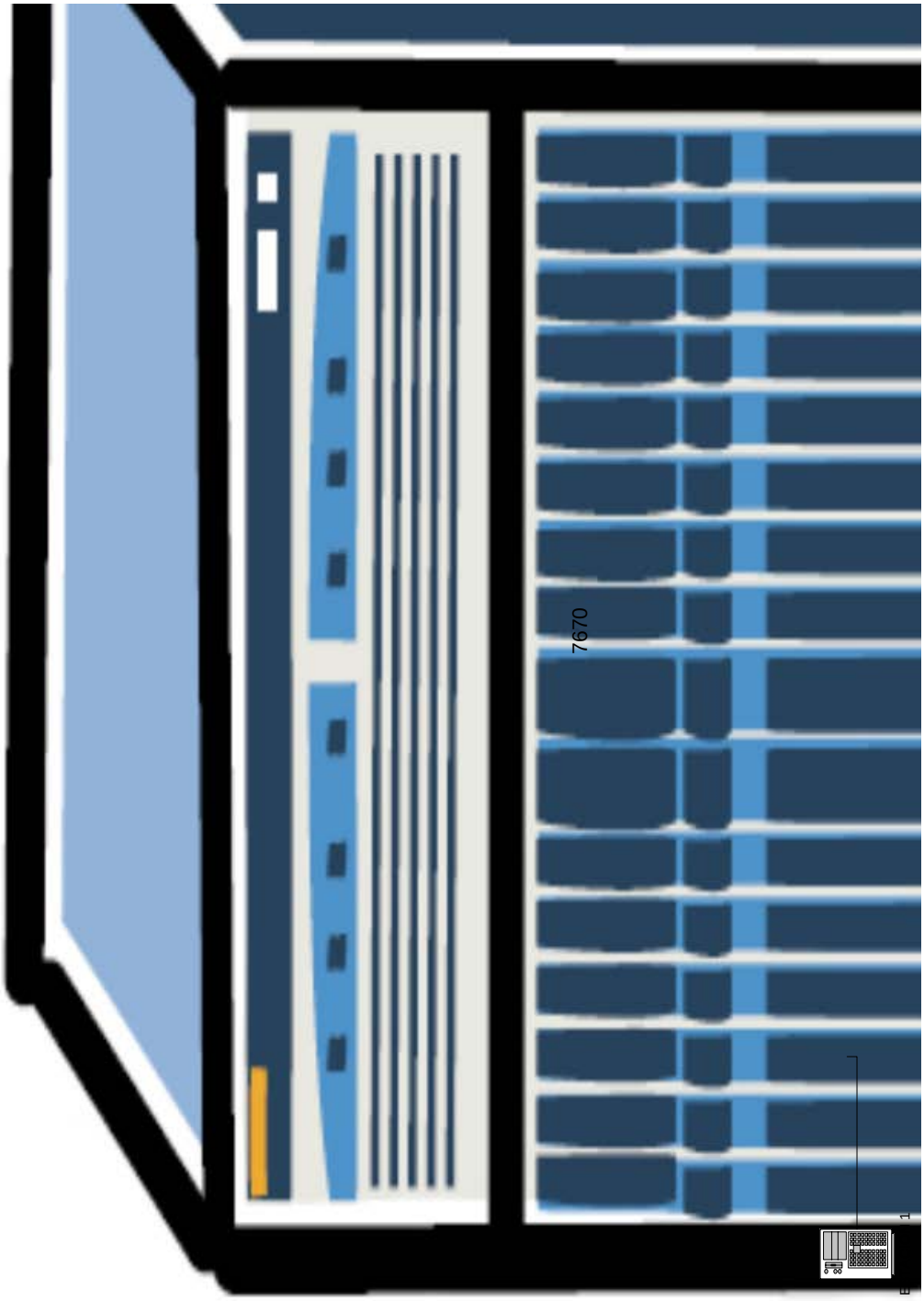


Figura 5.1 Red ETAPA ATM


7670

En el diseño de nuestra red se utilizo un equipo ALCATEL como nuestro Backbone IP/MPLS el mismo que soporta ATM, IP y MPLS en un mismo shelf.

La integración del multiprotocolo IP/MPLS/ATM del Alcatel 7670 minimiza el riesgo asociado con cualquier tecnología sola. Además, la plataforma posibilita interoperar entre los protocolos para permitir la migración.

El Alcatel 7670 RSP soporta una arquitectura de estante solo o de multiestante, que consta de los siguientes estantes: El estante periférico (PS o “el estante 50Gig”) el Estante de Conmutación (SS), el Estante periférico de alta velocidad (HSPS) y Estante de extensión para Servicios de borde (ESE).

Para lo cual se eligió la configuración stanalone PS, la misma que se describe a breves rasgos a continuación:

Estante periférico (PS o “el estante 50Gig”): Este estante puede ser usado en aplicaciones standalone o como parte de un sistema multiestante. Tiene 14 ranuras, y pueden acomodar hasta 224 puertos de STM-1/OC-3/DS3, o 56 puertos STM-4/OC-12, o 14 puertos STM-16/OC-48, o 56 puertos GigE. Cualquier mezcla de tipos de interfaz puede ser soportada. Cuando la expansión es precisada, el estante solo

puede transformarse en parte de un sistema multiestante. Esta conversión es lograda sin impacto de servicio.

Donde la configuración del 7670 RSP es la siguiente:

1 tarjeta IP/ATM de 4 puertos STM-1

2 tarjetas IP/ATM de 8 puertos OC-3c/STM-1

1 tarjeta IP/ATM de 1 puerto OC-12c/STM-4

1 tarjeta GigE de 2 puertos

1 tarjeta POS de 1 puerto OC-48c/STM-16

DISEÑO DE LA RED VPN AL CLIENTE SERICORP

En la figura 5.4 puede verse el diseño de la red del cliente ServiCorp unida al Backbone IP/MPLS de Etapa. Este cliente va a contar con una VPN MPLS y una VPN basada en IPSec para sus enlaces fuera del Backbone de ETAPA.

La organización ServiCorp tiene sucursales en Guayaquil, Quito, y Cuenca. La matriz y la sucursal de Cuenca tienen servicio de VPN de Intranet, mientras que la matriz y las sucursales de Guayaquil (GYQ) y Quito (UIO) tienen un servicio VPN de extranet.

ROUTER	DIRECCION IP
Matriz	200.0.4.1
Sucursal Cuenca	200.0.6.1
Sucursal GYQ	200.0.9.1
Sucursal UIO	200.0.3.1

Para suministrar el servicio de VPN de intranet, a través del Backbone de ETAPA se sigue estos pasos:

1. Defina y configure las VRF
2. Defina y configure los distintivos de ruta
3. Define y configure las normas de importación y exportación
4. Configure los enlaces PE y CE
5. Configure multiprotocolo BGP

Todas las configuraciones de los routers que a continuación se mostrarán para que funcione la VPN MPLS/IP se basa en las direcciones IP de la figura 5.3.

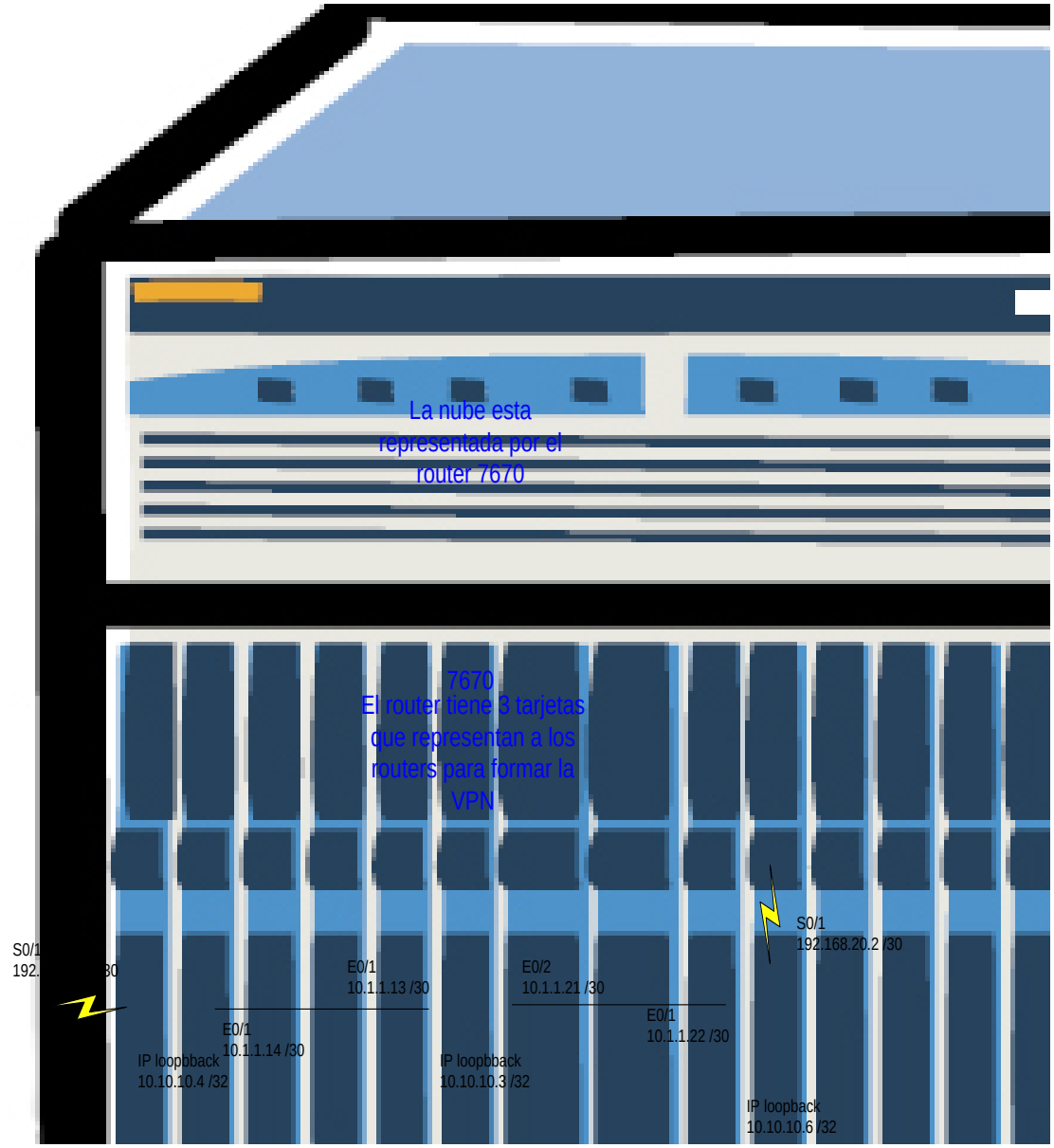


Figura 5.3 Nube del Backbone MPLS

CONFIGURACION - ROUTER ETAPA NORTE

```
Current configuration:
!
version 12.2
!
hostname Etapa_Norte
!
ip cef
!
ip vrf ServiCorp
 rd 100:110
route-target export 100:110
route-target import 100:110
!
interface Loopback0
 ip address 10.10.10.4 255.255.255.255
!
interface Serial0/1
description ** interface a SeviCorp Matriz**
ip vrf forwarding ServiCorp
ip address 192.168.10.2 255.255.255.252
!
interface Ethernet0/1
description link to Router P
ip address 10.1.1.14 255.255.255.252
tag-switching ip
!
router bgp 100
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 10.10.10.6 remote-as 100
 neighbor 10.10.10.6 update-source Loopback0
!
 address-family vpnv4
 neighbor 10.10.10.6 activate
 neighbor 10.10.10.6 send-community both
 exit-address-family
 !
 address-family ipv4 vrf ServiCorp
 redistribute static
 no auto-summary
 no synchronization
 network 200.0.4.0 mask 255.255.255.0
```

```
network 192.168.10.0 mask 255.255.255.252
exit-address-family
!
ip classless
!
ip route 200.0.4.0 255.255.255.0 Serial0/1 192.168.10.1
ip route vrf ServiCorp 0.0.0.0 0.0.0.0 192.168.67.1 global
!
ip route vrf ServiCorp 200.0.4.0 255.255.255.0 192.168.10.1
!
end
```

CONFIGURACION - ROUTER ETAPA SUR

```
Current configuration:
!
version 12.2
!
hostname Etapa_Sur
!
ip cef
!
ip vrf ServiCorp
 rd 100:110
route-target export 100:110
route-target import 100:110
!
interface Loopback0
 ip address 10.10.10.6 255.255.255.255
!
interface Serial0/1
description ** interface a ServiCorp Sucursal Cuenca**
ip vrf forwarding ServiCorp
ip address 192.168.20.2 255.255.255.252
!
interface Ethernet0/1
description link to Router P
ip address 10.1.1.22 255.255.255.252
tag-switching ip
!
router bgp 100
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
```

```
 neighbor 10.10.10.4 remote-as 100
 neighbor 10.10.10.4 update-source Loopback0
!
 address-family vpnv4
 neighbor 10.10.10.4 activate
 neighbor 10.10.10.4 send-community both
 exit-address-family
 !
 address-family ipv4 vrf ServiCorp
  redistribute static
 no auto-summary
 no synchronization
 network 200.0.6.0 mask 255.255.255.0
network 192.168.20.0 mask 255.255.255.252
  exit-address-family
 !
 ip classless
 ip route 200.6.0.0 255.255.255.0 Serial0/1 192.168.20.1
ip route vrf ServiCorp 0.0.0.0 0.0.0.0 192.168.67.1 global
! routes
ip route vrf ServiCorp 200.6.0.0 255.255.255.0 192.168.20.1
!
 end
```

CONFIGURACION ROUTER MATRIZ Cuenca

```
version 12.2
!
hostname Servicorp Matriz
!
ip subnet-zero
!
interface Loopback0
 ip address 200.0.4.1 255.255.255.0
!
!
interface Serial0/1
 ip address 192.168.10.1 255.255.255.252

 !
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.10.2
```

CONFIGURACION ROUTER SUCURSAL Cuenca

```
version 12.2
!
hostname ServiCorp Sucursal Cuenca
!
ip subnet-zero
!
interface Loopback0
 ip address 200.6.0.1 255.255.255.0
!
interface Serial0/1
 ip address 192.168.20.1 255.255.255.252
 !
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.20.2
```

CONFIGURACION DE ROUTER P

```
version 12.2
!
hostname Router_P
!
ip subnet-zero
!
ip cef
!
interface Loopback0
 ip address 10.10.10.3 255.255.255.255
!
interface Ethernet0/1
 ip address 10.1.1.13 255.255.255.252
 tag-switching ip
!
interface Ethernet 0/2
 ip address 10.1.1.21 255.255.255.252
 tag-switching ip

interface Ethernet0/3
 ip address 200.109.55.1 255.255.255.0
 tag-switching ip
!
```

Para suministrar el servicio de VPN de extranet, a través de la VPN basada en IPSec siga los siguientes pasos:

Configuración Router linux GYQ

Configuración Router linux UIO

Configuración Router linux Matriz

Configuración Gateway VPN Matriz

Configuración Gateway VPN GYQ

Configuración Gateway VPN UIO

Equipos Utilizados:

- Un computador clone P4 1.8Ghz, 384MB RAM, 40GB, actuando como Server Gateway VPN, con Linux RedHat 9.0.
- Un computador clone 1.2GHz, 256MB, 40GB, actuando como Server Gateway VPN, con Linux RedHat 9.0.
- Un computador clone 1.2GHz, 256MB, 40GB, actuando como Server Gateway VPN, con Linux RedHat 9.0.

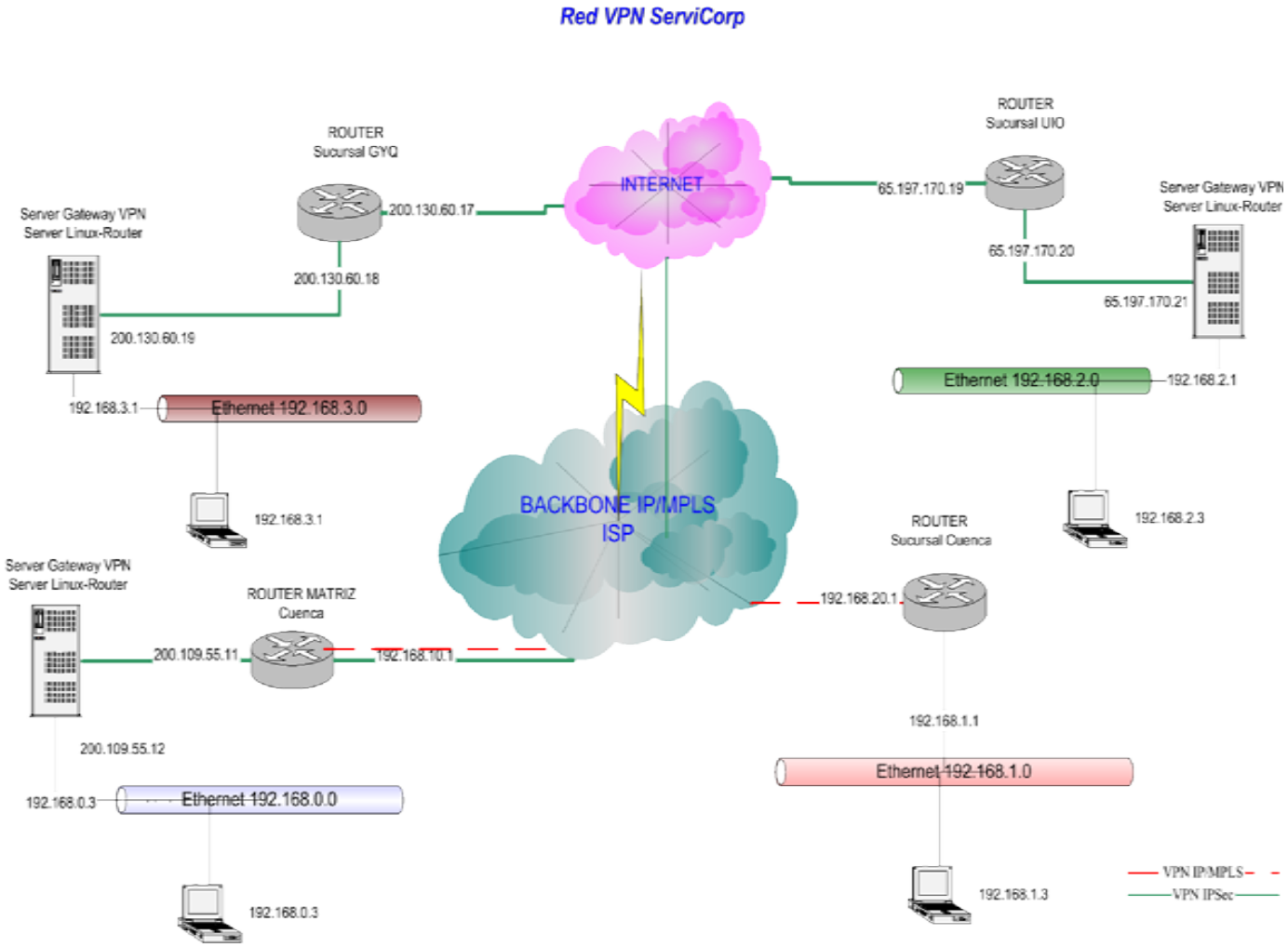


Figura 5.4 Red del Cliente ServiCorp

INSTALACION Y CONFIGURACION

FreeS/WAN25 es una implementación Linux del protocolo IPSec que brinda servicios de cifrado y autenticación a conexiones IP.

FreeS/WAN convierte una máquina Linux en un gateway seguro IPSec, permitiendo implementar topologías LAN-to-LAN.

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

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

Las fuentes de FreeS/WAN se pueden obtener de la siguiente dirección: ftp://ftp.xs4all.nl/pub/crypto/freeswan/

Si la distribución es RedHat, se pueden descargar los RPMs de la siguiente dirección:

ftp://ftp.xs4all.nl/pub/crypto/freeswan/binaries/RedHat-RPMs

Antes de proceder a descargar el software es necesario determinar el kernel con el que se cuenta, para esto se ejecuta el comando:

uname –a

Una vez hecho este paso se comienza la descarga de la respectiva RPM (en este caso el kernel con el que se trabaja es 2.4.20-8). Los archivos descargados fueron:

freeswan-module-2.00_2.4.20_8-0.i386.rpm

freeswan-userland-2.00_2.4.20_8-0.i386.rpm

Es necesario también bajar la firma digital contenida en el archivo freeswan-rpmsign.asc que sirve para comprobar la autenticidad de los RPMs descargados. Para lo anterior se ejecuta el comando: rpm --checksig freeswan*.rpm y la salida deberá ser:

freeswan-module-2.00_2.4.20_8-0.i386.rpm: pgp md5 OK

freeswan-userland-2.00_2.4.20_8-0.i386.rpm: pgp md5 OK

Para instalar las RPMs es necesario tener privilegios de administrador de la máquina. Para proceder con la instalación se ejecuta el comando: rpm -ivh freeswan*.rpm

Una vez finalizada la instalación, se inicia el servicio con el comando:

service ipsec Start

y para probar la instalación se ejecuta el comando:

ipsec verify

La salida deberá ser OK para al menos las 4 primeras líneas, así:

Checking your system to see if IPsec got installed and started correctly
Version check and ipsec on-path [OK]
Checking for KLIPS support in kernel [OK]
Checking for RSA private key (/etc/ipsec.secrets) [OK]
Checking that pluto is running [OK]

Una vez comprobada la adecuada instalación del paquete, se procede a la configuración de los archivos /etc/ipsec.conf y /etc/ipsec.secrets.
Hay que aclarar que cada Server Gateway VPN debe tener un IP estático dado por el ISP, bien sea en una interfaz ppp (por ejemplo ppp0) o en una interfaz ethernet (por ejemplo eth0).

A cada Server Gateway VPN se le debe asignar por nomenclatura como right o left, indistintamente de cual escoja para cada nombre.

En nuestro caso los Server Gateway VPN asignados como left serán las Sucursales y el Server Gateway VPN asignado como right será la Matriz. Lo importante es ser congruente con esta nomenclatura a lo largo del proceso de configuración del archivo /etc/ipsec.conf.

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

La parte más importante del archivo /etc/ipsec.conf es la que define cada conexión IPSec, de hecho todas las opciones en la sección config setup son opcionales. Los campos básicos que define cada pareja IPSec son:

left=

leftsubnet=

leftnexthop=

leftrsasigkey=

right=

rightsubnet=

rightnexthop=

rightrsasigkey=

auto=

Los campos left y right son las direcciones IP públicas de cada Server Gateway VPN.

Los campos leftsubnet y rightsubnet son las subredes que se encuentran detrás de cada Server Gateway VPN (la red privada).

Los campos leftnexthop y rightnexthop son las direcciones IP del equipo que recibe la conexión en el ISP. Es la puerta de enlace de cada máquina Linux.

Los campos leftrsasigkey y rigthrsasigkey son las llaves públicas de cada gateway IPSec, y se obtienen con los comandos:

ipsec showhostkey --left (para la máquina llamada left), y

ipsec showhostkey --right (para la máquina llamada right).

En caso de no contar con estas llaves, se puede generar cada una de ellas con el comando:

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

Los archivos /etc/ipsec.conf con los cuales debe trabajar la implementación son:

```
[root@Matriz root]# more /etc/ipsec.conf
version  2.0     # conforms to second version of ipsec.conf specification

# basic configuration
config setup
# Debug-logging controls:  "none" for (almost) none, "all" for lots.

interfaces=%defaultroute
klipsdebug=none
plutodebug=none
uniqueids=yes

# Add connections here.
conn %default
keyingtries=0
authby=rsasig

conn Matriz-SucursalGYQ
left= 200.130.60.19
leftsubnet=192.168.3.0/24
leftnexthop=200.130.60.18

leftrsasigkey=0sAQOHbmJjlOUboH6IEm9alDzc7fvV0xxGCZV2iNrOJ4y
UfSok2Plvw8fCAERzZcmOy53tE1E71Qkuz6qVZpsFbW0GfyEiJyws9/g
SD3khJtLK2/3tQxkOGN+d1vJYQdlbpf0+EMCX8HSp/9sCR86G7wuMYT
bNtuRh1Sl6GTDGfuJ2Xn/lULIOOX1DmtdNzdFPrvKpC3bQWocE3Mum
V96Bkumutm49UhLiOa3FGn0699HbcJLh1glMoOb+EJ8in8glfTTDU4ad
bq5Z0wvnOlAc46gAkWLffOeeWgUQtT/KA4wVLp5RYqXgX43ytSPF5o
MLsXApVcTuClbXg+u+ctfEcbfCkNRr8Fvk0C1KgDicq4/LN2P9

right=200.109.55.12
rightsubnet=192.168.0.0/24
rightnexthop=200.109.55.11
```

rightrsasigkey=0sAQNj25OiRTaMkDn1S/SdzXeRD0zQfXUPnsBQaXDtk
vqTcCVaefJ5DUGZM8Nli796pDvsP0W9OMis25so1whsYygkzYsacrZIlw
yr+GvRDIf8xarV2YqvGDs0wvyk22891h4twzGD9yfFwgfUBEysMmGpJn
GrNxFEL9TDggp9A3UeCBx+qgYv9CCWjgPXYfzKomP3tHtiB7gUTgIBlp
xTva1Gs4rM9IJIUUNBwfpuNDglD23KMibWBQn1YTPsJ9mQccIBaHao4
3EkM2BHRG6KbNYGD8GQ7DGbd95QLXzjdASeCc0t9TrtOI7cwxGxs6
LF3NQRZrCKH1sE1OsTIkacYHxIOQ/dN53CpPMKhNQR4tl7Jm8t
auto=start

conn Matriz-SucursalUIO
left=65.197.170.21
leftsubnet=192.168.2.0/24
leftnexthop=65.197.170.20

leftrsasigkey=0sAQNc5aRo4JhtphC+FsWzBJ/AFjn5qDUh5kk7I21StG2K
ngpffp61pQH9fGtf73iCrBIX5CxM8h5hQOTdZj98+fq4rkSKI1sQn+FGvM
E4yqKb8ttLeyLwzq9ZH4M5CgOdBX3VbELO3Zt1aZnbXV3WR1CFT83n
QEtpIIcYrv6lCnltXJH9TFm7/qXRbSA9iwpXk2jx3MgM83eii0VY5cV+0yG
J25W1fcUftlYZgEVUDb6lQMQ1itp4rAxc7rnviyQTltPkFxNUpsLanA8KdU
6OiYH/+rg/RM0915fzk9SsjPndQMHyOy0hDNC74tpmOsDUWGbA/zZIa
TbJ13KNcZjDu0wS+QFLkRjHZD00hmqJA7AmTrWx

right=200.109.55.12
rightsubnet=192.168.0.0/24
rightnexthop=200.109.55.11

rightrsasigkey=0sAQNj25OiRTaMkDn1S/SdzXeRD0zQfXUPnsBQaXDtk
vqTcCVaefJ5DUGZM8
Nli796pDvsP0W9OMis25so1whsYygkzYsacrZIlwyr+GvRDIf8xarV2YqvG
Ds0wvyk22891h4twzGD9yfFwgfUBEysMmGpJnGrNxFEL9TDggp9A3U
eCBx+qgYv9CCWjgPXYfzKomP3tHtiB7gUTgIBlpxTva1Gs4rM9IJIUUNB
wfpuNDglD23KMibWBQn1YTPsJ9mQccIBaHao43EkM2BHRG6KbNYG
D8GQ7DGbd95QLXzjdASeCc0t9TrtOI7cwxGxs6LF3NQRZrCKH1sE1O
sTIkacYHxIOQ/dN53CpPMKhNQR4tl7Jm8t
auto=start

#sample# VPN connection
#sample# conn sample
#sample# # Left security gateway, subnet behind it, next hop toward right.
#sample# left=10.0.0.1
#sample# leftsubnet=172.16.0.0/24
#sample# leftnexthop=10.22.33.44

```
#sample#                # Right security gateway, subnet behind it, next
                         hop toward left.
#sample#                right=10.12.12.1
#sample#                rightsubnet=192.168.0.0/24
#sample#                rightnexthop=10.101.102.103
#sample#                # To authorize this connection, but not actually
                         start it, at startup,
#sample#                # uncomment this.
#sample#                #auto=start


[root@SucursalGYQ root]# more /etc/ipsec.conf

version  2.0     # conforms to second version of ipsec.conf specification

# basic configuration
config setup
# Debug-logging controls:  "none" for (almost) none, "all" for lots.

interfaces=%defaultroute
klipsdebug=none
plutodebug=none
uniqueids=yes

# Add connections here.
conn %default
keyingtries=0
authby=rsasig
conn Matriz-SucursalGYQ

left=200.130.60.19
leftsubnet=192.168.3.0/24
leftnexthop=200.130.55.11

leftrsasigkey=0sAQOHbmJjlOUboH6IEm9alDzc7fvV0xxGCZV2iNrOJ4y
UfSok2Plvw8fCAERzZcmOy53tE1E71Qkuz6qVZpsFbW0GfyEiJyws9/g
SD3khJtLK2/3tQxkOGN+d1vJYQdlbpf0+EMCX8HSp/9sCR86G7wuMYT
bNtuRh1Sl6GTDGfuJ2Xn/lULIOOX1DmtdNzdFPrvKpC3bQWocE3Mum
V96Bkumutm49UhLiOa3FGn0699HbcJLh1glMoOb+EJ8in8glfTTDU4ad
bq5Z0wvnOlAc46gAkWLffOeeWgUQtT/KA4wVLp5RYqXgX43ytSPF5o
MLsXApVcTuClbXg+u+ctfEcbfCkNRr8Fvk0C1KgDicq4/LN2P9

right=200.109.55.12
rightsubnet=192.168.0.0/16
```

```
rightnexthop=200.109.55.11

rightrsasigkey=0sAQNj25OiRTaMkDn1S/SdzXeRD0zQfXUPnsBQaXDtk
vqTcCVaefJ5DUGZM8
Nli796pDvsP0W9OMis25so1whsYygkzYsacrZIlwyr+GvRDIf8xarV2YqvG
Ds0wvyk22891h4twzGD9yfFwgfUBEysMmGpJnGrNxFEL9TDggp9A3U
eCBx+qgYv9CCWjgPXYfzKomP3tHtiB7gUTgIBlpxTva1Gs4rM9IJIUUNB
wfpuNDglD23KMibWBQn1YTPsJ9mQccIBaHao43EkM2BHRG6KbNYG
D8GQ7DGbd95QLXzjdASeCc0t9TrtOI7cwxGxs6LF3NQRZrCKH1sE1O
sTIkacYHxIOQ/dN53CpPMKhNQR4tl7Jm8t
                auto=start

#sample# VPN connection
#sample#       conn sample
#sample#                # Left security gateway, subnet behind it, next hop
                         toward right.
#sample#                left=10.0.0.1
#sample#                leftsubnet=172.16.0.0/24
#sample#                leftnexthop=10.22.33.44
#sample#                # Right security gateway, subnet behind it, next
                         hop toward left.
#sample#                right=10.12.12.1
#sample#                rightsubnet=192.168.0.0/24
#sample#                rightnexthop=10.101.102.103
#sample#                # To authorize this connection, but not actually
                         start it, at startup,
#sample#                # uncomment this.
#sample#                #auto=start


[root@SucursalUIO root]# more /etc/ipsec.conf

version  2.0     # conforms to second version of ipsec.conf specification

# basic configuration
config setup
# Debug-logging controls:  "none" for (almost) none, "all" for lots.

interfaces=%defaultroute
klipsdebug=none
plutodebug=none
uniqueids=yes

# Add connections here.
```

```
conn %default
keyingtries=0
authby=rsasig

conn Matriz-SucursalUIO
left=65.109.170.21
leftsubnet=192.168.2.0/24
leftnexthop=65.109.170.20

leftrsasigkey=0sAQNc5aRo4JhtphC+FsWzBJ/AFjn5qDUh5kk7I21StG2K
ngpffp61pQH9fGtf73iCrBIX5CxM8h5hQOTdZj98+fq4rkSKI1sQn+FGvM
E4yqKb8ttLeyLwzq9ZH4M5CgOdBX3VbELO3Zt1aZnbXV3WR1CFT83n
QEtpIIcYrv6lCnltXJH9TFm7/qXRbSA9iwpXk2jx3MgM83eii0VY5cV+0yG
J25W1fcUftlYZgEVUDb6lQMQ1itp4rAxc7rnviyQTltPkFxNUpsLanA8KdU
6OiYH/+rg/RM0915fzk9SsjPndQMHyOy0hDNC74tpmOsDUWGbA/zZIa
TbJ13KNcZjDu0wS+QFLkRjHZD00hmqJA7AmTrWx

right=200.109.55.11
rightsubnet=192.168.0.0/16
rightnexthop=200.109.55.12

rightrsasigkey=0sAQNj25OiRTaMkDn1S/SdzXeRD0zQfXUPnsBQaXDtk
vqTcCVaefJ5DUGZM8Nli796pDvsP0W9OMis25so1whsYygkzYsacrZIlw
yr+GvRDIf8xarV2YqvGDs0wvyk22891h4twzGD9yfFwgfUBEysMmGpJn
GrNxFEL9TDggp9A3UeCBx+qgYv9CCWjgPXYfzKomP3tHtiB7gUTgIBlp
xTva1Gs4rM9IJIUUNBwfpuNDglD23KMibWBQn1YTPsJ9mQccIBaHao4
3EkM2BHRG6KbNYGD8GQ7DGbd95QLXzjdASeCc0t9TrtOI7cwxGxs6
LF3NQRZrCKH1sE1OsTIkacYHxIOQ/dN53CpPMKhNQR4tl7Jm8t
                auto=start

#sample# VPN connection
#sample#       conn sample
#sample#               # Left security gateway, subnet behind it, next hop
                       toward right.
#sample#               left=10.0.0.1
#sample#               leftsubnet=172.16.0.0/24
#sample#               leftnexthop=10.22.33.44
#sample#               # Right security gateway, subnet behind it, next
                       hop toward left.
#sample#               right=10.12.12.1
#sample#               rightsubnet=192.168.0.0/24
#sample#               rightnexthop=10.101.102.103
#sample#               # To authorize this connection, but not actually
                       start it, at startup,
```

```
#sample#              # uncomment this.
#sample#              #auto=start
```

Es necesario agregar la línea versión 2.0 en el inicio de cada archivo. La línea auto=start hace que el túnel se establezca durante el proceso de boot de la máquina. Inicialmente, para propósitos de troubleshooting, se recomienda que la línea auto tenga el valor de add, lo cual obliga a que cada vez el administrador inicie el túnel de manera manual y así pueda detectar errores en el establecimiento de la SA. Una vez afinado este procedimiento, la línea auto deberá quedar con el valor start (tal como aparece en el archivo ejemplo) para que el túnel se establezca automáticamente cada vez que la máquina reinicia.

El comando para establecer los túneles de manera manual en la matriz son:

```
ipsec auto --up Matriz-SucursalGYQ
ipsec auto --up Matriz-SucursalUIO
```

Donde Matriz-SucursalGYQ y Matriz-SucursalUIO son los nombres dado a cada pareja IPSec en el archivo /etc/ipsec.conf, y auto indica que las llaves se negocian de forma automática (no manual). No es necesario ejecutar este comando en las maquinas, en una es suficiente.

La salida de este comando deberá mostrar algo como:

```
[root@Matriz root]# ipsec auto --up Matriz-SucursalGYQ
104    "Matriz-SucursalGYQ"    #1:   STATE_MAIN_I1:   initiate
106    "Matriz-SucursalGYQ"    #1:   STATE_MAIN_I2:   sent MI2,       expecting MR2
108    "Matriz-SucursalGYQ"    #1:   STATE_MAIN_I3:   sent MI3,       expecting MR3
004    "Matriz-SucursalGYQ"    #1:   STATE_MAIN_I4:   ISAKMP  SA   established
112    "Matriz-SucursalGYQ"    #2:   STATE_QUICK_I1:  initiate
004      "Matriz-SucursalGYQ"      #2:     STATE_QUICK_I2:     sent     QI2,     IPsec     SA
established

[root@Matriz root]# ipsec auto --up Matriz-SucursalUIO
104    "Matriz-SucursalUIO"    #1:   STATE_MAIN_I1:   initiate
106    "Matriz-SucursalUIO"    #1:   STATE_MAIN_I2:   sent MI2,       expecting MR2
108    "Matriz-SucursalUIO"    #1:   STATE_MAIN_I3:   sent MI3,       expecting MR3
004    "Matriz-SucursalUIO"    #1:   STATE_MAIN_I4:   ISAKMP  SA   established
112    "Matriz-SucursalUIO"    #2:   STATE_QUICK_I1:  initiate
004    "Matriz-SucursalUIO"    #2:   STATE_QUICK_I2:  sent   QI2,   IPsec   SA   established
```

Reglas iptables para la conexión VPN

```
#IKE
iptables -I INPUT -p udp --dport 500 -j ACCEPT
iptables -I FORWARD -p udp --dport 500 -j ACCEPT
#ESP
iptables -I INPUT -p 50 -j ACCEPT
iptables -I FORWARD -p 50 -j ACCEPT
#AH
iptables -I INPUT -p 51 -j ACCEPT
iptables -I FORWARD -p 51 -j ACCEPT
#test ipsec tunel
iptables -A FORWARD -s $all192 -d $local_net -j ACCEPT
iptables -A INPUT -s $all192 -d $local_net -j ACCEPT
iptables -I FORWARD -s 192.168.0.0/16 -d 192.168.0.0/16 -j ACCEPT
iptables -I INPUT -i ipsec0 -s 192.168.0.0/24 -d 192.168.0.0/16 -j
ACCEPT
iptables -I OUTPUT -i ipsec0 -s 192.168.0.0/16 -d 192.168.0.0/16 -j
ACCEPT
```

iptables -I FORWARD -i ipsec0 -s 192.168.0.0/16 -d 192.168.0.0/16 -j ACCEPT

Se vuelve a ejecutar el comando ipsec verify y se verifica la salida:

Para Matriz:

```
[root@Matriz root]# ipsec verify
Checking your system to see if IPsec got installed and started correctly
Version check and ipsec on-path
[OK]
Checking for KLIPS support in kernel
[OK]
Checking for RSA private key (/etc/ipsec.secrets)
[OK]
Checking that pluto is running
[OK]
DNS checks.
Looking for forward key for berkeley.telesat.com.co             [NO KEY]
Does the machine have at least one non-private address          [OK]
Two or more interfaces found, checking IP forwarding            [OK]
```

Para SucursalGYQ:

```
[root@SucursalGYQ root]# ipsec verify
Checking your system to see if IPsec got installed and started correctly
Version check and ipsec on-path
[OK]
Checking for KLIPS support in kernel
[OK]
Checking for RSA private key (/etc/ipsec.secrets)
[OK]
Checking that pluto is running
[OK]
DNS checks.
Looking for forward key for julrodrig                           NO KEY]
Does the machine have at least one non-private address
[OK]
```

Two or more interfaces found, checking IP forwarding
[OK]

Para SucursalUIO:

[root@SucursalUIO root]# ipsec verify
Checking your system to see if IPsec got installed and started correctly
Version check and ipsec on-path
[OK]
Checking for KLIPS support in kernel
[OK]
Checking for RSA private key (/etc/ipsec.secrets)
[OK]
Checking that pluto is running
[OK]
DNS checks.
Looking for forward key for julrodrig [NO KEY]
Does the machine have at least one non-private address
[OK]
Two or more interfaces found, checking IP forwarding
[OK]

Un comando para obtener más información sobre las asociaciones de seguridad que están establecidas en un Server Gateway IPSec es: ipsec look

Dado que la implementación FreeS/WAN no permite realizar ping desde los Server Gateways VPN hasta las máquinas de la red privada remota, las pruebas de conectividad IP se tienen que realizar desde las máquinas que se encuentran detrás de cada Server Gateway VPN. En el escenario montado, se realizó un ping desde el equipo con IP 192.168.0.3 hasta el equipo con IP 192.168.1.3 con resultados fueron satisfactorios.

5.2. VENTAJAS Y DESVENTAJAS DE IP/MPLS

Ventajas:

- IP/MPLS permite crear redes escalables y flexibles con un incremento en el desempeño y la estabilidad.
- Esta tecnología nos permite dar nuevos servicios que antes nos era imposibles dar, debido a su conectividad con múltiples tecnologías.
- MPLS permite establecer trayectorias en función de la carga de la red y de las características de desempeño que se requieran (Ingeniería de Tráfico). También permite Clases de Servicios (CoS) y soporte de VPNs.
- Esta tecnología nos permite tener una mejor Gestión del Backbone, gracias a que integra características de Capa 2 y Capa 3 del modelo OSI. Y no como ocurría con IP ATM donde se tenían que gestionar 2 redes; una infraestructura ATM y una red lógica IP superpuesta.
- En MPLS tan pronto un paquete es asignado a un FEC el análisis del encabezado no es hecho por los routers subsecuentes, a medida que el paquete atraviesa la red MPLS, cada LSR intercambia la etiqueta entrante por una saliente, esto continua hasta alcanzar el LSR de Salida.

- Cada paquete encapsula y acarrea las etiquetas a través de su paso por la trayectoria. La conmutación se efectúa a altas velocidades, debido a que las etiquetas son de una longitud fija, son insertadas al principio del paquete y pueden ser manejadas por hardware para conmutar rápidamente los paquetes entre los enlaces correspondientes
- La diferencia más significativa entre la Tecnología MPLS y la tradicional WAN es la forma como se asignan las etiquetas y la capacidad de transportar una pila de etiquetas adjuntas a un paquete.
- MPLS permite incrementar o decementar el Ancho de Banda de una ruta o LSP según le convenga al Administrador de la Red.
- MPLS es una tecnología que nos permite trabajar con varias tecnologías de transporte como son ATM y Frame Relay en un mismo Backbone.
- Nos permite crear VPN más seguras como las VPN MPLS
- El tráfico se supervisa y gestiona en todo momento, lo que nos permite respaldar el servicio con las garantías de nivel de servicio más completas
- Las aplicaciones críticas y en tiempo real pueden necesitar mayor prioridad que el tráfico por la Intranet

Desventaja:

- IP MPLS es una nueva tecnología y no estandarizada por completo.
- No todos los ISP están dispuesto a invertir en la nueva tecnología de la cual no están familiarizados
- Para poner en marcha todas las aplicaciones que le permite MPLS, necesitaría hacer una fuerte inversión adicional, al reemplazo del Backbone MPLS.
- No se aprovecha por completo toda la capacidad de la tecnología MPLS utilizando tecnología de trasporte ATM. Pudiendo utilizar tecnología de Fibra Óptica como por ejemplo SDH, WDM, etc. para sacarle el máximo beneficio.

5.3. COSTOS

Plan de producción

Los servicios principales que se ofertará a los clientes son: Internet y Servicio de Carrier, dentro de esto tenemos que considerar 4 tipos de clientes:

- *Clientes Internet con Ethernet*, que corresponden a clientes que contratan ambos servicios y que requieren un gran ancho de banda

- *Clientes de Transporte de datos*, que corresponden a clientes que requieren del servicio de carrier para transportar datos de su red.
- *Clientes Dial-up*, corresponden a usuarios que no priorizan el servicio de banda ancha ni tener una conexión permanente.
- *Clientes Internet Dedicado*. En este caso, se ofrecerá el servicio de Internet por medio de un canal dedicado, sea este alámbrico o inalámbrico. Este tipo servicio esta orientado a los cybers y empresas que requieren un ancho de banda considerable para comunicarse con el exterior.

Con el ISP en marcha y totalmente reestructurado, nos dedicamos a la tarea de aumentar la participación del mercado gracias a la incorporación de nuevos servicios, aumento de ancho de banda y a la optimización de nuestro Backbone. Esto se realizará mediante paquetes de productos que incluyan el tipo de servicio, y accesoria técnica personalizada.

El plan de producción general para la captación de nuevos usuarios está dado por la siguiente tabla 5.1:

Años	Cantidad de abonados	% de capacidad Instalada
1	740	20
2	1480	40
3	2220	60
4	2960	80
5	3700	100

TABLA 5.1: Plan de producción a 5 años plazo

En la figura 5.4 se muestra una curva anual de desarrollo en base al crecimiento de nuestros clientes:

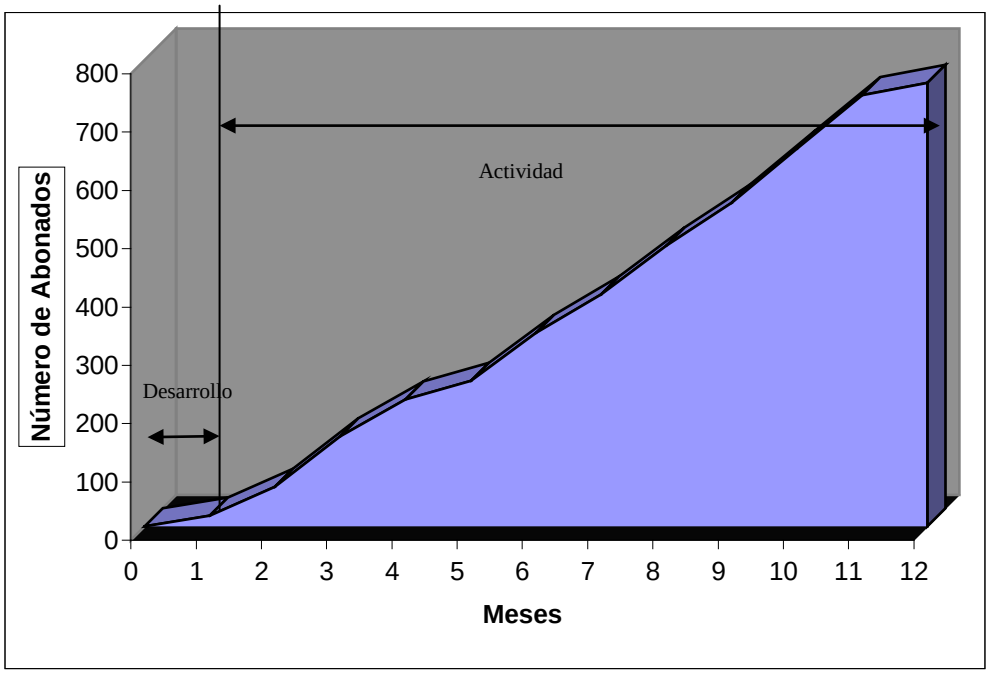


FIGURA 5.5: Curva de crecimiento anual de nuevos clientes

Como se puede ver en al figura 5.4, existe un periodo de un mes en el cual el proyecto estará en fase de implementación, donde no se aumentará significativamente el número de nuevos clientes, luego existirán meses de constante crecimiento del número de clientes, y por último, la curva se estabilizará, una vez cubierto el objetivo (20% de

producción anual), que servirá como preparación para actualizar y mejorar el servicio, a fin de ganar nuevos clientes en el siguiente año.

Análisis de la demanda

En Cuenca, la demanda por el servicio de Internet esta en constante crecimiento y para el servicio de carrier nos encontramos con una demanda insatisfecha, la misma que se pretende satisfacer con el servicio que se oferta.

La tabla 5.2 muestra la frecuencia de acceso que tienen los usuarios de Internet en nuestro país:

FRECUENCIA	**% 2002**	**% 2003**
ALTA: 1 vez al día promedio	28.3	36.2
BAJA: 1 o varias veces por semana	71.7	63.8

TABLA 5.2: Frecuencia de Acceso de usuarios de Internet

La tabla 5.3 muestra los servicios de Internet que se ofrece en el país y el porcentaje de usuarios que lo usa.

SERVICIO	**PORCENTAJE DE USUARIOS**
Dial –up	94%
Líneas dedicadas alámbricas	2%
Cable módem o ADSL	3%
Dedicados inalámbricos	1%

TABLA 5.3: Porcentaje de usuarios de Internet según el servicio

La tabla 5.4 nos muestra el tipo de servicio requerido por los usuarios

USUARIOS	PORCENTAJE DE USUARIOS
Residenciales	92.2 %
Empresariales	2.5 %
De uso público	1 %
Gobierno, educación, otros	4.3 %

TABLA 5.4: Porcentaje Internet según la preferencia de los usuarios

La tabla 5.5 muestra el tipo de servicio que requieren los usuarios residenciales.

SERVICIO	Porcentaje de usuarios residenciales
Dial –up	95.5 %
Líneas dedicadas alámbricas	0.5 %
Cable módem o ADSL	3.5 %
Dedicados inalámbricos	0.5 %

TABLA 5.5: Porcentaje de usuarios residenciales según el servicio

La tabla 5.6 muestra el tipo de servicio que requieren los usuarios empresariales.

SERVICIO	Porcentaje de usuarios empresariales
Internet Dial –up	55.5 %
Internet Líneas dedicadas alámbricas	24.5 %
Internet Cable módem o ADSL	18.8 %
Internet Dedicados inalámbricos	1.2 %
Transporte de datos	22 %

TABLA 5.6: Porcentaje de usuarios empresariales según el servicio

La tabla 5.7 nos muestra el porcentaje de usuarios de Internet, según el ancho de banda.

ANCHO DE BANDA	Porcentaje de Usuarios
Menores a 64 Kbps	62.4 %
Entre 64 Kbps y 128 Kbps	26.8 %
Entre 128 Kbps y 256 Kbps	5.3 %
Entre 256 Kbps y 512 Kbps	3 %
Entre 512 Kbps y 1024 Kbps	1.5 %
Entre 1Mbps y 2 Mbps	1 %
Mayores a 2Mbps	0.1 %

TABLA 5.7: Porcentaje de usuarios de Internet según el ancho de banda

Para analizar las condiciones económicas de los clientes potenciales, observamos la figura 5.5 que muestra la distribución de ingresos que

existe en el país, tomando en cuenta a la Población Económicamente Activa (PEA), que en el país representa el 35% de la población total.

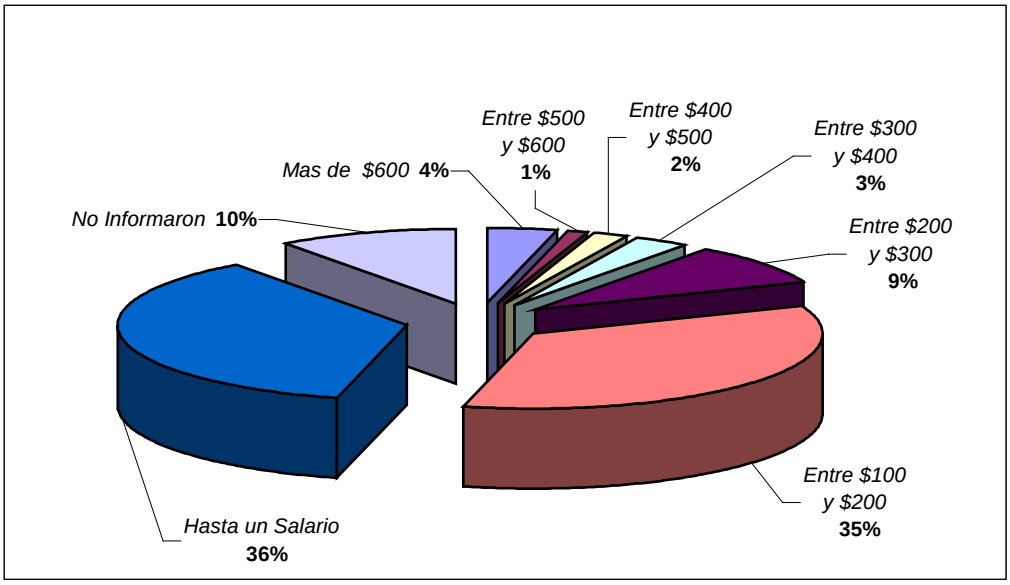


FIGURA 5.6: Distribución de ingresos en el Ecuador

Inversión inicial

En la tabla 5.8 se muestra los costos generados por la inversión inicial de los equipos. La tabla incluye lo gastos que se generaran en el primer año, tanto en la inversión de equipos, que es única, así como en los gastos por servicios, que se pagan anualmente.

COSTOS DE INVERSIÓN INICIAL				
RUBRO	**CANTIDAD**	**PRECIO**	**TOTAL**	**TIPO**
7670 Routing Switch Platform (RSP)				
Peripheral Shelf (PS)-50Gig shelf	1	158550	158550	Único
Tarjeta IP/ATM de 4 puertos STM-1	1	3000	3000	Único
tarjetas IP/ATM de 8 puertos OC-3c/STM-1	2	6250	12500	Único
Tarjeta IP/ATM de 1 puerto OC-12c/STM-4	1	8000	8000	Único
Tarjeta GigE de 2 puertos	1	2250	2250	Único
Tarjeta POS de 1 puerto OC-48c/STM-16	1	5250	5250	Único
Tarjeta ATM de 8-puertos DS3	1	1450	1450	Único

Software ALCATEL 5620 Service Router Manager	1	16000	16000	Único
SERVICIOS:				
Capacitación	1	25000	25000	Único
Montaje, instalación	1	5000	5000	Único
Costo de energía eléctrica	12	125	1500	Anual
Estudios de preinversión	1	1000	1000	Único
TOTAL GASTOS			**238000**	Único
IVA			**28560**	Único
TOTAL DE SERVICIOS RENOVABLES			**1500**	Anual
TOTAL INVERSION INICIAL			**268060**	Único

TABLA 5.8: Costos de inversión inicial

A Continuación se especifica algunos supuestos considerados en nuestro análisis:

- Para el Backbone IP/MPLS: Nos hemos inclinado por la línea de equipos ALCATEL debido a su alta confiabilidad.
- Algunos precios indicados en este cuadro son los costos de inversión, es decir, sólo se pagan una única vez en el proyecto. En cambio, hay otros rubros que deben seguir cancelándose mensual o anualmente, según lo contratado.
- Si deseamos aumentar la capacidad de nuestros equipos o servicios, se puede realizar una nueva inversión, sin embargo, debemos cubrir la demanda propuesta en los 5 años y, tanto el diseño como los equipos que vamos a adquirir puede soportar el crecimiento de la demanda estimada.

- En los costos varios incluyen rubros tales como: cables, herramientas, conectores, materiales, etc., que servirán para realizar las instalaciones y reparaciones.
- El rubro estudios de preinversión automáticamente se convierte en un gasto, aunque el proyecto no se ponga en marcha.

La planificación del proyecto esta basada a lo presentado en la figura 5.4, por ende, si queremos cubrir el objetivo anual, debemos tener el stock necesario de equipos antes de ese periodo. Como se ve, la cifra es de 740 nuevos abonados, que corresponde a 660 usuarios dedicados y 80 no dedicados, según el plan de producción.

Financiamiento

El financiamiento para la inversión inicial será del 30% con recursos propios de ETAPA, y el restante 70% mediante crédito bancario.

El aporte de ETAPA proviene de la utilidad neta del año fiscal anterior, la misma que alcanzo la cantidad de $ 115.000,00. El crédito bancario otorgado será pagado mensualmente durante 5 años en alícuotas fijas. Los valores a financiar se dan en la tabla 5.9.

INVERSION:	268060	**% DE LA DEUDA**	**MONTO:**	187642	**Dólares**
ETAPA:	80418	30%	**INTERES:**	12%	**Anual**
BANCO:	187642	70%	**MESES:**	60	**Meses**

TABLA 5.9: Financiamiento de la inversión

En vista de las condiciones presentadas, solicitamos un préstamo a un banco local o internacional, el mismo que será un monto de $187642, que los vamos a cancelar basándonos en la tasa de interés activa del 12% anual (1% mensual), lo que da 60 pagos mensuales de $4173.99.

La amortización de la deuda contraída se puede observar en la tabla 5.10:

MES	Monto	Mensual	Capital	Interés	Capital Insoluto
1	$ 187.642,00	$ 4.173,99	$ 2.297,57	$ 1.876,42	$ 185.344,43
2	$ 185.344,43	$ 4.173,99	$ 2.320,55	$ 1.853,44	$ 183.023,88
3	$ 183.023,88	$ 4.173,99	$ 2.343,75	$ 1.830,24	$ 180.680,13
4	$ 180.680,13	$ 4.173,99	$ 2.367,19	$ 1.806,80	$ 178.312,93
5	$ 178.312,93	$ 4.173,99	$ 2.390,86	$ 1.783,13	$ 175.922,07
6	$ 175.922,07	$ 4.173,99	$ 2.414,77	$ 1.759,22	$ 173.507,30
7	$ 173.507,30	$ 4.173,99	$ 2.438,92	$ 1.735,07	$ 171.068,38
8	$ 171.068,38	$ 4.173,99	$ 2.463,31	$ 1.710,68	$ 168.605,07
9	$ 168.605,07	$ 4.173,99	$ 2.487,94	$ 1.686,05	$ 166.117,13
10	$ 166.117,13	$ 4.173,99	$ 2.512,82	$ 1.661,17	$ 163.604,31
11	$ 163.604,31	$ 4.173,99	$ 2.537,95	$ 1.636,04	$ 161.066,36
12	$ 161.066,36	$ 4.173,99	$ 2.563,33	$ 1.610,66	$ 158.503,03
13	$ 158.503,03	$ 4.173,99	$ 2.588,96	$ 1.585,03	$ 155.914,07
14	$ 155.914,07	$ 4.173,99	$ 2.614,85	$ 1.559,14	$ 153.299,21
15	$ 153.299,21	$ 4.173,99	$ 2.641,00	$ 1.532,99	$ 150.658,21
16	$ 150.658,21	$ 4.173,99	$ 2.667,41	$ 1.506,58	$ 147.990,80
17	$ 147.990,80	$ 4.173,99	$ 2.694,08	$ 1.479,91	$ 145.296,72
18	$ 145.296,72	$ 4.173,99	$ 2.721,03	$ 1.452,97	$ 142.575,69
19	$ 142.575,69	$ 4.173,99	$ 2.748,24	$ 1.425,76	$ 139.827,46
20	$ 139.827,46	$ 4.173,99	$ 2.775,72	$ 1.398,27	$ 137.051,74
21	$ 137.051,74	$ 4.173,99	$ 2.803,48	$ 1.370,52	$ 134.248,26
22	$ 134.248,26	$ 4.173,99	$ 2.831,51	$ 1.342,48	$ 131.416,75
23	$ 131.416,75	$ 4.173,99	$ 2.859,83	$ 1.314,17	$ 128.556,93
24	$ 128.556,93	$ 4.173,99	$ 2.888,42	$ 1.285,57	$ 125.668,50
25	$ 125.668,50	$ 4.173,99	$ 2.917,31	$ 1.256,69	$ 122.751,20
26	$ 122.751,20	$ 4.173,99	$ 2.946,48	$ 1.227,51	$ 119.804,72
27	$ 119.804,72	$ 4.173,99	$ 2.975,95	$ 1.198,05	$ 116.828,77
28	$ 116.828,77	$ 4.173,99	$ 3.005,70	$ 1.168,29	$ 113.823,07
29	$ 113.823,07	$ 4.173,99	$ 3.035,76	$ 1.138,23	$ 110.787,30
30	$ 110.787,30	$ 4.173,99	$ 3.066,12	$ 1.107,87	$ 107.721,18
31	$ 107.721,18	$ 4.173,99	$ 3.096,78	$ 1.077,21	$ 104.624,40

32	$ 104.624,40	$ 4.173,99	$ 3.127,75	$ 1.046,24	$ 101.496,66
33	$ 101.496,66	$ 4.173,99	$ 3.159,03	$ 1.014,97	$ 98.337,63
34	$ 98.337,63	$ 4.173,99	$ 3.190,62	$ 983,38	$ 95.147,01
35	$ 95.147,01	$ 4.173,99	$ 3.222,52	$ 951,47	$ 91.924,49
36	$ 91.924,49	$ 4.173,99	$ 3.254,75	$ 919,24	$ 88.669,74
37	$ 88.669,74	$ 4.173,99	$ 3.287,30	$ 886,70	$ 85.382,45
38	$ 85.382,45	$ 4.173,99	$ 3.320,17	$ 853,82	$ 82.062,28
39	$ 82.062,28	$ 4.173,99	$ 3.353,37	$ 820,62	$ 78.708,91
40	$ 78.708,91	$ 4.173,99	$ 3.386,90	$ 787,09	$ 75.322,01
41	$ 75.322,01	$ 4.173,99	$ 3.420,77	$ 753,22	$ 71.901,23
42	$ 71.901,23	$ 4.173,99	$ 3.454,98	$ 719,01	$ 68.446,25
43	$ 68.446,25	$ 4.173,99	$ 3.489,53	$ 684,46	$ 64.956,72
44	$ 64.956,72	$ 4.173,99	$ 3.524,43	$ 649,57	$ 61.432,30
45	$ 61.432,30	$ 4.173,99	$ 3.559,67	$ 614,32	$ 57.872,63
46	$ 57.872,63	$ 4.173,99	$ 3.595,27	$ 578,73	$ 54.277,36
47	$ 54.277,36	$ 4.173,99	$ 3.631,22	$ 542,77	$ 50.646,14
48	$ 50.646,14	$ 4.173,99	$ 3.667,53	$ 506,46	$ 46.978,61
49	$ 46.978,61	$ 4.173,99	$ 3.704,21	$ 469,79	$ 43.274,40
50	$ 43.274,40	$ 4.173,99	$ 3.741,25	$ 432,74	$ 39.533,16
51	$ 39.533,16	$ 4.173,99	$ 3.778,66	$ 395,33	$ 35.754,49
52	$ 35.754,49	$ 4.173,99	$ 3.816,45	$ 357,54	$ 31.938,05
53	$ 31.938,05	$ 4.173,99	$ 3.854,61	$ 319,38	$ 28.083,43
54	$ 28.083,43	$ 4.173,99	$ 3.893,16	$ 280,83	$ 24.190,28
55	$ 24.190,28	$ 4.173,99	$ 3.932,09	$ 241,90	$ 20.258,19
56	$ 20.258,19	$ 4.173,99	$ 3.971,41	$ 202,58	$ 16.286,78
57	$ 16.286,78	$ 4.173,99	$ 4.011,12	$ 162,87	$ 12.275,65
58	$ 12.275,65	$ 4.173,99	$ 4.051,24	$ 122,76	$ 8.224,41
59	$ 8.224,41	$ 4.173,99	$ 4.091,75	$ 82,24	$ 4.132,67
60	$ 4.132,67	$ 4.173,99	$ 4.132,67	$ 41,33	$ 0,00
totales		**$ 250.439,56**	**$ 187.642,00**	**$ 62.797,56**	

TABLA 5.10: Tabla de Amortización de la deuda bancaria

Comercialización y facturación del servicio

Los servicios que ofertamos a los usuarios son:

- Acceso ilimitado dial-up.
- Acceso Internet con Ethernet, ofreciendo anchos de banda de: 64K, 128K, 256K, 512K y 1000K tanto para Internet como para la transmisión de datos.

- Acceso Internet dedicado, ofreciendo anchos de banda de: 64K, 128K, 256K y 512K, destinados de forma única a clientes de enlaces punto a punto.
- Acceso Transporte de Datos, ofreciendo anchos de banda de: 32K, 64K, 128K, 256K, 512k y 1000K destinados de forma única a clientes de enlaces punto a punto

La tabla 5.1 muestra el plan de producción que vamos a seguir anualmente. La tabla 5.11 resume el número de usuarios que esperamos obtener según el tipo de servicio que ofrecemos:

SERVICIO/ MES	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Dial – up	4	6	8	11	14	20	27	33	40	52	80	90
Transporte de Datos	0	12	46	65	72	90	110	139	155	175	200	205
Internet con Ethernet	0	15	55	77	86	130	149	165	200	239	260	260
Internet dedicado	15	35	46	65	78	92	112	140	160	183	200	206
Total de Usuarios	19	68	155	218	250	332	398	482	555	649	740	761

TABLA 5.11: Crecimiento mensual de nuevos usuarios, en un año

Los resultados mostrados en la tabla 5.11 corresponden al número de usuarios suscritos hasta ese momento, teniendo en cuenta que a partir del mes 11, el número de clientes se mantendrá casi constante,

esperando que ese comportamiento sea debido a un periodo de altibajo en ETAPA. Un comportamiento similar se espera en los años siguientes, a fin de cumplir con los objetivos planteados.

En lo que respecta a la facturación del servicio, este sistema se subdivide en 3 clases:

- Para los usuarios dial-up se lo hará basado en la facturación que se viene realizando con estos usuarios
- Para los usuarios Internet dedicado y Internet con ethernet la facturación será de tarifa plana, basado en el ancho de banda contratado y el número de direcciones IP asignadas.
- Para los usuarios Transporte de Datos la facturación será de tarifa plana, basado en el ancho de banda contratado.

Los valores dispuestos a cobrar por el servicio, así como de la instalación del mismo, se detallan en la tabla 5.12:

SERVICIO	**Precio x usuario**	**Tipo de Cobro**
Dial-up ilimitado	25	Mensual
Internet dedicado 32K	50	Mensual
Internet dedicado 64K	75	Mensual
Internet dedicado 128K	130	Mensual
Internet dedicado 256K	220	Mensual
Internet con ethernet 64K	110	Mensual
Internet con ethernet 128K	200	Mensual
Internet con ethernet 256K	360	Mensual
Internet con ethernet 512K	700	Mensual

Internet con ethernet 1000K	1100	Mensual
Transporte de datos 64K	75	Mensual
Transporte de datos 128K	130	Mensual
Transporte de datos 256K	220	Mensual
Transporte de datos 512K	390	Mensual
Transporte de datos 1000K	730	Mensual
Instalación de punto dedicado	50	Único
Instalación de punto dial-up	20	Único

TABLA 5.12: Servicios que se van a facturar al usuario

Proyecciones futuras

En la tabla 5.12 los ingresos son variables de acuerdo al ancho de banda que el usuario contrate. Sin embargo, dados los estudios de mercado realizados y el valor a cobrar por el servicio, es obvio que la mayoría de clientes se inclinarán por el servicio más económico, por lo que el valor promedio estará más cerca del valor mínimo.

Para nuestro análisis económico hemos optado por tomar un valor promedio para cada cliente dedicado, éste debe ser cercano al valor mínimo y debe tener un margen de error muy bajo. El valor promedio lo obtenemos basándonos en los datos estadísticos de la tabla 5.7 y de la tabla 5.12, de esto nos resulta:

Para el acceso Internet con ethernet (260 usuarios):

- **Promedio =** 26.8%*260*110 + 5.3%*260*200 + 3%*260*360 + 1.5%*260*700 + 1%*260*1100 = 18818.8 / 260 = **$ 72.38**

Para el acceso transporte de datos (200 usuarios):

- **Promedio =** 26.8%*200*75 + 5.3%*200*130 + 3%*200*220 + 1.5%*200*390 + 1%*200*730 = 9348 / 200 = **$ 46.74**

Para el acceso Internet dedicado (200 usuarios):

- **Promedio =** 62.4%*200*50 + 26.8%*200*75 + 5.3%*200*130 + 3%*200*220 = 12958 / 200 = **$ 64.79**

Los valores promedio que hemos considerado para nuestros clientes son:

- Para usuarios Internet con ethernet: $ 72 por usuario
- Para usuarios Internet dedicado: $ 64 por usuario
- Para usuarios Transporte datos: $ 46 por usuario.

Teniendo en cuenta lo anterior y basándonos en la proyección de crecimiento mensual de clientes de la tabla 5.11, la proyección de ingresos mensual por concepto de nuevos usuarios en un año, es la siguiente:

Servicios /Meses	Dial-up	Transporte Datos	Internet Dedicado	Internet con Ethernet	Total Ingresos
1	$ 0,00	$ 0,00	$ 0,00	$ 0,00	
2	$ 100,00	$ 0,00	$ 960,00	$ 0,00	
3	$ 150,00	$ 552,00	$ 2.240,00	$ 1.080,00	
4	$ 200,00	$ 2.116,00	$ 2.944,00	$ 3.960,00	
5	$ 275,00	$ 2.990,00	$ 4.160,00	$ 5.544,00	
6	$ 350,00	$ 3.312,00	$ 4.992,00	$ 6.192,00	
7	$ 500,00	$ 4.140,00	$ 5.888,00	$ 9.360,00	
8	$ 675,00	$ 5.060,00	$ 7.168,00	$ 10.728,00	
9	$ 825,00	$ 6.394,00	$ 8.960,00	$ 11.880,00	
10	$ 1.000,00	$ 7.130,00	$ 10.240,00	$ 14.400,00	
11	$ 1.300,00	$ 8.050,00	$ 11.712,00	$ 17.208,00	
12	$ 2.000,00	$ 9.200,00	$ 12.800,00	$ 18.720,00	
Total	**$ 7.375,00**	**$ 48.944,00**	**$ 72.064,00**	**$ 99.072,00**	**$ 227.455,00**

TABLA 5.13: Flujo mensual de ingresos por servicio de usuarios nuevos

La explicación de la tabla 5.13 es la siguiente: El servicio es pospago y se lo cobra los primeros días de cada mes. A partir del 2do Mes se empieza a percibir los ingresos por la facturación de las ventas realizadas el mes anterior por los diferentes servicios ofertados. Terminando el año con una facturación total de $ 227455.

La tabla 5.14 nos muestra el costo que cada usuario tiene que pagar por concepto de instalación y los totales aquí reflejados serán anuales.

	ABONADOS	PRECIO	TOTAL
INSTALACION			
INSTALACION DIAL-UP	80	20	1600
INSTALACION DEDICADO	660	50	33000
EQUIPOS			
CABLES Y CONECTORES	660	0	0
TOTAL INSTALACION			**34600**

TABLA 5.14: Total ingresos por instalación de nuevos usuarios

El precio de los equipos e instalación se suma al precio del servicio contratado. El contrato que firma el usuario es de carácter indefinido y finalizará por mutuo acuerdo o por decisión de una de las partes según esta especificado en las cláusulas del mismo. La tabla 5.15 muestra el ingreso anual generado por servicios de los usuarios que mantienen el servicio, y corresponde a los ingresos del segundo año de los usuarios que adquirieron el servicio durante el año anterior, y no incluye el ingreso por concepto de usuarios que se agregan al servicio durante este año**.**

SERVICIOS	NUMERO	PRECIO	MESES	TOTAL
DIAL-UP ILIMITADO	80	25	12	24000
TRASPORTE DATOS	200	46	12	110400
INTERNET DEDICADO	200	64	12	153600
INTERNET CON ETHERNET	260	72	12	224640
TOTAL SERVICIOS				**512640**

TABLA 5.15: Flujo de ingresos anuales por servicios para usuarios instalados

En los ingresos, hay que tener un especial cuidado en no bajar el volumen de ventas, puesto que una disminución de ellas, es decir, si no se cumple con la meta anual, afectará directamente al flujo de ingresos del año siguientes.

En la tabla 5.16 se muestra el flujo total de ingresos anuales para usuarios que mantienen el servicio.

SERVICIOS	POR SERVICIO	POR INSTALACION	TOTAL
DIAL-UP ILIMITADO	24000	1600	25600
TRASPORTE DATOS	110400	10000	120400
INTERNET DEDICADO	153600	10000	163600
INTERNET ACCESO DEDICADO	224640	13000	237640
TOTAL INGRESOS			**547240**

Tabla 5.16 Flujo total de Ingresos anuales de usuarios instalados

Para proyectar los gastos, tenemos que existe una inversión inicial mostrada en la tabla 5.8, donde algunos son fijos, como los equipos, pero hay otros que son renovables cada año. Un detalle de este se da en la tabla 5.17:

COSTOS DE RENOVACIÓN ANUAL				
RUBRO	**CANTIDAD**	**PRECIO**	**RENOVACIÓN**	**TIPO**
Gastos Operacionales				
Obtención de bloque de direcciones IP /20	1	2500	2500	anual
Mantenimiento	1	2000	2000	anual
Materiales varios	1	750	750	anual
TOTAL GASTOS ANUALES			**5250**	

TABLA 5.17: Gastos por renovación de servicios para nuevos usuarios

Como en este proyecto sólo se ha considerado el equipo Alcatel 7670 RSP, el mismo que esta financiado a 5 años. La depreciación de este activo se encuentra en la siguiente tabla 5.18

Equipos	valor total	10% rescate	Valor Dep.	Dep. Anual	Dep. Acumulada	Saldo Libros
1Peripheral Shelf (PS)-50Gig shelf	$ 158.550,00	$ 15.855,00	$ 142.695,00	20%	$ 142.695,00	$ 15.855,00
1tarjeta IP/ATM de 4 puertos STM-1	$ 3.000,00	$ 300,00	$ 2.700,00	20%	$ 2.700,00	$ 300,00
2 tarjetas IP/ATM de 8 puertos OC-3c/STM-1	$ 12.500,00	$ 1.250,00	$ 11.250,00	20%	$ 11.250,00	$ 1.250,00
1 tarjeta IP/ATM de 1 puerto OC-12c/STM-4	$ 8.000,00	$ 800,00	$ 7.200,00	20%	$ 7.200,00	$ 800,00
1tarjeta GigE de 2 puertos	$ 2.250,00	$ 225,00	$ 2.025,00	20%	$ 2.025,00	$ 225,00
1 tarjeta POS de 1 puerto OC-48c/STM-16	$ 5.250,00	$ 525,00	$ 4.725,00	20%	$ 4.725,00	$ 525,00
1Tarjeta ATM de 8-puertos DS3	$ 1.450,00	$ 145,00	$ 1.305,00	20%	$ 1.305,00	$ 145,00
TOTAL DEPRECIABLE	**$ 191.000,00**	**$ 19.100,00**	**$ 171.900,00**		**$ 171.900,00**	**$ 19.100,00**

Tabla 5.18. Depreciación de activos

Se ha establecido el valor de rescate en un 10% del valor total, algunos de los activos como computadoras y equipos electrónicos y de redes, se deprecian a los 5 años. El valor en libros corresponde al valor total del equipo menos la depreciación acumulada y corresponde al valor contable que tienen nuestros activos.

La tabla 5.19 muestra el valor tentativo al cual vamos a vender los equipos, luego de ser depreciados durante los 5 años transcurridos.

Equipos	Valor en Libros	VENTA	Utilidad o Pérdida
1Peripheral Shelf (PS)-50Gig shelf	$ 15.855,00	$ 50.000,00	$ 34.145,00
1tarjeta IP/ATM de 4 puertos STM-1	$ 300,00	$ 800,00	$ 500,00
2 tarjetas IP/ATM de 8 puertos OC-3c/STM-1	$ 1.250,00	$ 2.500,00	$ 1.250,00
1 tarjeta IP/ATM de 1 puerto OC-12c/STM-4	$ 800,00	$ 3.000,00	$ 2.200,00
1tarjeta GigE de 2 puertos	$ 225,00	$ 600,00	$ 375,00
1 tarjeta POS de 1 puerto OC-48c/STM-16	$ 525,00	$ 2.000,00	$ 1.475,00
1Tarjeta ATM de 8-puertos DS3	$ 145,00	$ 400,00	$ 255,00
Total Contable	**$ 19.100,00**	**$ 59.300,00**	**$ 40.200,00**

TABLA 5.19: Utilidad o pérdida por venta de activos depreciados

Basándose en lo que muestra la tabla 5.10, se obtiene los siguientes egresos anuales por concepto de pagos de capital e interés, que se muestra en la tabla 5.20:

AÑO	Pago Capital	Pago Interés	Pagos Anuales
1	$ 29.138,97	$ 20.948,94	$ 50.087,91
2	$ 32.834,52	$ 17.253,39	$ 50.087,91
3	$ 36.998,76	$ 13.089,15	$ 50.087,91
4	$ 41.691,13	$ 8.396,78	$ 50.087,91
5	$ 46.978,61	$ 3.109,30	$ 50.087,91
TOTAL	**$ 187.642,00**	**$ 62.797,56**	**$ 250.439,56**

TABLA 5.20: Egresos anuales por pago de capital e interés de préstamo bancario

Análisis de la rentabilidad del proyecto

Habiendo analizado las proyecciones de ingresos, costos y gastos. Tenemos suficiente criterio para establecer los flujos de caja, utilidades anuales, rentabilidad y factibilidad del proyecto. A continuación

analizaremos lo que respecta a las utilidades que se generarán durante los 5 años que dure el proyecto.

AÑO	INGRESOS	GASTOS	DEPRECIACION	TOTAL GASTO	UTILIDAD BRUTA
0	$ 0,00	$ 268.060,00	$ 0,00	$ 268.060,00	**$ -268.060,00**
1	$ 422.455,00	$ 135.337,91	$ 34.380,00	$ 169.717,91	**$ 252.737,09**
2	$ 1.164.695,00	$ 135.337,91	$ 34.380,00	$ 169.717,91	**$ 994.977,09**
3	$ 1.906.935,00	$ 135.337,91	$ 34.380,00	$ 169.717,91	**$ 1.737.217,09**
4	$ 2.649.175,00	$ 135.337,91	$ 34.380,00	$ 169.717,91	**$ 2.479.457,09**
5	$ 3.391.415,00	$ 135.337,91	$ 34.380,00	$ 169.717,91	**$ 3.221.697,09**
Total	$ 9.534.675,00	$ 944.749,55	$ 171.900,00	$ 1.116.649,55	**$ 8.418.025,45**

TABLA 5.21: Utilidad Bruta Anual

La tabla 5.21 muestra los ingresos brutos del negocio reestructurado, donde se encuentran incluidos los ingresos brutos del negocio que se encontraba en marcha, más los nuevos ingresos generados por el proyecto. En la misma tabla se ven reflejados los gastos que genera el negocio reestructurado, donde están considerados los gastos del negocio en marcha así como los gastos del proyecto.

La utilidad bruta se obtiene mediante la siguiente fórmula:

Utilidad Bruta = Ingresos – Gastos– Gasto por Depreciación

En el rubro de gastos esta incluido el pago de la deuda adquirida para el financiamiento del proyecto. De la Utilidad Bruta, se deduce el 15% que va a los trabajadores, quedando un subtotal, del cual se deduce el 25% para el impuesto a la renta siendo el resultado la Utilidad Neta.

La utilidad neta se obtiene de la siguiente manera:

Utilidad antes de Impuesto = utilidad bruta - aporte a los trabajadores (15%)

UTILIDAD NETA = Utilidad antes de Impuesto – Impuesto a la renta (25%)

La obtención de la utilidad neta en nuestro proyecto se muestra en la tabla 5.22:

Año	Utilidad Bruta	Part. Trabajadores	Ut. Antes Imp.	Imp. a la renta	UTILIDAD NETA
0	$ -268.060,00	$ 0,00	$ -268.060,00	$ 0,00	**$ -268.060,00**
1	$ 252.737,09	$ 37.910,56	$ 214.826,53	$ 53.706,63	**$ 161.119,89**
2	$ 994.977,09	$ 149.246,56	$ 845.730,53	$ 211.432,63	**$ 634.297,89**
3	$ 1.737.217,09	$ 260.582,56	$ 1.476.634,53	$ 369.158,63	**$ 1.107.475,89**
4	$ 2.479.457,09	$ 371.918,56	$ 2.107.538,53	$ 526.884,63	**$ 1.580.653,89**
5	$ 3.221.697,09	$ 483.254,56	$ 2.738.442,53	$ 684.610,63	**$ 2.053.831,89**
TOTAL	**$ 8.418.025,45**	**$ 1.302.912,82**	**$ 7.115.112,63**	**$ 1.845.793,16**	**$ 5.269.319,47**

TABLA 5.22: Utilidad neta anual

Como se puede ver, el proyecto empezará a generar utilidades a partir del primer año; sin embargo no recuperamos la inversión, sino hasta el transcurso del 2do año como se demostrará más adelante.

El flujo de Caja se obtiene mediante la siguiente fórmula:

Flujo de caja = Utilidad Neta + Depreciación + Venta de act. Fijo

Los resultados del flujo de caja de nuestro proyecto son los siguientes:

AÑO	Ut. Neta	Depreciación	Venta act. Fijo	Flujo de Caja
0	$ -268.060,00	$ 0,00	$ 0,00	$ -268.060
1	$ 161.119,89	$ 34.380,00	$ 0,00	$ 195.499,89
2	$ 634.297,89	$ 34.380,00	$ 0,00	$ 668.677,89
3	$ 1.107.475,89	$ 34.380,00	$ 0,00	$ 1.141.855,89
4	$ 1.580.653,89	$ 34.380,00	$ 0,00	$ 1.615.033,89
5	$ 2.053.831,89	$ 34.380,00	$ 59.300,00	$ 2.088.211,89
TOTAL	**$ 5.269.319,47**	**$ 171.900,00**		**$ 5.441.219,47**

TABLA 5.23: Flujo de Caja anual

El flujo de caja es negativo cuando arrancamos el proyecto. A finales del año recién obtenemos un flujo de caja con saldo favorable, pero aún así el valor total gastado es mayor al recibido, de manera similar a lo que se hace con la utilidad neta, se demostrará que la inversión en efectivo se recuperará en el transcurso del 2do año.

A continuación mostraremos los valores de las utilidades netas acumuladas, así como del flujo de caja acumulado. A medida que transcurre el periodo de ejecución de nuestro proyecto notamos claramente que al final del primer año, ambos valores aún son negativos lo que quiere decir que todavía no recuperamos la inversión. Recién al final del año 2 obtenemos valores acumulados positivos, lo que quiere decir que durante ese año, el flujo de ingresos menos el flujo de gastos son iguales. Como conclusión, nuestro proyecto se recuperará en 2 años.

Años	Utilidad Neta Acumulada	Flujo de Caja Acumulado
0	$ -268.060,00	$ -268.060,00
1	$ -106.940,11	$ -72.560,11
2	**$ 527.357,79**	**$ 596.117,79**
3	$ 1.634.833,68	$ 1.737.973,68
4	$ 3.215.487,58	$ 3.353.007,58
5	$ 5.269.319,47	$ 5.441.219,47

TABLA 5.24: Utilidad acumulada y flujo de caja acumulado

Los indicadores más relevantes para analizar la rentabilidad de un proyecto son: el VAN (Valor actual neto) y el TIR (Tasa interna de retorno). El VAN es el valor de todos los ingresos y egresos realizados a través del tiempo, traídos a un presente, este valor tiene que ser mayor que 0 para decir que el proyecto es rentable. La obtención del VAN está basada en el flujo de caja y no en la utilidad neta. El TIR es la tasa cuando el valor presente es 0, es la mínima tasa admitida por lo que se puede decir que el proyecto es rentable, es la tasa con la que nuestra inversión regresa y tiene que ser mayor que la tasa del mercado para que sea rentable el proyecto.

En ambos casos hay que traer los valores a valor presente. Para realizar dichos traslados, hay que usar la TMAR (Tasa mínima atractiva de retorno).

Existen muchas formas de obtener la TMAR, sin embargo, la más común depende de las tasas de interés activa y pasiva.

Tasa de interés pasiva = 5% anual (socios)

Tasa de interés activa = 12% anual (bancos)

TMAR = Tasa activa * %participación + Tasa pasiva * %participación **=**

TMAR = 12%*0.70 + 5%*0.3 = 8.4 + 1.5 **= 9.9%**

Con el valor de la TMAR, vamos a analizar la rentabilidad del proyecto. Hallaremos el VAN y el TIR, primero sin considerar la inflación.

Para hallar el VAN:

- **VAN sin inflación =** -268060 + 195499,89*(P/F,9.9%,1) + 668.677,89*(P/F,9.9%,2) + 1.141.855,89*(P/F,9.9%,3) + 1.615.033,89*(P/F,9.9%,4) + 2.088.211,89*(P/F,9.9%,5) = **3.397.028,17**
- Como: **VAN > 0, el proyecto es RENTABLE.**

Para hallar el TIR:

- **TIR sin inflación =** Tasa (VAN = 0) **= 170%**
- Como: **TIR > TMAR, el proyecto es RENTABLE**

Todos estos parámetros los obtuvimos sin considerar la inflación, cuyo índice actualmente en nuestro país es del 6% anual y tiende a la baja. Para el cálculo usaremos este valor, el mismo que influirá en la tasa del

mercado (TMAR), y por ende, se deberá obtener nuevos valores de TIR y VAN.

Primero hallamos la tasa del mercado mediante la fórmula:

Tasa inflada = TMARi = i + f + i*f

Donde: **i** es la tasa normal del Mercado, y **f** es la tasa de inflación.

Lo que nos da como resultado:

Tasa inflada = i + f + i*f = 9.9% + 6% + 9.9%*6% = **16.494%**

Usando la **tasa inflada** en vez de la TMAR, hallamos ahora el VAN:

VAN con inflación = -268060 + 195499,89*(P/F,16.494%,1) + 668.677,89*(P/F,16.494%,2) + 1.141.855,89*(P/F,16.494%,3) + 1.615.033,89*(P/F,16.494%,4) + 2.088.211,89*(P/F,16.494%,5) = **2.545.212,59**

Como: **VAN > 0, el proyecto es RENTABLE.**

Ahora hallamos el TIR:

TIR con inflación = Tasa (VAN = 0) **= 170%**

Como: **TIR > TMARi, el proyecto es RENTABLE**

De los resultados anteriores, incluso considerando la inflación, notamos que nuestro proyecto es rentable.

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

Implementar IP/MPLS en el backbone de ETAPA ofrecerá una flexibilidad en la forma que asigna los paquetes a las FECs, es decir que un grupo de paquetes seguirán el mismo camino para llegar a un destino; gracias a esta flexibilidad se podrá aplicar ingeniería de tráfico sobre el backbone y así soportar requisitos aplicativos específicos de diversos paquetes, como de video conferencias ó voz IP.

Con el envió de IP convencional el procesamiento de paquetes se efectúa en cada salto en la red. No obstante cuando se introduce MPLS, se asigna un paquete particular a una FEC una sola vez. La FEC a la que se asigna el paquete se codifica entonces con un identificador corto de longitud fija, conocido como etiqueta. Una etiqueta es análoga a un identificador de conexión, como el VPI/VCI en ATM o el DLCI en Frame Relay, y tiene significado únicamente en el Backbone MPLS.

Con la introducción de MPLS, que combina los beneficios de la conmutación de capa 2 y del enrutamiento de capa 3, se hace posible la construcción de una tecnología que combina beneficios de una VPN overlay, como la seguridad y el aislamiento entre clientes, y los beneficios del enrutamiento simplificado que tiene la implementación de una VPN igual a igual, a esta tecnología se la llama VPN IP/MPLS.

Por todo lo expuesto a lo largo de la tesis, especialmente en los capítulos de MPLS y VPN, se recomienda implementar IP/MPLS en el backbone de proveedores de internet. El ISP que adopte esta tecnología podrán ofrecer distintos tipos de servicios como internet de banda ancha, servicios de ADSL y SDSL, servicios de carrier, entre otros., gracias a las ventajas que brinda IP/MPLS en lo concerniente a Ingeniería de Trafico y Gestión de Red de clientes que manejan diferentes aplicaciones criticas y servicios de alta prioridad dentro de su Intranet.

Para aprovechar todas las ventajas de IP/MPLS se recomienda montarlo en una infraestructura óptica. Como se sabe la Fibra Optica maneja un mayor ancho de banda que el Cu, lo que significa mayor número de clientes, mayor capacidad, mayor velocidad, en fin un manejo más óptimo de la tecnología IP/MPLS.

ANEXO 1

GLOSARIO

GLOSARIO

Agregación de direcciones: Procedimiento mediante el que se asocia una única etiqueta a una unión de FECs, que será a su vez una FEC (en algún dominio) y que aplica dicha etiqueta a todo el tráfico de la unión.

Algoritmo de encaminamiento: Parte del software de un Router responsable de tomar las decisiones relacionadas con el encaminamiento de los paquetes. Cuando se reciba un paquete deberá decidir por qué línea de salida deberá transmitir el paquete.

Ancho de banda: Capacidad de transmisión medida en bits por segundo. Indica la máxima capacidad teórica de conexión, aunque puede verse deteriorada por factores negativos como el retardo de transmisión.

Arquitectura no orientada a conexión: Arquitectura en la que no es necesario establecer y liberar la conexión. Típicamente, cada mensaje lleva la dirección del destino y cada uno es dirigido a través del sistema independientemente del resto.

Arquitectura orientada a conexión: Arquitectura en la que para establecer la comunicación primero se debe establecer la conexión. Acto seguido se usa la conexión y por último se libera la conexión.

Backbone: Nivel más alto de una red jerárquica. Se garantiza que las redes aisladas y de tránsito conectadas al mismo eje troncal están interconectadas.

Base de información del reenvío: Tabla que forma parte de un LSR y que contiene la NHLFE, la ILM y la FTN. Se utiliza para reenviar paquetes.

Best-effort: "Lo mejor posible". Los paquetes se entregan de la mejor forma posible.

Buffer: Memoria de almacenamiento.

Cabecera de un paquete: Información de control de un sistema definido que precede a los datos del usuario.

Cabecera shim: Campo que sirve para transportar la etiqueta y que permite que MPLS funcione con cualquier tecnología del nivel de enlace. Está situado entre la cabecera del nivel de enlace y la cabecera del nivel de red.

Calidad de servicio: Nivel de prestaciones de una red, basada en parámetros tales como la velocidad de transmisión, la variación del retardo, el rendimiento y la pérdida de paquetes.

Camino de conmutación de etiquetas: Camino a través de uno o más LSRs en un nivel de la jerarquía que siguen los paquetes de una FEC particular.

Canal virtual: En ATM, término genérico para describir la capacidad de comunicación unidireccional para transportar células ATM.

Celda: Paquete de longitud fija utilizado en ATM. Una célula tiene 48 octetos de información y 5 octetos de control. El hecho de utilizar células de tamaño fijo permite el uso de nodos de conmutación a velocidades muy altas.

Checksum: Es una prueba para asegurar la integridad de los datos enviados a través de la red.

Clase de equivalencia funcional: Grupo de paquetes IP que se reenvían de la misma forma. La FEC permite agrupar paquetes en clases.

Clase de servicio: Categoría basada en el tipo de usuario, aplicación o criterio que los sistemas de QoS usan para proporcionar diferentes servicios.

Circuito virtual: Conexión establecida entre dos estaciones al comienzo de la transmisión. La ruta se establecerá antes de la transferencia de los datos. Todos los paquetes seguirán el mismo camino.

Cola: Conjunto de paquetes en espera de ser procesados.

Condiciones de carrera: Condición que se da cuando se tiene la asociación de la etiqueta y no se tiene la información de encaminamiento asociada (asociación entre FECs y siguientes saltos).

Conexión de canal virtual: Conexión lógica de ATM.

Conexión de trayecto virtual: Conjunto de VCCs que tienen el mismo punto de terminación. Las células del conjunto de los VCCs se conmutarán conjuntamente en una VPC.

Congestión: Circunstancia producida cuando el tráfico existente sobrepasa la capacidad de una ruta de comunicación de datos.

Conmutación de etiquetas: Término genérico usado para refererirse al reenvío de paquetes IP usando el algoritmo de intercambio de etiquetas.

Conmutación de etiquetas multiprotocolo: Estándar del IETF para la conmutación de etiquetas. Se basa en el uso de etiquetas las cuales identifican la ruta para encaminar los paquetes.

Conmutador: Dispositivo de nivel 2. Utiliza la cabecera de nivel 2 para enviar las tramas.

Conmutar: Operación que realizan Routers y Swiches. Éstos reciben un paquete por la línea de entrada y redirigen el paquete a la línea de salida adecuada en base a la información en la cabecera del paquete.

Control Independiente: Asociación de una etiqueta a una FEC realizada por un LSR de forma independiente. Una vez realizada dicha asociación el LSR informará a los LSRs vecinos.

Control Ordenado: Asociación de una etiqueta a una FEC de forma ordenada, desde un extremo del LSP hacia el otro. El establecimiento del LSP puede iniciarse por el LSR de entrada o por el de salida del LSP.

Correlación de la etiqueta entrante: Entrada de la FIB que sirve para correlacionar cada etiqueta entrante con un conjunto de NHLFEs. Se utiliza cuando se reenvían paquetes que llegan como paquetes etiquetados.

Correlación de la FEC con la NHLFE: Esta entrada de la FIB se utiliza cuando se quieren reenviar paquetes que no llegan etiquetados, pero que se quieren reenviar etiquetados.

Datagrama: Término utilizado para referirse a un paquete en una arquitectura no orientada a conexión.

Denial of Service: Es una forma de ataque, donde se suprimen los servicios de SMTP, HTTP, FTP, DNS, entre otros

Descriptor de flujo: Petición de reserva realizada por un sistema final. Se compone de Rspec y Filter Spec.

Difusión: Transmisión simultánea de datos a varias estaciones.

Dominio de conmutación de etiquetas: Conjunto contiguo de nodos que operan con conmutación de etiquetas y que pertenecen a un mismo dominio de encaminamiento IP (o dominio administrativo).

Router: Dispositivo de nivel 3. Analiza la información de la cabecera de nivel 3 para reenviar los paquetes a través de la red.

Router de conmutación de etiquetas: Dispositivo que implementa la conmutación de etiquetas.

Router de etiquetas frontera: Nodo que conecta un dominio de conmutación de etiquetas con un nodo externo al dominio, bien porque no soporta la conmutación de etiquetas o porque pertenece a otro dominio de conmutación de etiquetas.

Router frontera: Nodo que conecta un dominio con un nodo externo al dominio.

Enrutamiento: Acciones realizadas por los Routers para mover los paquetes a través de la red.

Enrutamiento basado en restricciones: Enrutamiento en el que además de optimizar alguna métrica escalar, se deberán satisfacer una serie de restricciones.

Enrutamiento basado en restricciones LDP: Extensión de LDP utilizado para tráfico sensible al retardo.

Enrutamiento explícito: Enrutamiento en el que un LSR, generalmente el de entrada o salida, especificará el conjunto de saltos a usar en el LSP.

Enrutamiento explícito estricto: Enrutamiento explícito en el que se especifica el LSP entero.

Enrutamiento explícito parcial: Enrutamiento explícito en el que se especifica parte del LSP.

Enrutamiento salto a salto: Enrutamiento usual en redes IP. Cada LSR elegirá el siguiente salto hacia donde reenviar los paquetes de una FEC de forma independiente.

Encapsular: Información de control que le añade una entidad del protocolo a los datos obtenidos de un usuario de protocolo.

Entrada para el reenvío con la etiqueta del siguiente salto: Entrada de la FIB utilizada para reenviar paquetes etiquetados.

Espacio de etiquetas: Alcance de una etiqueta en un LSR y cómo este alcance se relaciona con su par adyacente. Se hablará de alcance por interfaz y alcance por plataforma.

Espacio de etiquetas por interfaz: Una etiqueta se podrá interpretar de distinta forma dependiendo de la interfaz de entrada de dicha etiqueta.

Espacio de etiquetas por plataforma: Una etiqueta se interpretará de la misma forma independientemente de la interfaz de entrada de dicha etiqueta, siempre y cuando estas interfaces sean comunes con su par LSR.

Ethernet: IEEE 802.3 (CSMA/CD). Red de difusión basada en bus con control descentralizado que opera a 10, 100, 1000 Mbps. En una red ethernet, los computadores pueden transmitir cuando quieran. Si dos o más paquetes colisionan, los computadores esperarán un tiempo aleatorio y probarán a retransmitir más tarde.

Etiqueta: Identificador de tamaño fijo que tiene significado local. Se usa para reenviar paquetes. Un dispositivo de conmutación de etiquetas reemplazará la etiqueta de un paquete antes de reenviarlo.

Etiqueta de nivel 1: Si la profundidad de la pila de etiquetas de un paquete es m, la etiqueta que está al fondo de la pila se llama etiqueta de nivel 1.

Extracción en el penúltimo salto: Extracción de la etiqueta en el penúltimo LSR del LSP.

Extranet: Una extranet es similar a una intranet que es parcialmente accesible desde fuera a usuarios autorizados. Las extranets están siendo muy utilizadas como medio de intercambio de información entre las compañías y sus partners.

Fiabilidad: Tasa media de error en la red.

Función Hash: Un algoritmo criptográfico de un solo sentido que cambia una variable de tamaño arbitrario y la convierte en una variable de tamaño fijo.

Fusión de caminos virtuales: Fusión de etiquetas en donde la etiqueta MPLS se transporta en el campo ATM VPI. De esta forma se permite que múltiples caminos virtuales se fusionen en uno sólo. Dos células con el mismo valor VCI se han originado en el mismo nodo.

Fusión de canales virtuales: Nombre aplicado a cualquier técnica que le permita a un conmutador ATM realizar la fusión de etiquetas.

Fusión de circuitos virtuales: Fusión de etiquetas en donde la etiqueta MPLS se transporta en el campo ATM VPI/VCI. De esta forma se permite que múltiples circuitos virtuales se fusionen en un único circuito virtual.

Fusión de etiquetas: Reemplazo de múltiples etiquetas de entrada para una FEC particular por una sola etiqueta de salida.

Identificador de canal virtual: Etiqueta que identifica al canal virtual en cada enlace.

Identificador de la conexión del enlace de datos: Número de circuito virtual conmutado en una red de retransmisión de tramas. Está situado en la cabecera de la trama e identifica el circuito lógico por el que van los datos.

Identificador de familias de direcciones consecutivas: Campo que sirve para indicar que el campo NLRI contiene una etiqueta en MPLS-BGP.

Identificador de trayecto virtual: Etiqueta que identifica al trayecto virtual en cada enlace.

Identificador LDP: Identicador usado para identificar el espacio de etiquetas de un LSR.

Ingeniería de tráfico: Persigue adaptar flujos de tráfico a recursos físicos de la red, de tal forma que exista un equilibrio entre dichos recursos. De esta forma se conseguirá que no haya recursos excesivamente utilizados, con cuellos de botella, mientras existan recursos poco utilizados.

Intercambio de etiquetas: Algoritmo empleado por el componente de reenvío de un LSR. Cuando un LSR recibe un paquete extrae el valor de la etiqueta y accede con él a la tabla de encaminamiento. En dicha tabla de encaminamiento encontrará el nuevo valor de la etiqueta que ha de ponerle al paquete antes de reenviarlo, así como la interfaz de salida por donde ha de mandarlo. También podrá encontrar información sobre si debe o no encolar el mensaje.

Interfaz: Zona de contacto o conexión entre dos aplicaciones o entre un usuario y una aplicación.

Intranet: Red perteneciente a una organización, basada en TCP/IP, accesible exclusivamente a los miembros de la organización, empleados, o a personas con autorización.

LDP peers: Pares o iguales LDP.

LSR de entrada: LSR que recibe tráfico de usuario (por ejemplo datagramas IP) y lo clasifica en su correspondiente FEC. Genera una cabecera MPLS

asignándole una etiqueta y encapsula el paquete junto a la cabecera MPLS obteniendo una PDU MPLS.

LSR de salida: LSR que desencapsula un paquete removiendo la cabecera MPLS.

LSR exterior: Ver LSR frontera.

LSR frontera: LSR encargado de etiquetar los paquetes que entran en la red. Para poder realizar este trabajo, dicho LSR deberá implementar el componente de control y el componente de reenvío tanto del encaminamiento convencional como de la conmutación de etiquetas.

LSR interior: LSR que realiza el intercambio de etiquetas examinando exclusivamente la cabecera MPLS (obteniendo la etiqueta para poder realizar la búsqueda en la tabla de encaminamiento).

LSR intermedio: Ver LSR interior.

Mensaje: Conjunto de datos transmitido por una línea de comunicaciones.

Mensaje de ruta: Mensaje RSVP que envía el emisor al receptor creando en cada nodo RSVP el estado de la ruta.

Mensaje de solicitud de reserva: Mensaje RSVP que establece la reserva desde el receptor al emisor creando en cada nodo RSVP el estado de la reserva.

Mensaje Path: Ver Mensaje de ruta.

Modelo acoplado: Modelo en el que los protocolos de control IP corren directamente en hardware ATM. Habrá por tanto inteligencia IP en cada nodo.

Modelo superpuesto: Red IP superpuesta en una red ATM. Habrá inteligencia IP externa, esto es, la red ATM permite una conectividad de alta velocidad mientras que la red IP tendrá la inteligencia para reenviar datagramas IP.

Modo de transferencia asíncrono: Tecnología utilizada tanto para redes locales como redes de área amplia. Utiliza conmutadores que establecen circuitos lógicos entre sistemas finales por lo que hay una garantía de QoS. Esta tecnología se utiliza como espina dorsal en redes de proveedores y en grandes compañías. Tiene una alta escalabilidad.

Modos de retención de etiquetas: Comportamiento de un LSR ante la recepción de asociaciones de etiquetas a FECs que no use.

Multicast: Ver multidifusión.

Multidifusión: Modo de difusión de información que permite que ésta pueda ser recibida por múltiples nodos de la red y por tanto, por múltiples usuarios.

Multiplexación: Función que permite a dos o más fuentes de datos compartir un medio de transmisión común de tal forma que cada fuente de datos tenga su propio canal.

Nivel de enlace: Nivel 2 del modelo de referencia OSI. La tarea principal de este nivel es transformar unos recursos de transmisión y presentárselo al

nivel de red como una línea libre de errores de transmisión sin detectar. Este nivel debe resolver los problemas causados por daño, pérdida y duplicado de tramas.

Nivel de red: Nivel 3 de la arquitectura OSI. Controla la operativa relacionada con la utilización de redes de comunicaciones. El aspecto clave está en la determinación de cómo encaminar los paquetes desde la fuente al destino.

Nivel de transporte: Nivel 4 de la arquitectura OSI. La función básica de este nivel es el de aceptar datos del nivel de sesión, descomponerlos en unidades más pequeñas, en caso de ser necesario, pasárselos al nivel de red y asegurarse de que llegan correctamente al otro extremo. En condiciones normales, el nivel de transporte crea conexiones de red distintas para cada conexión de transporte requerida por el nivel de sesión.

Nodo: Dispositivo direccionable conectado a una red de ordenadores.

Paquete: Unida de datos del protocolo de red. Un paquete incluirá datos y señales de control.

Paquete etiquetado: Paquete que tiene al menos una etiqueta en la pila de etiquetas.

Paquete no etiquetado: Paquete que no tiene etiqueta, como por ejemplo un paquete IP.

Par de distribución de etiquetas: LSRs que utilizan un protocolo de distribución de etiquetas para intercambiar información de asociaciones de etiquetas a FECs.

Pares: Entidades del mismo nivel de máquinas distintas.

Piggybacking: En MPLS, protocolos que incorporan la etiqueta encima de protocolos existentes de encaminamiento.

Pila de etiquetas: Conjunto ordenado de etiquetas.

Prefijo de dirección: En vez de utilizar la máscara de subred se puede utilizar un valor llamado valor de prefijo. El valor de prefijo describe cuántos bits se deben usar como máscara.

Protocolo: Conjunto de reglas que gobiernan el formato y significado de las tramas, paquetes o mensajes que se intercambian entidades pares dentro de un nivel.

Protocolo de distribución de etiquetas: Conjunto de los procedimientos gracias a los cuales un LSR le informa a otro del significado de las etiquetas usadas para reenviar el tráfico a través de ellos.

Protocolo de estado blando: Protocolos en los que si no se reciben mensajes de actualización o refresco de la información de estado, marcan dicho estado como no válido y descartan la información.

Protocolos de estado duro: Protocolos en los que en ausencia de eventos que disparen una respuesta del protocolo, el estado del protocolo permanece sin cambio alguno durante un periodo de tiempo ilimitado.

Protocolo de pasarela externa: Protocolo de encaminamiento usado entre sistemas autónomos.

Protocolo de pasarela Interior: Protocolo de encaminamiento usado dentro de un sistema autónomo.

Protocolo punto a punto: Protocolo del nivel de enlace para líneas punto a punto que realiza control de errores, soporta múltiples protocolos y que permite negociar en tiempo de conexión la dirección IP.

Protocolo de reserva de recursos: Protocolo de estado blando utilizado para reservar recursos en una sesión en un entorno IP. Es un protocolo simplex. Este protocolo permite la asignación de diferentes niveles de servicio a diferentes usuarios. Se utiliza para ofrecer discriminación de servicio a las aplicaciones sensibles al retardo mediante la asignación de recursos.

Protocolo de resolución de direcciones: Protocolo TCP/IP que convierte direcciones IP en direcciones físicas, como por ejemplo una dirección ethernet. Un host que desee obtener una dirección física enviará una petición ARP a la red. El host con la dirección IP que contenga la petición ARP responderá con su dirección física.

Protocolo de resolución del siguiente salto: Protocolo usado para permitir que dos dispositivos pertenecientes a distinta LIS puedan comunicarse.

Proveedor de servicios Internet: Organización que da acceso a Internet ofreciendo una serie de servicios.

Protocolo simplex: Protocolo en el que los datos sólo van en un sentido.

Puerto: Identificador usado por los protocolos de transporte para distinguir los flujos de aplicaciones entre un par de hosts.

Punto de fusión: Nodo en el que se realiza la fusión de etiquetas.

Red totalmente mallada: Red en la que todos los nodos están conectados entre sí.

Reenvío: Operación que realizan tanto conmutadores como routers. Consiste básicamente en encaminar un paquete recibido por la línea de entrada en base a unos campos que contiene el paquete.

Retransmisión de tramas: Forma de conmutación de paquetes basada en el uso de tramas del nivel de enlace. No existe capa de red.

Salto de conmutación de etiquetas: Salto entre dos nodos MPLS en los que el reenvío se hace usando etiquetas.

Servidor: Dispositivo o computadora de una red que maneja recursos de la red. Ejemplo: servidor de ficheros.

Sistema anfitrión: Sistema informático que, mediante la utilización de los protocolos TCP/IP, permite a los usuarios comunicarse con otros sistemas anfitriones.

Sniffers: Programa que se utiliza para escudriñar una red

Spoofing: Obtener privilegios de acceso a una red de forma fraudulenta, por su dirección IP.

Subred lógica IP: Conjunto de hosts y routers conectados a través de una red ATM. Dichos hosts y routers están en una red IP, por lo que comparten la misma dirección de subred.

Tag: Término usado para referirse a una etiqueta en la aproximación de la conmutación de etiquetas de Cisco.

Tag switching: Aproximación de Cisco a la conmutación de etiquetas.

Tag switching router: Router de conmutación de etiquetas en la aproximación de Cisco a la conmutación de etiquetas.

Tasa máxima de transmisión: Compone de un cubo de Token_Bucket_Tspec que indica la tasa máxima de transmisión generada por la aplicación.

Tiempo de respuesta: Tiempo transcurrido desde que se hace una petición hasta que se recibe la respuesta.

Tiempo de vida: Número de nodos que puede atravesar un paquete. Cuando este campo llega a cero se desacarta el paquete.

Tipo de servicio: Campo de la cabecera IP utilizado por los elementos de la red para realizar una solicitud con un determinado nivel de QoS.

Trama: Grupo de bits que incluye datos, direcciones e información de control del protocolo. Se refiere a la PDU del nivel de enlace.

Trayecto virtual: Término genérico para designar un agrupamiento de canales virtuales. Todos los canales virtuales de un trayecto virtual tienen los mismos puntos de terminación.

Unidad de datos del protocolo: Conjunto de datos especificado en un protocolo en un nivel dado. Está compuesto por datos de control del protocolo y datos de usuario.

Unidifusión: Dirección que es reconocida por un sólo sistema anfitrión.

ANEXO 2

ACRONIMOS

ACRÓNIMOS

ACRÓNIMO	EN INGLÉS	EN ESPAÑOL
AAL	ATM Adaptation Layer.	Nivel de adaptación ATM.
ARIS	Aggregate Route-based IP switching.	Conmutación IP basada en la agregación de rutas.
ARP	Address Resolution Protocol.	Protocolo de resolución de direcciones.
ATM	Asynchronous Transfer Mode.	Modo de transferencia asíncrono.
ATMARP	Asynchronous Transfer Mode Address Resolution Protocol.	Protocolo de resolución de direcciones del modo de transferencia asíncrono.
BGP	Border Gateway Protocol.	Protocolo de pasarela externa.
CBS	Commited Burst Size.	Tamaño de ráfagas garantizada.
CDR	Commited Data Rate.	Velocidad de datos garantizada.
COS	Class Of Service.	Clase de servicio.
CR-LDP	Constraint-based Routing LDP.	Enrutamiento basado en restricciones del protocolo de distribución de etiquetas.
CSR	Cell Switching Router.	Router de conmutación de células.
DiffSer	Differentiated Services.	Servicios diferenciados.

DLCI	Data Link Connection Identifier	Identificado de la conexión del enlace de datos.
DWDM	Dense Wavelength Division Multiplexing	Multiplexación por división de la longitud de onda densa.
EBS	Excess Burst Size.	Tamaño de la ráfaga en exceso.
FANP	Flow Attribute Notification Protocol.	Protocolo de notificación de atributos de flujo.
FEC	Functional Equivalence Class.	Clase de equivalencia funcional.
FIB	Forwarding Information Base.	Base de información del reenvío.
FIFO	First In First Out.	Cola
FTN	FEC-to-NHLFE.	Correlación de la FEC con la NHLFE.
GSMP	General Switch Management Protocol.	Protocolo General de manejo del conmutador.
IETF	Internet Engineering Task Force.	Grupo de trabajo de ingenieros de Internet.
IFMP	Ipsilon Flow Management Protocol.	Protocolo de manejo del flujo de Ipsilon.
IGP	Interior Gateway Protocol.	Protocolo interior de pasarela.
ILM	Incoming Label Map.	Correlación de la etiqueta entrante.
IP	Internet Protocol.	Protocolo de Internet.
IPv4	IP version 4.	IP versión 4.

IPv6	IP version 6.	IP versión 6.
ISR	Integrated Switch Router.	Router de conmutación integrado.
LDP	Label Distribution Protocol.	Protocolo de distribución de etiquetas.
LER	Label Edge Router.	Router de etiquetas frontera.
LIS	Logical IP Subnet.	Subred lógica IP.
LSP	Label Switched Path.	Camino de conmutación de etiquetas.
LSR	Label Switching Router.	Router de conmutación de etiquetas.
MAC	Media Access Control.	Control de acceso al medio.
MPEs	Multiprotocol Extensions.	Extensiones multiprotocolo.
MPLS	Multiprotocol Label Switching.	Conmutación de etiquetas multiprotocolo.
MPOA	Multiprotocol Over ATM	Multiprotocolo a través de grandes redes.
NHLFE	Next Hop Label Forwarding Entry.	Protocolo de resolución del siguiente salto.
NHS	Next Hop Servers.	Servidores del siguiente salto
NLRI	Network Layer Reachability Information.	Información de alcance del nivel de red.
OSPF	Open Shortest Path First.	Protocolo abierto del primer camino más corto.

PBS	Peak Burst Size.	Tamaño de pico de la ráfaga.
PDR	Peak Data Rate.	Velocidad de pico de datos.
PDU	Protocol Data Unit.	Unidad de datos del protocolo.
PHB	Per-Hop-Behaviour.	Comportamiento por salto.
PPP	Point to Point Protocol.	Protocolo punto a punto.
QOS	Quality Of Service.	Calidad de servicio
RFC	Request For Comments	Documento de especificaciones del IETF.
RIP	Routing Information Protocol.	Protocolo de información de enrutamiento.
ROLC	Routing Over Large Clouds.	Enrutamiento a través de grandes nubes.
RSVP	Resource reSerVation Protocol.	Protocolo de reserva de recursos.
RSVP-TE	RSVP tunnel Extensions	Extensiones de RSVP para túneles LSP.
SAFI	Subsequent Address Family Identifier.	Identificador de familias de direcciones consecutivas
SDH	Synchronous Digital Hierarchy.	Jerarquía digital sincrona.
SONET	Synchronous Optical NETwork.	Red óptica síncrona.
SVC	Switched Virtual Circuit.	Circuito virtual conmutado.
SVP	Switched Virtual Path.	Camino virtual conmutado.

TCP	Transmisión Control Protocol.	Protocolo de control de la transmisión.
TCP/IP	Transmisión Control Protocol/Internet Protocol	Protocolo de control de la transmisión/Protocolo IP.
TOS	Type Of Service.	Tipo de servicio.
TLV	Type-Length-Value.	Tipo-Longitud-Valor.
TTL	Time To Live.	Tiempo de vida.
UDP	User Datagram Protocol.	Protocolo de datagramas de usuario.
VC	Virtual Channel.	Canal virtual.
VCC	Virtual Channel Connection.	Conexión de canal virtual.
VCI	Virtual Channel Identifier.	Identificador de canal virtual.
VP	Virtual Path.	Trayecto virtual.
VPC	Virtual Path Connection.	Conexión de trayecto virtual.
VPI	Virtual Path Identifier.	Identificador de trayecto virtual.
VPN	Virtual Private Network.	Red privada virtual.

BIBLIOGRAFIA

1. http://www.ietf.org/html.charters/mpls-charter.html
2. http://www.mplsforum.org/
3. http://www.ee.ust.hk/~eejie/mpls/sld019.html
4. http://www.freeswan.org
5. http://www.cis.ohio-state.edu/~jain/ talks/ftp/mpls_te/sld019.htm
6. http://www.nanog.org/mtg-9905/ppt/mpls/tsld067.htm
7. http://www.run.montefiore.ulg.ac.be/ CSS/MPLS.May.5.99/info.html
8. http://www.cs.fsu.edu/~xyuan/cis6930_ipqos/diffserv3mpls1.ppt
9. http://www.lcmi.ufsc.br/redes/redes00/mpls/mpls.ppt
10. http://www.riverstonenet.com/pdf/portugues_mpls_fuss.pdf
11. http://www.itpapers.com/
12. http://www.mplsrc.com/
13. http://keskus.hut.fi/opetus/s38310/ 01-02/Susitaival_060802.pdf
14. http://www.angoya.net/lni/papers/thesis/thesis-vuppala.pdf
15. http://morse.uml.edu/research.d/traffic/ theses/parikhthesis_2000.pdf
16. http://renoir.csc.ncsu.edu/Faculty/Vouk/vouk_students.html
17. http://www.elec.qmw.ac.uk/research/thesis/felicia.pdf
18. http://www.hut.fi/~mloukola/pub2/lic.pdf

19. http://red-mpls.udg.es/presentaciones/ariza_girona.pdf
20. http://people.bu.edu/hqiang/papers/gzh00.pdf
21. http://www.spc.org.pe/boletines/2002/pdf/SPCMagazineI-11.pdf
22. http://www.mor.itesm.mx/~albreyes/reportes/rvp2002.pdf
23. https://www.juniper.net/techpubs/software/junos54/ swconfig54-vpns/download/vpnl2-overview.pdf
24. http://conference.roedu.net/site/conference/papers/ PUSZTAI_K-Traffic_Engineered_Multicast_in_MLPS_Domains.pdf
25. http://www.cisco.com/en/US/tech/tk436/tk798/ tech_configuration_examples_list.html
26. http://www.ietf.org/proceedings/99jul/slides/ mpls-switching-99jul/tsld003
27. http://www.anarg.jp/achievements/web1999/papers/arakawa/ arakawa00mastersthesis--ip-over-wdm.pdf
28. argus.doit.wisc.edu/netengr/projects/mpls/ ilabs-lv00/lv00-interop2/tsld013.htm
29. argus.doit.wisc.edu/netengr/projects/mpls/ ilabs-lv99/interop-mpls/sld015.htm
30. Lee, Thomas y Davies, Joseph. Windows 2000 TCP/IP Protocols and Services. Technical Reference. Redmon: Microsoft Press, 1999.
32. Man, Scott y Krell, Mitchel. Linux TCP/IP Network Administration. New Jersey: Prentice Hall PTR, 2002.

33. Pepelnjak, Ivan y Guichard, Jim. MPLS and VPN Architectures. Indianapolis: Cisco Press, 2001