ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

ESTUDIO Y DISEÑO DE REDES VIRTUALES PRIVADAS (VPN) BASADAS EN TECNOLOGÍA MPLS

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

COSIOS CASTILLO EDUARDO RICHARD

SIMBAÑA LOACHAMÍN WILSON XAVIER

DIRECTOR: MSc. JIMÉNEZ MARÍA SOLEDAD

Quito, Junio 2004

DECLARACIÓN

Nosotros, COSIOS CASTILLO EDUARDO RICHARD, SIMBAÑA LOACHAMÍN WILSON XAVIER, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Cosios Castillo Eduardo Richard

Simbaña Loachamín Wilson Xavier

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por COSIOS CASTILLO EDUARDO RICHARD, SIMBAÑA LOACHAMÍN WILSON XAVIER, bajo mi supervisión.

Ing. MSc. JIMÉNEZ MARIA SOLEDAD
DIRECTOR DE PROYECTO

AGRADECIMIENTO

A nuestros Padres y hermanos, a nuestra Directora de Proyecto por su comprensión y paciencia, a nuestros profesores por su labor. Un agradecimiento especial para nuestros amigos quienes compartieron junto con nosotros buenos y malos momentos.

Gracias a todos !!

DEDICATORIA

A Dios, a mis Padres y hermanos,
Por estar conmigo ahora y por siempre.

DEDICATORIA

Al gran espíritu,
A mis Padres y hermanas
por su comprensión y apoyo incondicional.
Y en especial a dos personas excepcionales:
Carmen Celinda (+) y Asunción.

CONTENIDO

		Página
PRESENTACIÓN		xi
RESUMEN		xiii
CAPÍTULO 1		
1	**REDES PRIVADAS VIRTUALES CLÁSICAS**	**1**
1.1	Definición de VPN	1
1.2	Conceptos más usados en VPNs	2
1.3	Descripción de un camino de datos	5
1.3.1	Segmento dial – in	5
1.3.2	Segmento externo (Internet)	6
1.3.3	Segmento interno (Intranet)	6
1.4	Áreas de trabajo para las VPNs	6
1.4.1	Intranet	7
1.4.2	Acceso Remoto	7
1.4.3	Extranet	8
1.5	Requisitos para una VPN	9
1.6	Seguridad para las VPNs	12
1.7	*Firewall*	13
1.8	Criptografía	16
1.8.1	Algoritmos de Criptografía	16
1.8.1.1	Algoritmos de Clave Privada o Simétricos	16
1.8.1.1.1	Algoritmos de Bloque	17
1.8.1.1.2	Algoritmos de Flujo	17
1.8.1.2	Algoritmos de Clave Pública o Asimétricos	17
1.8.1.3	Hash (*Message Digest*)	18
1.8.2	Mecanismos de Seguridad	19
1.8.2.1	Firma digital	20
1.8.2.2	Certificados Digitales y Autoridades de Certificación	21
1.8.3	Ataques comunes en Algoritmos Criptográficos	23
1.9	Protocolos usados en VPNs	25
1.9.1	Protocolo Punto a Punto (PPP)	26
1.9.2	PPTP, L2F y L2TP	28
1.9.2.1	PPTP (*Point-to-Point Tunneling Protocol*)	28
1.9.2.2	L2F (*Layer 2 Forwarding*)	30
1.9.2.3	L2TP (*Layer 2 Tunneling Protocol*)	31
1.9.3	Protocolo de Seguridad en Internet (IPSec)	33
1.9.3.1	Asociación de Seguridad (SA)	34
1.9.3.2	Protocolo IKE	36
1.10	Las VPNs y sus beneficios	38
	Bibliografía – Capítulo 1	42
CAPÍTULO 2		
2	**ARQUITECTURA MPLS**	**43**
2.1	Introducción	43
2.2	Orígenes	44
2.3	Componentes de MPLS	45
2.3.1	LER (*Label Edge Router*)	45

2.3.2	LSR (*Label Switching Router*)	46
2.3.3	FEC (*Forwarding Equivalence Class*)	46
2.3.4	Etiqueta	47
2.3.4.1	Asignación de etiquetas	48
2.3.4.2	Asignación y distribución de etiquetas	49
2.3.4.2.1	Asignación de etiquetas *Downstream*	49
2.3.4.2.2	Asignación de etiquetas *Upstream*	50
2.3.4.2.3	*Downstream* No Solicitado versus *Downstream* Bajo Demanda	50
2.3.4.3	Control de la distribución de etiquetas	51
2.3.4.4	Modo de retención de etiquetas	52
2.3.4.5	Formato de la cabecera MPLS	53
2.3.4.6	Pila de etiquetas o etiquetas en *stack*	54
2.3.4.7	Encapsulación de Etiquetas	56
2.3.5	LSP (*Label Switched Path*)	57
2.4	Distribución de Tareas	60
2.4.1	Plano de Control	60
2.4.2	Plano de Datos	61
2.5	Funcionamiento de MPLS	62
2.6	Protocolos de Distribución de Etiquetas	66
2.6.1	Protocolo LDP (*Label Distribution Protocol*)	67
2.6.1.1	Detalles de LDP	68
2.6.1.1.1	Espacios de Etiquetas	68
2.6.1.1.2	Identificadores LDP	69
2.6.1.1.3	Sesión LDP	70
2.6.1.2	Mecanismo LDP	70
2.6.1.2.1	Descubrimiento LDP	70
2.6.1.2.2	Establecimiento de la Sesión LDP	71
2.6.1.2.3	Distribución de Etiquetas	72
2.6.1.3	PDUs de LDP	73
2.6.1.4	Mensajes de LDP	73
2.6.1.5	Codificación TLV	74
2.6.2	Protocolo CR-LDP	75
2.6.3	Protocolo RSVP-TE	76
2.7	Tunelización y Jerarquías en MPLS	78
2.8	MPLS *Multicast*	79
2.9	Beneficios de MPLS	80
	Bibliografía – Capítulo 2	82

CAPÍTULO 3

3	**REDES PRIVADAS VIRTUALES BASADAS EN MPLS**	**83**
3.1	Introducción	83
3.2	Definición de una IP-VPN y los Tipos Básicos	85
3.3	Modelo de VPNs *Overlay* y *Peer to Peer*	86
3.3.1	Modelo *Overlay*	87
3.3.2	Modelo *Peer to Peer*	88
3.4	VPNs MPLS	89
3.4.1	VPNs BGP/MPLS	90
3.4.1.1	Componentes de Red	91
3.4.1.2	Topologías de Redes Privadas Virtuales	93
3.4.1.3	Tablas VRF (VPN *Routing and Forwarding*)	95
3.4.1.4	Solapamiento de los espacios de dirección del cliente	96
3.4.1.5	Opciones de conectividad PE a CE	98
3.4.1.6	Distribución de rutas mediante BGP	101

3.4.1.6.1 El protocolo BGP y Sistemas Autónomos 101
3.4.1.6.2 Extensiones Multiprotocolo BGP 102
3.4.1.6.3 Atributos de la Comunidad Extendida BGP 103
3.4.1.6.4 Actualización de BGP 104
3.4.1.6.5 Distribución de la Información de enrutamiento 105
3.4.1.7 Envío de datos 106
3.4.1.8 Seguridad en las VPNs BGP/MPLS 108
3.4.2 VPNs MPLS de Capa 2 109
3.4.2.1 Arquitectura L2 VPN 111
3.4.2.2 Martini L2 VPN 111
3.4.2.2.1 Encapsulación del paquete 112
3.4.2.2.2 Transporte del paquete en una Martini L2 VPN 113
3.4.2.3 Kompella L2 VPN 115
3.4.2.3.1 Transporte del paquete en una Kompella L2 VPN 116
3.4.2.3.2 Formato de la trama 117
3.4.2.3.3 Señalización en las VPNs MPLS de capa 2 117
3.4.2.3.4 Diferencia entre los *drafts* de Kompella y Martini 119
3.4.3 Modelo de capa 3 versus Modelo de capa 2 120
3.5 Calidad de Servicio en Redes Privadas Virtuales 123
3.5.1 Servicios Integrados (IntServ) 123
3.5.2 Servicios Diferenciados (DiffServ) 124
3.5.3 Soporte de MPLS a los Servicios Diferenciados 126
3.5.4 DS-TE (*DiffServ-aware Traffic Engineering*) 129
3.5.5 Calidad de Servicio en las VPNs MPLS 131
Bibliografía – Capítulo 3 134

CAPÍTULO 4

4 DISEÑO DE REDES PRIVADAS VIRTUALES CLÁSICAS 135
4.1 Introducción 135
4.2 Diseño de la VPN Clásica 136
4.2.1 Descripción Actual del Escenario 136
4.2.1.1 Matriz 137
4.2.1.2 Primera Sucursal 138
4.2.1.3 Segunda Sucursal 139
4.2.2 Características de diseño para la VPN Clásica 140
4.2.3 Determinación de la Capacidad del Canal 141
4.2.3.1 Análisis del tráfico de datos actual de la empresa 141
4.2.3.2 Determinación de la capacidad requerida para la VPN 149
4.2.4 Conexión a Internet 153
4.2.5 Topología de la VPN 154
4.2.6 Equipos para la VPN Clásica 155
4.2.7 Asignación de un espacio de direcciones IP 158
4.2.8 Enrutamiento 162
4.3 Costos 165
4.4 Beneficios y Desventajas de las VPNs Clásicas 166
4.4.1 Beneficios 166
4.4.2 Desventajas 167
Bibliografía – Capítulo 4 169

CAPÍTULO 5

5 DISEÑO DE REDES PRIVADAS VIRTUALES CON MPLS 170

5.1	Introducción	170
5.2	Diseño de la VPN MPLS	172
5.2.1	Características de diseño para la VPN MPLS	173
5.2.2	Determinación de la Capacidad del Canal	174
5.2.3	Conexión al Proveedor	174
5.2.3.1	Puntos de Acceso al Servicio	175
5.2.3.1.1	SAP-CE	175
5.2.3.1.2	SAP-PE	176
5.2.3.2	Red de Acceso	177
5.2.4	Topología de la VPN MPLS	178
5.2.5	Acuerdo del Nivel de Servicio	179
5.2.5.1	Calidad de Servicio	181
5.2.5.2	Determinación de la Calidad de Servicio	182
5.2.6	Asignación de un espacio de direcciones IP	187
5.2.7	Enrutamiento	187
5.2.8	Equipos para la VPN MPLS	188
5.2.9	Requerimiento para el Servicio VPN MPLS	189
5.2.9.1	Definición de las VRFs	189
5.2.9.2	Definición de los Distinguidores de Ruta	190
5.2.9.3	Definición de las políticas de importación y exportación	191
5.2.9.4	Asociación de interfaces a las VRFs	192
5.2.9.5	MP-iBGP en los *routers* PE	193
5.3	Costos de la VPN MPLS	196
5.4	Comparación entre VPNs basadas en IPSec y basadas en MPLS	200
	Bibliografía – Capítulo 5	204

CONCLUSIONES Y RECOMENDACIONES **205**

REFERENCIAS BIBLIOGRÁFICAS 211

ANEXO A 215
ANEXO B 230
ANEXO C 232

ÍNDICE DE FIGURAS

Página

CAPÍTULO 1

Figura 1.1: Una VPN corporativa 2
Figura 1.2: Enrutamiento punto a punto o *tunneling* 3
Figura 1.3: Camino típico de datos 6
Figura 1.4: VPN de Intranet 7
Figura 1.5: VPN de acceso remoto 8
Figura 1.6: VPN de Extranet 8
Figura 1.7: Tecnología VPN en el modelo OSI 12
Figura 1.8: *Firewall* 13
Figura 1.9: Tipos de *Firewall* a diferentes niveles OSI 14
Figura 1.10: Mecanismos de Seguridad 20
Figura 1.11: Trama del protocolo PPP 27
Figura 1.12: Canal punto a punto a través de una red intermedia 29
Figura 1.13: WAN sobre líneas arrendadas 39
Figura 1.14: Conexión a un ISP para la conectividad de una WAN 39

CAPÍTULO 2

Figura 2.1: LERs y LSRs 46
Figura 2.2: FEC(*Forwarding Equivalence Class*) 47
Figura 2.3: Asignación *Downstream* y *Upstream* 50
Figura 2.4: *Downstream* Bajo Demanda vs. *Downstream* No solicitado 51
Figura 2.5: Modo de retención de etiquetas 52
Figura 2.6: Estructura de la cabecera genérica MPLS 54
Figura 2.7: Pila de Etiquetas 55
Figura 2.8: Encapsulación ATM, Frame Relay y IEEE 802 56
Figura 2.9: *Label Switched Path* 58
Figura 2.10: Plano de control y de datos 60
Figura 2.11: Componentes del plano de control y de datos 62
Figura 2.12: Funcionamiento de MPLS 63
Figura 2.13: Funcionamiento del manejo y envío de etiquetas 66
Figura 2.14: Espacio de etiquetas por interfaz 69
Figura 2.15: Espacio de etiquetas por plataforma 69
Figura 2.16: Intercambio de mensajes de LDP 72
Figura 2.17: Estructura de la cabecera LDP 73
Figura 2.18: Formato de los mensajes de LDP 74
Figura 2.19: Cabecera TLV 74
Figura 2.20: CR-LDP LSP 76
Figura 2.21: RSVP-TE LSP 77
Figura 2.22: Jerarquía MPLS 79

CAPÍTULO 3

Figura 3.1: Modelo *Overlay* y Modelo *Peer to Peer* 87
Figura 3.2: Componentes de red de una VPN BGP/MPLS 92
Figura 3.3: Topología *Hub and Spoke* o radial 94
Figura 3.4: Topología *Full Mesh* o completamente mallada 94
Figura 3.5: Tablas VRF 96
Figura 3.6: Distinguidor de ruta 98
Figura 3.7: Protocolos dc enrutamiento usados en una VPN BGP/MPLS 102

Figura 3.8: Actualización de BGP 105
Figura 3.9: Envío de datos 107
Figura 3.10: Palabra de control 113
Figura 3.11: VPN de capa 2 basada en MPLS (Martini) 114
Figura 3.12: Etiqueta del túnel y etiqueta del circuito virtual 114
Figura 3.13: Pila de etiquetas en una red MPLS (Martini) 115
Figura 3.14: VPN de capa 2 basada en MPLS (Kompella) 117
Figura 3.15: E-LSP y L-LSP 128
Figura 3.16: Panorama de la Calidad de Servicio 129
Figura 3.17: Modelo *Hose* 131
Figura 3.18: Modelo *Pipe* 132

CAPÍTULO 4

Figura 4.1: Modelo de referencia para las VPNs basadas en dispositivos CE 136
Figura 4.2: Esquema general de la red empresarial 137
Figura 4.3: Tráfico para el Lunes 17 de Mayo del 2004 142
Figura 4.4: Tráfico para el Martes 18 de Mayo del 2004 142
Figura 4.5: Tráfico para el Miércoles 19 de Mayo del 2004 142
Figura 4.6: Tráfico para el Jueves 20 de Mayo del 2004 143
Figura 4.7: Tráfico para el Viernes 21 de Mayo del 2004 143
Figura 4.8: Tráfico para el Lunes 17 de Mayo del 2004 para la Primera Sucursal 146
Figura 4.9: Tráfico para el Martes 18 de Mayo del 2004 para la Primera Sucursal 145
Figura 4.10: Tráfico para el Miércoles 19 de Mayo del 2004 para la Primera Sucursal 146
Figura 4.11: Tráfico para el Jueves 20 de Mayo del 2004 para la Primera Sucursal 146
Figura 4.12: Tráfico para el Viernes 21 de Mayo del 2004 para la Primera Sucursal 147
Figura 4.13: Tráfico para el Lunes 17 de Mayo del 2004 para la Segunda Sucursal 147
Figura 4.14: Tráfico para el Martes 18 de Mayo del 2004 para la Segunda Sucursal 148
Figura 4.15: Tráfico para el Miércoles 19 de Mayo del 2004 para la Segunda Sucursal 148
Figura 4.16: Tráfico para el Jueves 20 de Mayo del 2004 para la Segunda Sucursal 148
Figura 4.17: Tráfico para el Viernes 21 de Mayo del 2004 para la Segunda Sucursal 148
Figura 4.18: Distribución del tamaño de los paquetes de SAP 149
Figura 4.19: Topología de la VPN de diseño 154
Figura 4.20: Aplicación de NAT en la VPN de diseño 160
Figura 4.21: Lista de Control de Acceso 162
Figura 4.22: Diseño de la VPN clásica 163
Figura 4.23: Túnel IPSec entre la oficina Matriz y la Primera sucursal 164

CAPÍTULO 5

Figura 5.1: Modelo de referencia para las VPNs basadas en dispositivos PE 171
Figura 5.2: Conexión CE a CE con VPNs MPLS basadas en dispositivos PE 172
Figura 5.3: Elementos de la VPN MPLS de diseño 175
Figura 5.4: Punto de Acceso al Servicio en el dispositivo CE 175
Figura 5.5: Punto de Acceso al Servicio en el dispositivo PE 176
Figura 5.6: Red de acceso de la VPN MPLS 178
Figura 5.7: Clasificación de los servicios de la VPN de diseño 183
Figura 5.8: Mecanismo de la Calidad de Servicio entre el SP y la red empresarial 185
Figura 5.9: Asignación de prioridades en el *router* PE del proveedor 186
Figura 5.10: VPN basada en MPLS 194
Figura 5.11: Configuración del *router* PE que conecta a la oficina matriz 195
Figura 5.12: Localización en la red para VPNs basadas en MPLS e IPSec 203

ÍNDICE DE TABLAS

Página

CAPÍTULO 2

Tabla 2.1: Valores de las Etiquetas Reservadas 53

CAPÍTULO 3

Tabla 3.1: Tecnologías usadas en las VPNs MPLS 122
Tabla 3.2: Valores asignados al DSCP para AF PHB 125

CAPÍTULO 4

Tabla 4.1: Definición de los sitios de la VPN de diseño 141
Tabla 4.2: Tráfico para el Lunes 17 de Mayo del 2004 143
Tabla 4.3: Tráfico para el Martes 18 de Mayo del 2004 144
Tabla 4.4: Tráfico para el Miércoles 19 de Mayo del 2004 144
Tabla 4.5: Tráfico para el Jueves 20 de Mayo del 2004 144
Tabla 4.6: Tráfico para el Viernes 21 de Mayo del 2004 145
Tabla 4.7: Tráfico de datos promedio para la Matriz 145
Tabla 4.8: Tráfico de datos promedio para la Primera Sucursal 147
Tabla 4.9: Tráfico de datos promedio para la Segunda Sucursal 149
Tabla 4.10: Número de usuarios de la VPN 150
Tabla 4.11: Capacidad total para los canales de las sucursales 152
Tabla 4.12: Capacidad total para la Matriz 153
Tabla 4.13: *Router* de la oficina Matriz 156
Tabla 4.14: *Router* de la Primera Sucursal y Segunda Sucursal 156
Tabla 4.15: Direcciones IP asignadas a la VPN de diseño 159
Tabla 4.16: Numeración de las listas de acceso 161
Tabla 4.17: Costos del medio de comunicación 165
Tabla 4.18: Costo mensual por acceso de Internet 165

CAPÍTULO 5

Tabla 5.1: Resumen de las capacidades de los canales 174
Tabla 5.2: Clases de servicio dadas por un proveedor 180
Tabla 5.3: Clases de Servicio para la VPN MPLS 183
Tabla 5.4: Tipos de *routers* Cisco para las VPNs MPLS 188
Tabla 5.5: Definiciones de los distinguidores de ruta y *route targets* 190
Tabla 5.6: Políticas de importación/exportación de la Matriz 191
Tabla 5.7 Políticas de importación/exportación de la Primera Sucursal 192
Tabla 5.8: Políticas de importación/exportación de la Segunda Sucursal 192
Tabla 5.9: Costos de la conexión de acceso e Internet 196
Tabla 5.10: Costos mensuales de la Clase de Servicio 197
Tabla 5.11: Costo mensual de la Clase de Servicio de la VPN MPLS 198
Tabla 5.12: Costo mensual del servicio VPN MPLS para la empresa 199
Tabla 5.13: Comparación entre las dos soluciones de VPNs 199
Tabla 5.14: Diferencias entre las VPNs basadas en IPSec y basadas en MPLS 202

ACRÓNIMOS

AF	*Assured Forwarding*
AH	*Authentication Header*
ARP	*Address Resolution Protocol*
AS	*Autonomous System*
ASN	*Autonomous System Number*
ATM	*Asynchronous Transfer Mode*
BA	*Behavior Aggregate*
BGP	*Border Gateway Protocol*
CA	*Certification Authority*
CBR	*Constant Bit Rate*
CE	*Customer Edge*
CHAP	*Challenge Handshake Authentication Protocol*
CIR	*Committed Information Rate*
CoS	*Class of Service*
CR-LDP	*Constraint Based Routing LDP*
ER-LSP	*Explicitly Routed LSP*
DES	*Data Encryption Standard*
D-H	*Diffie-Hellman*
DLCI	*Data Link Connection Identifier*
DNS	*Domain Name System*
DSCP	*DiffServ Code Point*
DSL	*Digital Subscriber Line*
DS-TE	*DiffServ-aware Traffic Engineering*
eBGP	*External Border Gateway Protocol*
EF	*Expedited Forwarding*
E-LSP	*EXP-inferred-PSC LSP*
ESP	*Encapsulating Security Payload*
FEC	*Forwarding Equivalence Class*
FR	*Frame Relay*
FTP	*File Transfer Protocol*
GRE	*Generic Routing Encapsulation*
GW	*Gateway*
HDLC	*High Level Data Link Control*
HTTP	*Hypertext Transfer Protocol*
iBGP	*Internal Border Gateway Protocol*
IDEA	*International Data Encryption Algorithm*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IGP	*Interior Gateway Protocol*
IKE	*Internet Key Exchange*
IP	*Internet Protocol*
IPLS	*IP only LAN like Service*
IPSec	*Internet Protocol Security*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
IPVPN	*Internet Protocol-based Virtual Private Network*
IPX	*Internetwork Packet Exchange*
ISDN	*Integrated Services Digital Network*
IS-IS	*Intermediate System to Intermediate System*
ISO	*International Standardization Organization*
ISP	*Internet Service Provider*

ITU	*International Telecommunication Union*
ITU-T	*Telecommunication Standardization Sector*
L2F	*Layer 2 Forwarding*
L2TP	*Layer 2 Tunneling Protocol*
LAN	*Local Area Network*
LDP	*Label Distribution Protocol*
LER	*Label Edge Router*
L-LSP	*Label-Only-Inferred-PSC LSP*
LSP	*Label Switched Path*
LSR	*Label Switch Router*
MAC	*Media Access Control*
MD	*Message Digest*
MP-BGP	*Multiprotocol BGP*
MPLS	*Multiprotocol Label Switching*
MS	*Microsoft*
MTU	*Maximum Transfer Unit*
NAS	*Network Access Server*
NAT	*Network Address Translation*
NMS	*Network Management System*
OA	*Ordered Aggregate*
OSI	*Open Systems Interconnection*
OSPF	*Open Shortest Path First*
P	*Provider (core) router*
PDU	*Protocol Data Unit*
PE	*Provider Edge router*
PHB	*Per Hop Behavior*
PKI	*Public Key Infrastructure*
PPP	*Point-to-Point Protocol*
PPTP	*Point-to-Point Tunneling Protocol*
PPVPN	*Provider Provisioned Virtual Private Network*
PSC	*PHB Scheduling Class*
PSTN	*Public Switched Telephone Network*
PVC	*Permanent Virtual Circuit*
PWE3	*Pseudo Wire Emulation Edge-to-Edge*
QoS	*Quality of Service*
RADIUS	*Remote Authentication Dial In User Service*
RD	*Route Distinguisher*
RFC	*Request For Comments*
RIP	*Routing Information Protocol*
RSA	*Rivest Shamir Adleman*
RSVP	*Resource Reservation Protocol*
RSVP-TE	*RSVP - Traffic Engineering*
SA	*Security Association*
SAP	*Service Access Point*
SCR	*Sustainable Cell Rate*
SG	*Security Gateway*
SHA	*Security Hash Algorithm*
SLA	*Service Level Agreement*
SLS	*Service Level Specification*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*
SP	*Service Provider*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*

URL	*Uniform Resource Locator*
VC	*Virtual Circuit*
VFI	*VPN Forwarding Instance*
VLAN	*Virtual LAN*
VLL	*Virtual Leased Line*
VoIP	*Voice over IP*
VP	*Virtual Path*
VPDN	*Virtual Private Dial-up Network*
VPI	*Virtual Path Identifier*
VPLS	*Virtual Private LAN Service*
VPN	*Virtual Private Network*
VPWS	*Virtual Private Wire Service*
VR	*Virtual Router*
VRF	*VPN Routing and Forwarding*
WAN	*Wide Area Network*
WG	*Working Group*
WWW	*World Wide Web*

PRESENTACIÓN

Debido a que los requerimientos en telecomunicaciones son cada día más específicos y particulares, las redes de comunicaciones deben permitir el desarrollo de servicios variados, manteniendo los requerimientos de seguridad, costo y flexibilidad. Actualmente, el objetivo de los proveedores es ofrecer servicios de conexión entre localidades que además de un simple transporte de datos, suministren otras facilidades. Así se constituyen los denominados Servicios de Valor Agregado, es decir, servicios con funcionalidad adicional para los usuarios finales. Dentro de la gran gama de servicios de telecomunicaciones que han sido promovidos en los últimos años están las Redes Privadas Virtuales.

La idea básica de una Red Privada Virtual (VPN, *Virtual Private Network*) es bastante simple. Una corporación puede tener varias oficinas en diferentes lugares y cada una de estas oficinas pueden tener su propia red local. La interconexión de estas redes separadas sobre una red compartida (no privada) crea una VPN. A pesar de esta aparente simplicidad, existen un creciente número de tipos de VPNs disponibles y una gama desconcertante de tecnologías para implementar dichas redes.

En Enero del 2001, el grupo de trabajo MPLS (*Multiprotocol Label Switching*) del IETF publicó el primer estándar propuesto para el despliegue de MPLS en el núcleo de Internet. Desde ese primer hito, MPLS se ha vuelto la base de un número creciente de tecnologías relacionadas. Las soluciones de MPLS proporcionan ingeniería de tráfico, Calidad de Servicio (QoS) y Redes Privadas Virtuales (VPN).

Así, MPLS ha ganado un creciente interés de parte de los proveedores de servicio durante los últimos años. La última aplicación de MPLS es implementar VPNs suministradas por un proveedor. Usar MPLS para implementar VPNs es una alternativa viable para una solución de capa 2, de capa 3 o alguno de los métodos de *tunneling* comúnmente usados para la implementación de VPNs.

El mercado de las Redes Privadas Virtuales (VPNs) es un mercado de gran crecimiento para los proveedores de servicios. Pero, algunas de las tecnologías existentes que están usándose para proporcionar VPNs basadas en IP deben ser configuradas manualmente: ya que una nueva conexión supone alterar todas las configuraciones, y la falta de escalabilidad, son problemas que los SPs necesitan resolver en este mercado en vías de desarrollo. La tecnología MPLS es un mecanismo clave de VPNs escalables, haciendo fácil a los SPs usar sus redes para un crecimiento futuro, optimizar sus redes y diferenciarse en un mercado competitivo.

RESUMEN

El presente proyecto de titulación expone una apreciación global de las tecnologías que actualmente están siendo estudiadas para las soluciones de Redes Privadas Virtuales. Se enfoca en proporcionar una guía para el diseño de VPNs utilizando una tecnología relativamente nueva como lo es MPLS. Esta tecnología es útil para los proveedores de servicios, tales como portadores (*carriers*), ISPs, etc.

Este proyecto contiene cinco capítulos y tres anexos:

Capítulo 1, "VPNs Clásicas", presenta el concepto de redes privadas virtuales (VPNs, *Virtual Private Networks*), los requerimientos básicos que debe cumplir una VPN, estudia brevemente los conceptos de criptografía, los protocolos usados en VPNs. Además enumera los beneficios de esta tecnología.

Capítulo 2, "Arquitectura MPLS", describe la tecnología MPLS, su origen, sus componentes, tales como: LSR, etiqueta, LSP, planos de control y de datos; explica el funcionamiento de MPLS, describe los protocolos de distribución de etiquetas. Y enumera los beneficios de esta tecnología.

Capítulo 3, "VPNs basadas en MPLS", presenta el concepto de IP-VPNs y su taxonomía general. Define varios tipos de VPNs, en particular: VPNs basadas en dispositivos CE y VPNs basadas en dispositivos PE, y las VPNs "*Overlay*" vs. "*Peer to peer*". Además describe los modelos de VPNs basadas en MPLS de capa 3 y capa 2. Finalmente muestra conceptos de QoS combinados con MPLS y aplicados a las VPNs.

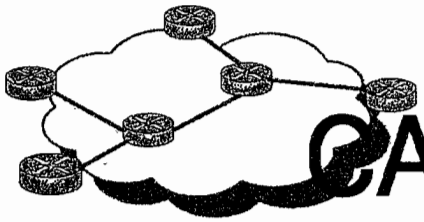
Capítulo 4, "Diseño de VPNs Clásicas", expone los conceptos, criterios y un modelo de diseño de una VPN clásica (basada en IPSec). Se presenta el equipo requerido para VPNs clásicas y su respectivo costo. Adicionalmente se enumera los beneficios y desventajas de esta tecnología.

Capítulo 5, "Diseño de VPNs con MPLS", expone los conceptos, criterios y un modelo de diseño de una VPN basada en MPLS. Se presenta el equipo requerido para VPNs con MPLS. Debe mencionarse que los costos aquí presentados no abarcan costos por operación y mantenimiento, los cuales no fueron contemplados como parte de este proyecto. Finalmente, IPSec y MPLS son comparadas como las dos principales tecnologías para proveer las actuales VPNs.

Anexo A, "Protocolos de Enrutamiento", presenta de forma breve varios protocolos de enrutamiento tales como: RIP, OSPF y BGP.

Anexo B, "Estado actual de las RFCs de MPLS", enumera los RFCs (*Request for Comments*) relacionados con la tecnología MPLS y su estado actual.

Anexo C, "Equipo a utilizar", presenta las características de los equipos utilizados para proporcionar la VPN.



CAPÍTULO 1

REDES PRIVADAS VIRTUALES CLÁSICAS

1.1 DEFINICIÓN DE VPN [1]

Desde una perspectiva histórica, el término *Virtual Private Network* (VPN) comenzó a forjar su camino a principios de 1997, pero hay quienes están en desacuerdo con esta afirmación, lo cual provoca ciertas confusiones con la fecha exacta en que apareció esta tecnología. Si bien es verdad que la tecnología subyacente utilizada en las redes privadas virtuales es el conjunto TCP/IP que se desarrolló en los sesenta, algunos de sus conceptos datan de mucho antes.

"Una red privada virtual (VPN) es una extensión de una Intranet privada de una empresa a través de una red pública tal como Internet, creando una conexión privada y segura, esencialmente a través de un túnel privado"[5]

Otra forma de ver a las VPNs es como el proceso más sencillo para enviar datos cifrados de un punto a otro, generalmente por Internet. No obstante, las VPNs también pueden utilizarse en líneas arrendadas, enlaces ATM (Modo de Transferencia Asíncrona), Frame Relay (FR) o redes digitales de servicios integrados (ISDN) y las líneas digitales de abonado (xDSL). Algunos proveedores de servicios de Internet (ISP) ya proporcionan diversas implementaciones de VPNs, como por ejemplo usando topologías basadas en Frame Relay. A pesar de que esto es una red privada desde el punto de vista de un ISP, sigue siendo una red pública desde el punto de vista de un usuario.

Al agregar la tecnología VPN a los segmentos de tramas, los clientes pueden obtener los beneficios adicionales de la tecnología VPN. La figura 1.1 muestra una red corporativa conectada a una red pública como transporte, una estructura común utilizada en las tecnologías VPN actuales. Se nota que Internet se utiliza como el medio de transporte de las tecnologías VPN, pero la nube Internet podría reemplazarse por una nube ATM, FR o MPLS (*Multiprotocol Label Switching*), tecnología que se estudiará en los capítulos posteriores.

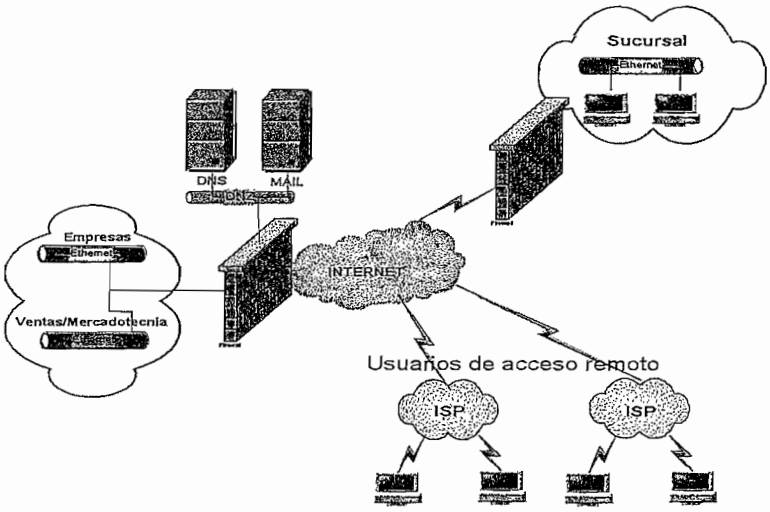


Figura 1.1: Una VPN corporativa [6]

Una característica importante de la tecnología VPN es su facilidad de crecimiento. Conforme los proveedores de red incrementan el ancho de banda en sus redes de *backbone*, las VPNs pueden crecer y aprovechar un aumento adicional en el ancho de banda. Además, puesto que las VPNs son independientes de la plataforma y no dependen de ningún sistema operativo particular, muchos dispositivos pueden funcionar como cliente o como servidor de la VPN.

Como ya se indicó anteriormente las VPNs dan cabida al crecimiento; muchos dispositivos de las VPNs manejan cualquier servicio que se instale en ellas. Permitirán crear "túneles" o comunicaciones punto a punto con cifrado, bajo demanda. Se podrá crear túneles hacia otros sitios, conforme se vaya de las oficinas centrales corporativas hasta las oficinas principales de ventas y más adelante podrá crear más túneles hacia otras oficinas.

1.2 CONCEPTOS MÁS USADOS EN VPNs [2], [3], [4]

Tunneling: El enrutamiento punto a punto o *tunneling*, es un método que permite enviar datos a una red utilizando una red intermedia. Los datos que se transfieren se denominan carga y los dos extremos del túnel se denominan extremos finales del túnel o del canal. El paquete que se envía se encapsula utilizando la cabecera del protocolo de enrutamiento punto a punto. Los *routers* de la red intermedia

utilizan la cabecera del protocolo de enrutamiento punto a punto para enrutar el paquete al punto de destino final del túnel.

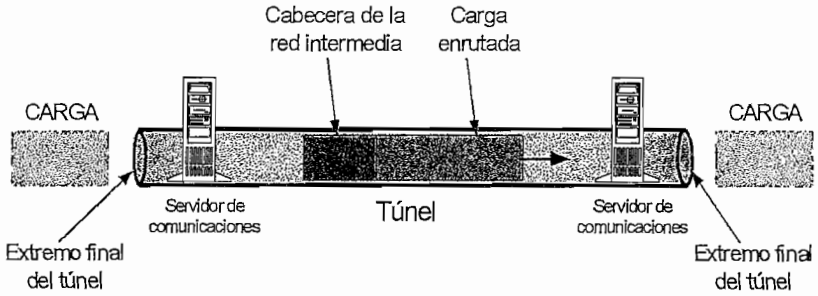


Figura 1.2: Enrutamiento punto a punto o tunneling [4]

Los *routers*[1] de la red intermedia no saben que están enrutando paquetes de un protocolo de enrutamiento punto a punto. Éstos tratan al paquete como uno más en la red. El paquete se origina en uno de los extremos del túnel y alcanza el otro extremo. En el extremo final del túnel, las cabeceras de los paquetes son removidas y el paquete es enrutado a su destino final.

Aunque la red de tránsito de la figura 1.2, puede ser cualquier red, Internet es la solución más económica y la más utilizada como red de tránsito.

TCP/IP: TCP/IP (*Transmission Control Protocol / Internet Protocol)* es la denominación que recibe una familia de protocolos diseñados para la interconexión de computadores, independientemente de su arquitectura y el sistema operativo que utilicen. A menudo el término TCP/IP es usado como un sinónimo para una colección completa de protocolos IP, incluyendo todos los protocolos usados en el Internet (como FTP, HTTP, etc.), porque la mayoría de estos protocolos dependen de TCP/IP.

TCP/IP no se preocupa por los dos niveles inferiores del modelo OSI (enlace de datos y físico), sino que comienza en el nivel de red, donde reside IP. En el nivel de transporte, aparecen TCP y UDP (*User Datagram Protocol*). Por encima de

[1] *Routers*. Dispositivos de conexión entre redes que operan en la capa de Red (Capa 3) del modelo OSI. Utilizan una combinación de *hardware* y *software* para enrutar paquetes entre redes.

esto, se ofrecen las utilidades y protocolos que componen el resto del conjunto TCP/IP y que utilizan los niveles de TCP o UCP e IP para sus sistemas de comunicaciones.

Criptografía: Son procesos matemáticos difíciles de revertir, empleados sobre un conjunto de datos, para que éstos atraviesen medios hostiles de forma más segura y puedan llegar a sus respectivos destinatarios sin variación o modificación de ninguna clase.

La criptografía es una ciencia que emplea técnicas como: autentificación, cifrado, y descifrado, para mantener un alto nivel de seguridad entre las entidades que intervienen en la comunicación.

Cifrado: es el proceso de tomar algún texto legible y convertirlo en un formato ilegible por medio de una función criptográfica. Todos los algoritmos de cifrado dependen de las funciones criptográficas. La tecnología VPN depende de las funciones criptográficas y la seguridad de las VPNs depende de la solidez criptográfica del algoritmo de cifrado. El proceso inverso, que permite comprender el contenido de un texto ilegible, se denomina descifrado.

Autentificación: La autentificación proporciona los medios para determinar de forma segura y confiable la identidad de las entidades que intervienen en una comunicación. Este proceso es necesario para negar o dar acceso a recursos protegidos de una empresa.

La autentificación de datos reafirma que el mensaje ha sido enviado *completamente* y que no ha sido alterado en ninguna forma. La autentificación de usuarios es un proceso que permite a un usuario tener acceso a la red. Es de suma importancia que se ofrezcan ambas en cualquier tecnología VPN. La criptografía, el cifrado y las funciones *hash* (tema a tratarse en la sección 1.8.1.3), permiten una autentificación adecuada.

Integridad: Es un método que le permite al transmisor o al receptor indicar si el mensaje o los paquetes de datos han sido modificados en el transcurso del viaje hacia el destinatario.

Privacidad o Confidencialidad: capacidad de que un mensaje sea leído solo por el destinatario previsto. La privacidad es proporcionada por las técnicas de cifrado.

No Rechazo: Posibilidad de demostrar que el emisor realmente envió el mensaje. Cuando se usan algoritmos que proporcionan el no rechazo, el emisor no es capaz de negar el hecho de que envió el mensaje en cuestión. Esto tiene enormes implicaciones en el comercio electrónico, para los proveedores, mayoristas, vendedores y principales socios comerciales. Si existe, aunque sea un poco de incertidumbre, una compañía no puede garantizar quién realizó el pedido. Para que el comercio electrónico en Internet se vuelva una opción viable, debe existir un proceso sin rechazo.

1.3 DESCRIPCIÓN DE UN CAMINO DE DATOS [5]

El tráfico de datos fluirá de un extremo a otro extremo, usualmente sobre una combinación de tres segmentos básicos: un segmento *Dial – in*, un segmento externo (Internet) y un segmento interno (Intranet). En la figura 1.3, se muestra los tres segmentos básicos.

1.3.1 SEGMENTO *DIAL – IN*

Constituye la conexión de un usuario remoto con un proveedor de servicios de Internet. Este segmento se extiende desde el usuario remoto hasta el acceso al ISP, comúnmente utiliza protocolos tales como PPP (*Point-to-Point Protocol*), aunque se puede usar otro protocolo, lo cual depende del ISP.

1.3.2 SEGMENTO EXTERNO (INTERNET)

Es un conjunto de distintos dominios de enrutamientos[2], cada uno de los cuales es operado por una autoridad distinta. Todos estos dominios de enrutamiento utilizan el protocolo IP para las comunicaciones, el cual realiza el enrutamiento de datos a nivel de capa red.

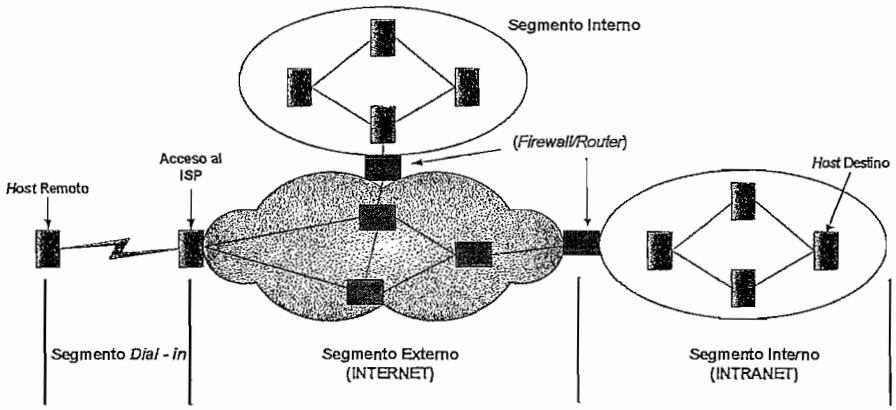


Figura 1.3: Camino típico de datos [5]

1.3.3 SEGMENTO INTERNO (INTRANET)

Es operado y administrado por una empresa, por lo que funciona en base a los protocolos que dicha empresa considere los más adecuados. Sin embargo hoy en día IP ha llegado a ser uno de los protocolos más populares usados entre Intranets corporativas y para el tráfico de datos.

1.4 ÁREAS DE TRABAJO PARA LAS VPNs [3]

Se utiliza el término área, puesto que así es como se describen las VPNs en muchos artículos. Las áreas simplemente significan implementaciones comunes de VPNs. Las VPNs no son nuevas, pero añaden un nivel de tecnología de cifrado a los servicios de Internet subyacentes.

---

[2] En redes IP, un dominio de enrutamiento se conoce como un sistema autónomo, ver la sección 3.4.1.6.1.

1.4.1 INTRANET

Una VPN de Intranet se crea entre la oficina central corporativa y una oficina remota, o entre las oficinas centrales y las oficinas dependientes. La figura 1.4 ilustra una Intranet típica.

Figura 1.4: VPN de Intranet

La única diferencia con otro tipo de redes está en que, el acceso es realizado desde afuera de la red. Normalmente, solo se utiliza dentro de la red de una compañía, para que únicamente accedan empleados autorizados que precisen alguna información de las oficinas centrales.

1.4.2 ACCESO REMOTO

Una VPN de acceso remoto se crea entre las oficinas centrales y los usuarios móviles remotos, trabajadores en casa, oficinas remotas o secundarias. La figura 1.5 ilustra uno de los tipos de acceso más comunes de las VPNs. Con el *software* de cifrado cargado en una computadora móvil, un individuo podrá establecer un túnel cifrado al dispositivo de la VPN en las oficinas centrales corporativas.

Figura 1.5: VPN de acceso remoto

1.4.3 EXTRANET

Una VPN de Extranet se crea entre la empresa y sus clientes o los proveedores. Por ejemplo, en la figura 1.6, la Extranet permitirá el acceso con el protocolo HTTP (Protocolo de Transferencia de documentos de Hipertexto) normal utilizado por los navegadores Web actuales, o permitirá que se realice la conexión utilizando otro servicio y protocolo acordados por las partes involucradas. Esta configuración le dará a la empresa la capacidad para realizar transacciones de manera segura y efectiva con sus principales socios comerciales y además con clientes que generen ingresos.

Figura 1.6: VPN de Extranet

1.5 REQUISITOS PARA UNA VPN [6]

Las VPNs consisten en *hardware*, *software* y otro conjunto de componentes. Estos componentes son simples requisitos que garantizan que las VPNs sean seguras, estén disponibles y sean fáciles de mantener.

Disponibilidad: La disponibilidad viene motivada principalmente por dos variables: una accesibilidad plena e independiente del momento y del lugar, y un rendimiento óptimo que garantice la calidad de servicio ofrecida al usuario final. La calidad de servicio (QoS, *Quality of Service*) hace referencia a la capacidad que dispone una red para asegurar un cierto nivel de funcionamiento extremo a extremo. La QoS puede venir dada como una cierta cantidad de ancho de banda o como un ancho de banda que no debe sobrepasarse o bien como una combinación de ambas. Actualmente, la entrega de datos en Internet es realizada en base al servicio del mejor esfuerzo (*best effort*), lo cual no garantiza completamente la calidad de servicio demandada.

No obstante y en un lapso de tiempo de pocos años, Internet será capaz de suplir esta carencia ofreciendo un soporte para la QoS a través de un conjunto de protocolos emergentes, como por ejemplo: RSVP-TE (*Resource ReSerVation Protocol – Traffic Engineering*), ver sección 2.6.3. Hasta ese momento, los proveedores deberán seguir proporcionando una cierta cantidad de ancho de banda en las VPNs, por ejemplo haciendo uso del tráfico CIR (*Committed Information Rate*) de Frame Relay u otras técnicas.

Compatibilidad: Para utilizar tecnologías de VPNs e Internet como medio de transporte, la arquitectura interna del protocolo de red de una compañía debe ser compatible con el protocolo IP nativo de Internet. Además, debe ser capaz de interpretar los protocolos de la red de una compañía al nivel de capa 3 del modelo de referencia OSI (*Open Systems Interconnection*). Esto implica que una compañía debe estar al tanto de las direcciones IP y saber que si los protocolos

SNA (Arquitectura de Sistemas de Red de IBM) o IPX[3] están en ejecución, no se puede establecer una conexión directa a Internet, a menos que convierta primero SNA o IPX a IP.

Actualmente existen tres técnicas básicas con las que se puede obtener la compatibilidad deseada entre las redes privadas e Internet: la conversión a direcciones Internet, la instalación de *gateways* IP y el empleo de técnicas de *tunneling*.

En la primera de estas técnicas, las direcciones Internet oficiales coexistirán con las redes IP privadas en el interior de la infraestructura de *routers* y *switches* de las organizaciones. De este modo, un usuario con una dirección IP privada puede acceder al exterior por medio de un servidor de direcciones IP oficiales mediante la infraestructura local y sin necesidad de emplear ningún tipo de acción especial.

Por otro lado, las pasarelas o *gateways* IP trabajan traduciendo de otro protocolo a IP y viceversa. Normalmente, el *gateway* IP soporta los clientes asignados a un servidor dotado de un sistema operativo de red con un cierto protocolo nativo. El *gateway* convierte el tráfico desde el protocolo nativo a IP y viceversa (por ejemplo clientes *Novell Netware* con protocolo IPX).

Por último, el *tunneling* es llevado a cabo entre ambos extremos de la conexión, proceso descrito en la sección 1.2. Dado que la realización del *tunneling* es relativamente simple, a menudo resulta la manera más sencilla y económica de llevar a cabo redes privadas virtuales bajo Internet.

Seguridad: La seguridad es, a menudo, el primer objetivo perseguido por las organizaciones dado que Internet es considerada una red "demasiado pública" para realizar comunicaciones privadas. Sin embargo, aplicando las correspondientes medidas de protección y seguridad, Internet puede convertirse

---

[3] IPX: Protocolo usado por *Novell NetWare*. IPX es un protocolo de capa red no confiable, sin conexión. Este protocolo transfiere paquetes desde el origen al destino en forma transparente, aun si la fuente y el destino se encuentra en redes diferentes.

en una red privada y segura. Para lograrlo, toda red privada virtual debe cumplir principalmente tres objetivos de seguridad:

- Proporcionar la seguridad adecuada: Un sistema mínimo de seguridad debe, al menos, validar a los usuarios mediante *passwords* con el fin de proteger los recursos de accesos no autorizados. Además, la inclusión de métodos de cifrado permitirá la protección del tráfico a lo largo de su tránsito.
- Proporcionar facilidad de administración: La elección de mecanismos de seguridad para las VPNs debe presentar métodos sencillos para su administración, pero sin descuidar que las funciones de administración deben ser seguras frente a posibles accesos ilegales.
- Transparencia hacia los usuarios: El sistema de seguridad en el acceso a la red privada virtual debe ser totalmente transparente a los usuarios.

Interoperabilidad: Las implementaciones de los tres primeros requisitos han provocado la aparición de un cuarto: la interoperabilidad. Puesto que la tecnología VPN es relativamente nueva desde el punto de vista de la implementación, surgen muchos problemas de compatibilidad a partir de la seguridad, el usuario y las normas de cifrado. Existen muchos productos de proveedores que ofrecen *hardware*, *software*, cifrado y esquemas de autentificación para la tecnología VPN. La Asociación Internacional de Seguridad en Computación (ICSA), una compañía aseguradora de seguridad establecida en 1989, tiene como meta mejorar la interoperabilidad de los productos de seguridad y certificarlos adecuadamente; los proveedores envían sus productos a ICSA para obtener una certificación.

Confiabilidad: Cuando una compañía decide instalar una VPN de un ISP, está a merced del ISP. Una frustración que sienten los usuarios es que cuando se cae la red, no tienen el control para supervisar o arreglar situaciones. Se resignan a esperar a que alguien más corrija el problema, y debido al número de usuarios que maneja el ISP, puede pasar mucho tiempo antes de disponer con los recursos necesarios para solucionar el problema.

1.6 SEGURIDAD PARA LAS VPNs [5], [6]

Cuando se analiza el tema de seguridad en redes, especialmente cuando se tiene que implementar en VPNs, se debería revisar el modelo de Interconexión de sistemas abiertos (OSI, *Open Systems Interconnection*). El modelo OSI describe la forma en que los componentes de los niveles individuales están a cargo de un conjunto específico de servicios y qué nivel se ubica por encima de otro.

El modelo OSI consta de siete niveles: aplicación, presentación, sesión, transporte, red, enlace de datos y físico. Cada nivel es responsable de su propio conjunto de funciones individuales, por ejemplo: confiabilidad, detección de y control de errores, etc.

Los ataques más comunes en la actualidad, como pueden ser las sobrecargas de la memoria intermedia (*buffer*) y otros ataques a la seguridad, suceden a través de todos estos niveles. Cada nivel puede ser atacado y verse comprometido, por lo tanto, ¿Qué hará que una VPN sea segura?. Una respuesta es hacer que la VPN se ubique en los niveles más bajos posibles del modelo OSI. La figura 1.7 ilustra una ubicación óptima para la tecnología VPN.

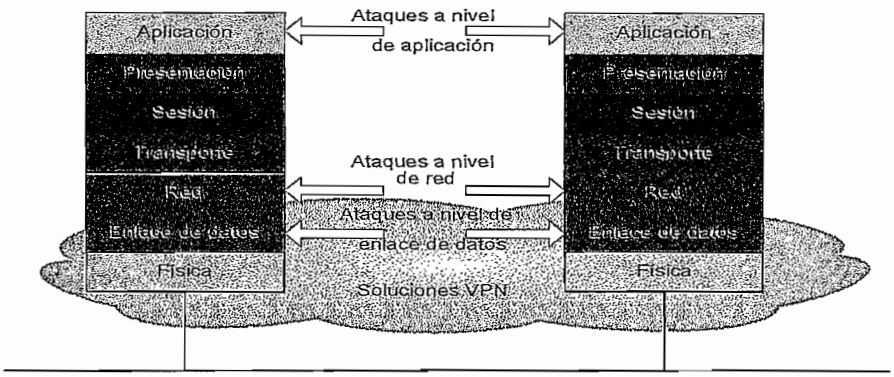


Figura 1.7: Tecnología VPN en el modelo OSI [6]

En la figura 1.7, la tecnología VPN está implementada en los niveles más bajos posibles del modelo OSI. Esto crea un beneficio y también un problema potencial.

Tener esta tecnología tan bajo como sea posible en la pila ayuda a eliminar muchos de los ataques que podrían suceder si estuviese más arriba.

No obstante, esta ubicación puede provocar problemas de compatibilidad. Al implementar el *software* de la VPN en los niveles más bajos del modelo OSI, la tecnología tiene la posibilidad de interactuar más con los componentes específicos que forman el sistema operativo.

Lamentablemente, los controladores de dispositivos, los optimizadores, pueden tener problemas de interoperabilidad con la tecnología VPN instalada. Esto puede ser un problema mas grave con los usuarios remotos que utilizan computadoras móviles y equipos de escritorios.

1.7 *FIREWALL* [2], [3], [5], [6]

Un *firewall* permite controlar qué máquinas de la red interna puedan ser vistas desde el exterior, además de los servicios a los que se puede acceder en dichas máquinas. En sentido contrario, el *firewall* también permite controlar las máquinas de la red externa que pueden ser vistas por un usuario de la red interna y los servicios a los que puede acceder en dichas máquinas.

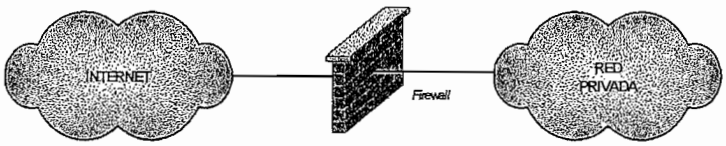


Figura 1.8: Firewall

Conceptualmente se tiene diferentes tipos de *firewalls*, éstos se clasifican dependiendo de los servicios que prestan a las capas de acuerdo al modelo de referencia OSI (ver figura 1.9) y son: *Firewall a* Nivel de Capa Red, *Firewall a* Nivel de Capa Transporte, *Firewall* a Nivel de Capa Aplicación.

***Firewall* a Nivel de Capa Red:** Un *firewall* a nivel de capa red suele ser *routers* o computadores especiales que examinan las direcciones de los paquetes para determinar si el paquete debe pasar a la red local o se debe impedir el acceso. Un paquete es la información que viaja a través del medio físico y que contiene la información a transmitir, la dirección IP del *host* emisor y la dirección IP del *host* receptor.

Figura 1.9: Tipos de Firewall a diferentes niveles OSI

Los *firewalls* de este tipo utilizan esta información almacenada en los paquetes para controlar su acceso. En este tipo de *firewalls* se elabora una especie de lista negra con las direcciones IP cuyo acceso se desea impedir, cabe destacar que este tipo de *firewalls* no permite la monitorización de los datos de niveles superiores intercambiados entre el cliente y el servidor. Por ejemplo, se puede permitir que los usuarios de Internet accedan a las páginas Web de su red privada pero impedir que accedan mediante Telnet[4] al servidor FTP. O bien hacer que se pueda acceder al servidor FTP y descarguen archivos. Para el diseño de un *firewall* a nivel de capa 3 hay que tener en cuenta algunos parámetros tales como: la dirección de origen de la que provienen los datos, la dirección de destino de los datos, el tipo de paquete transportado, el número de puerto y otros parámetros.

Un *firewall* a nivel de red correctamente configurado será transparente a los usuarios de su red, a no ser que intenten realizar una acción no permitida, como enviar información a una máquina que se encuentra en la lista negra. Además

[4] Telnet: Es un protocolo que proporciona la capacidad de conexión remota, se diseñó para trabajar con terminales sencillos. El tráfico del terminal entre usuario y el servidor Telnet se transporta en una conexión TCP.

todos los usuarios externos incluidos en la lista negra, no podrán enviar, ni recibir paquetes a y desde su red.

***Firewall* a Nivel de Capa Transporte:** Los *firewalls* a nivel de transporte son también llamados *firewall* a nivel de circuito y son similares a los de nivel de aplicación, pues ambos utilizan servidores *proxy*[5]. La diferencia radica en que los *firewalls* de circuito crean un circuito entre el cliente y el servidor sin que la aplicación sepa nada del servicio.

Los servidores a nivel de circuito, sólo utilizan un *proxy* y permiten a los usuarios utilizar sus aplicaciones cliente sin tener que preocuparse por la compatibilidad entre el servidor *proxy* y la aplicación cliente.

***Firewall* a Nivel de Capa Aplicación:** Los *firewalls* a nivel de aplicación suelen ser computadores que ejecutan *software de servidor proxy*, por lo que los administradores de red suelen referirse a estos *firewalls* simplemente como *servidor proxy*. Los servidores *proxy* se comunican con los servidores de Internet en nombre de los usuarios. Los usuarios de una red que se conectan a Internet a través de un *proxy* aparecen para los computadores de Internet con la dirección IP del servidor *proxy* (lo cual es muy apropiado para enmascarar la dirección IP).

Los servidores *proxy* se pueden configurar para los diferentes protocolos, puede permitir que se acceda a su servidor FTP para descargar archivos pero impedir que se envíen archivos a su servidor FTP. Existen servidores *proxy* para diferentes servicios; HTTP, FTP, Telnet. Se deberá configurar diferentes servidores *proxy* para los diferentes servicios que se van a utilizar. Al implementar servidores *proxy* se debe cerciorar que las aplicaciones cliente soportan el *proxy* instalado.

Normalmente los navegadores Web más difundidos pueden ser configurados para utilizar el servidor *proxy* que esté instalado, pero existe la posibilidad de que se

[5] Servidor *Proxy*: es una aplicación TCP o UDP. Su propósito es recibir solicitudes de un cliente y enviarlas a un servidor y reenviar las respuestas del servidor al cliente. La conexión de sistemas internos al mundo exterior se realiza a través de un *proxy*. Los sistemas externos responden a un servidor *proxy*.

tenga problemas con otras aplicaciones tales como FTP o IRC[6], lo que obliga a escoger el *proxy* más adecuado de acuerdo a las aplicaciones a utilizar. Con los servidores *proxy* se puede controlar fácilmente el tráfico que pasa por la red.

1.8 CRIPTOGRAFÍA [3], [5], [6]

Las redes son recursos compartidos, usados por muchas aplicaciones y por personas con diferentes propósitos. Existen casos en los cuales los datos deben ser confidenciales. Para proteger la información confidencial se requiere de mecanismos de protección. En la práctica la construcción de redes seguras requiere de complejas combinaciones de protocolos y algoritmos. La criptografía es usada para proteger la información cuando debe atravesar canales inseguros.

1.8.1 ALGORITMOS DE CRIPTOGRAFÍA

La criptografía es usada cuando los datos que viajan por una red pueden ser leídos por personas no autorizadas, por ejemplo el número de una tarjeta de crédito en una transacción de comercio electrónico. En términos generales existen dos tipos de algoritmos de criptografía:

- Clave privada (simétricos)
- Clave pública (asimétricos)

1.8.1.1 Algoritmos de Clave Privada o Simétricos

En los algoritmos simétricos, se emplea la misma clave tanto para el cifrado como para el descifrado. La prioridad en la seguridad es darle al receptor esa clave en una forma segura. En un sistema de clave privada, la prioridad de la clave es sumamente importante. Por lo tanto es necesario cambiar la clave periódicamente.

---

[6] IRC (*Internet Relay Chat*): surgió como una ampliación del programa *talk*, tratando de superar sus limitaciones. Se trata de un protocolo que permite la conversación en tiempo real a través de redes de computadoras.

El principal problema aquí es la clave; el emisor y el receptor no solo deben estar de acuerdo en usar la misma clave, sino que también deben idear una manera de intercambiarla. Los algoritmos de clave privada pueden ser de dos tipos: algoritmos de bloque y de flujo.

1.8.1.1.1 Algoritmos de Bloque

Estos algoritmos se aplican sobre bloques de *bits* del mensaje. Es un cifrado que repite varias operaciones débiles tales como sustitución, transposición, adición modular, multiplicación y transformación lineal; todas estas operaciones utilizadas sobre un bloque de datos hacen que el algoritmo sea mucho más sólido (hablando en términos de seguridad), al momento de transmitir un mensaje.

Existen muchas variantes de algoritmos, entre éstos se tiene: **DES** (*Data Encryption Standard*), **IDEA** (*International Data Encryption Algorithm*).

1.8.1.1.2 Algoritmos de Flujo

Son algoritmos simétricos que normalmente son más rápidos que los algoritmos mencionados en el párrafo anterior. A diferencia de los algoritmos de bloque que trabajan con bloques de datos, los algoritmos de flujo trabajan sobre *bits* individuales. Una característica de seguridad radica en que aún utilizando el mismo algoritmo y la misma clave, puede ser que no aparezca el mismo texto cifrado; eso depende del momento en que los *bits* se encuentran en el proceso de cifrado.

Existen muchas variantes de estos algoritmos, entre éstos se tiene: **RC** (*Rivest's Code*), **LFSR** (*Linear Feedback Shift Register*).

1.8.1.2 Algoritmos de Clave Pública o Asimétricos

Los sistemas criptográficos de clave pública utilizan una combinación de una clave privada que un determinado individuo mantiene en secreto y una clave

pública que es conocida por todos. Por lo tanto la idea es que si un mensaje se cifra con una clave privada, el mensaje solo podrá ser descifrado utilizando la correspondiente clave pública o viceversa. Estos algoritmos proporcionan no rechazo y autentificación.

RSA (*Rivest Shamir Adleman*) y ***Diffie-Hellman*** (*D-H*) son dos sistemas de clave pública conocidos que se emplean actualmente en las VPNs.

La desventaja de utilizar estos algoritmos es la velocidad, es decir son mucho más lentos que los algoritmos simétricos. Sin embargo los algoritmos de clave pública se pueden utilizar conjuntamente con los algoritmos de clave secreta.

1.8.1.3 *HASH (MESSAGE DIGEST)*

Hash es una función que toma un mensaje de longitud variable y genera una cadena de longitud fija, normalmente de 128 *bits* o más, a esto se denomina como *valor hash* y son usadas principalmente para asegurar la integridad de los datos. Las funciones *hash* son de un solo sentido, lo cual significa que son difíciles de invertir o revertir. Si se proporciona un mensaje y la función *hash* produce un valor correspondiente, no se podrá recibir el valor *hash* y utilizar la función para reproducir la cadena. Cuando un documento experimenta una función *hash*, este valor se transforma en la "huella digital" del documento original.

Para tener privacidad, el compendio de mensajes se cifra con la clave privada del emisor, a la cual se le llama firma digital. Los emisores envían esta firma digital y el mensaje original al destinatario, quien descifra la firma digital con la clave pública del emisor y crea un *hash* del mensaje original. Si estos dos mensajes producen el mismo valor *hash*, el destinatario puede estar seguro de que el mensaje proviene del emisor original. Las funciones más conocidas son el MD5 (*Message Digest 5*) y SHA (*Secure Hash Algorithm*).

Message Digest 2 (MD2), 4 (MD4), 5 (MD5 [5], [7]): Ron Rivest de los Laboratorios RSA creó Message Digest 2, 4 y 5. Todas son funciones *hash* que toman una

cadena de una longitud arbitraria y producen una salida de longitud fija. El más usado es MD5.

MD2 se diseñó en 1989 y está descrito en el RFC 1319. La implementación de MD2 ya no es recomendable, debido a su lentitud de proceso.

MD4 se diseñó en los noventa y utiliza bloques de 512 *bits* de datos. Esta función *hash* utiliza tres ciclos en su implementación. Los ataques a MD4 ocurrieron muy pronto. MD4 no está recomendado para un uso general.

MD5 se desarrolló en 1991 y es la quinta serie de funciones de dispersión diseñadas por Ron Rivest. MD5 es un algoritmo hash utilizado para autentificar los datos de un paquete. Opera alternando los *bits* de una manera tan complicada que cada *bit* de salida es afectado por cada *bit* de entrada.

***Secure Hash Algorithm* (SHA y SHA-1):** SHA es un algoritmo publicado por el Gobierno de Estados Unidos. SHA-1, una modificación de SHA, se dio a conocer en 1994; este algoritmo toma una longitud de cadena y produce un compendio de mensajes de 160 *bits*. Aun cuando es más lento que otras funciones *hash*, se lo considera más seguro.

Los algoritmos *hash* han evolucionado hasta los HMAC (*Hashed Message Authentication Code*), que combinan la seguridad demostrada de los algoritmos *hash* con funciones criptográficas adicionales.

1.8.2 MECANISMOS DE SEGURIDAD

Durante las primeras décadas de su existencia, las redes de computadoras fueron usadas principalmente por investigadores universitarios, para el envío de correo electrónico y por empleados corporativos para compartir impresoras. En estas condiciones, la seguridad no recibió mucha atención. Pero ahora, cuando millones de ciudadanos comunes usan redes para sus transacciones bancarias, compras y

declaraciones de impuestos, la seguridad de las redes aparece en el horizonte como un problema potencial de grandes proporciones.

La seguridad es un tema muy amplio que cubre una multitud de violaciones. En su forma más sencilla, la seguridad se ocupa de garantizar que las personas no autorizadas no puedan leer, o peor aún, modificar mensajes dirigidos a otros destinatarios.

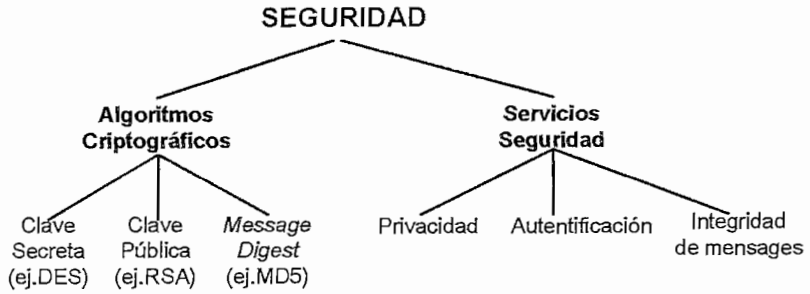


Figura 1.10: Mecanismos de Seguridad

La tecnología subyacente que hace que las VPNs sea una solución viable en las redes públicas actuales, es la criptografía; pero no solo este factor es el más importante para tener comunicaciones seguras, como se muestra en la figura 1.10, además es necesario tener otros servicios de seguridad, que permitan obtener: control de integridad, autentificación y no rechazo, en los mensajes enviados.

1.8.2.1 Firma Digital

La validación de identificación de muchos documentos legales, financieros y de otros tipos se determina por la presencia o ausencia de una firma manuscrita autorizada. Para que los sistemas computarizados de mensajes reemplacen el transporte físico de papel y tinta, se debe encontrar una solución a este problema. El problema de inventar un reemplazo para las firmas manuscritas es difícil. Básicamente, lo que se requiere es un sistema mediante el cual una parte pueda enviar un mensaje "firmado" a otra parte de tal modo que:

- El receptor pueda verificar la identidad del transmisor.
- El transmisor no pueda rechazar después el contenido del mensaje.
- El receptor no haya podido confeccionar el mensaje él mismo.

El cifrado de un valor *hash* con la clave privada de un emisor se denomina *firma digital*. La firma digital es una forma de cifrado que funciona de manera inversa al proceso de cifrado normal. La firma digital utiliza la clave privada en algunos bloques de datos (y solo un determinado individuo tiene acceso a su clave privada) y el receptor descifra esos datos con la clave pública que está disponible y es conocida. Cuando se utilizan firmas digitales, se quiere tener la certeza en la identificación del emisor; de otro modo, la firma se podría invalidar y habría rechazo.

1.8.2.2 Certificados Digitales y Autoridades de Certificación

La criptografía con claves públicas es muy útil, pero depende de la distribución de las claves públicas. Entonces el problema es cómo saber que una clave pública es legítima. Existe una forma: los certificados digitales.

La idea se basa en firmas digitales, el poseedor de alguna clave puede criptográficamente firmar un conjunto de datos. La firma digital asegura que los datos fueron generados por el propietario de alguna clave y que esta información no ha sido modificada desde el momento que se firmó digitalmente. Un certificado no es otra cosa que un caso especial de un documento firmado que diría algo así:

Certifico que la clave pública que aparece en este documento, pertenece a la entidad que aquí se menciona

XXXXXXX

Firma

Donde XXXXXXX podría ser cualquiera que tenga una clave pública pero lo más común es que sea alguna autoridad de certificación (CA, *Certificate Authority*).

Para obtener un certificado, una persona presenta su clave pública a una autoridad emisora de certificados, junto con algún distintivo único de identificación de usuario. La clave pública, el distintivo único de identificación de usuario y una identificación particular de la CA forman el certificado sin firma. Luego, la autoridad emisora de certificados tiene que firmar esta información. Esto se realiza como sigue: la autoridad emisora de certificados crea un *hash* del certificado sin firma. Después, la CA toma el *hash* y lo cifra con su clave privada. Entonces, la CA adjunta esta firma al certificado original para crear el certificado firmado.

Una vez que la información a ser enviada haya pasado por el proceso anterior el usuario puede dar este certificado a cualquiera que lo necesite o puede adjuntarlo a su clave pública. Para que el receptor verifique esto, debe descifrar la firma con la autoridad emisora de certificados y con la clave pública para recuperar el valor *hash* original. Después, el usuario recalcula el valor *hash* del documento, junto con el código recuperado en el primer paso. Si ambos coinciden, entonces el receptor puede estar seguro que el certificado coincide con el emisor original.

Este proceso ocurre durante una primera comunicación entre las partes interesadas, antes de una fecha de expiración o de que el emisor revoque su clave pública. Una vez que el receptor almacena esta firma digital que ha sido verificada por la autoridad emisora de certificados, puede aceptar cualquier comunicación futura por parte del emisor que tenga su firma digital.

Uno de los principales estándares de certificación es el **X.509**, éste especifica una estructura básica para certificados. Los componentes de un certificado deben incluir:

- El nombre de la entidad que es certificada.
- La clave pública de la entidad.
- El nombre de la autoridad certificadora (CA), que puede ser una agencia gubernamental, una institución financiera o un servidor confiable dentro de una oficina.

- La firma digital.

La norma X.509 también incluye otros elementos como un identificador que indica el algoritmo empleado para firmar el documento, la fecha de expiración del certificado; y, en la versión 3 de la norma X.509, es posible añadir información en circunstancias especiales.

Es importante tener en cuenta aspectos como:

- La posesión de un certificado no dice nada respecto a la identidad del que lo posee.
- Los certificados pueden ser libremente copiados y distribuidos.
- Para probar la identidad que aparece en el certificado, la única forma es a través de la clave privada que corresponde a la clave pública que aparece en el certificado.

1.8.3 ATAQUES COMUNES EN ALGORITMOS CRIPTOGRÁFICOS [6]

Las siguientes son varias de las categorías comunes de ataques a los algoritmos criptográficos:

Ataque de solo texto cifrado: En este caso el agresor no sabe nada respecto al mensaje de texto simple, pero al obtener el texto cifrado, intenta adivinar el texto simple. El agresor intenta encontrar un patrón común donde pueda identificar un conjunto de palabras de uso común. En la práctica, generalmente es posible hacer conjeturas con cierta base sobre el texto simple, ya que muchos tipos de mensajes tienen cabeceras de formato fijo. Las cartas y los documentos ordinarios comienzan de una forma predecible, y este patrón es útil en muchos ataques.

Ataque de texto simple conocido: En este ataque el agresor conoce parte del documento en texto simple o puede hacer conjeturas con cierta base sobre el mismo. Este texto simple puede adivinarse debido a que es posible que sea un

saludo, cabecera o una sinopsis estándar. Debido a que el atacante tiene el texto cifrado, puede utilizar el texto simple para decodificar el resto del texto.

Ataque de texto simple seleccionado: En este tipo de ataque, el agresor toma algún texto y lo cifra con la clave desconocida. En una inferencia, el atacante intenta adivinar la clave utilizada para ese cifrado. El atacante alimenta datos en el mecanismo de cifrado con la esperanza de determinar algunas salidas de cifrado de textos comunes para descifrar textos futuros. Algunos creen que RSA es vulnerable a este tipo de ataques.

Ataque de texto cifrado seleccionado: El agresor tiene la ventaja de elegir un texto cifrado seleccionado arbitrariamente y puede encontrar el texto simple descifrado correspondiente. Algunos sistemas criptográficos de clave pública son vulnerables a este tipo de ataques y en muchos casos pueden revelar la clave privada.

Ataque de intermediario: Es práctico para comunicaciones criptográficas y protocolos de intercambio de claves. Aquí dos partes intercambian sus claves para comunicaciones posteriores. El "intermediario" secuestra las claves del emisor y receptor y las sustituye con las propias, por lo cual posee la capacidad de interceptar todas las comunicaciones posteriores sin que el emisor o receptor lo sepan. La única forma de impedir esto es con el uso de firmas digitales y con el mecanismo de claves secretas compartidas.

Ataque de sincronización: Este tipo de ataque es relativamente nuevo y se basa en la medida de los tiempos de ejecución de una operación de exponenciación modular que se utiliza en los algoritmos criptográficos. Los sistemas criptográficos toman unidades de tiempo ligeramente diferentes para procesar entradas distintas. Aparentemente puede utilizarse en los algoritmos RSA y Diffie-Hellman.

Ataque de fuerza bruta: Un ataque de fuerza bruta es popular entre los agresores que poseen mucha capacidad de cómputo a su disposición, y consiste en probar todas las claves posibles en secuencia. El algoritmo más sólido

disponible se quebrantó en un tiempo récord por la Fundación de la Frontera Electrónica (EFF) usando un método de fuerza bruta. Afortunadamente, el número de pasos requeridos para los ataques de fuerza bruta crece en forma exponencial con la longitud de la clave, así por ejemplo: una clave de 32 *bits* requiere 2^{32} o alrededor de 4.2×10^9 pasos.

1.9 PROTOCOLOS USADOS EN VPNs [4], [5], [6]

Una vez vista la relevancia que presentan los requisitos para una VPN en la sección 1.5, se procederá a realizar una breve descripción así como una comparación funcional entre los principales protocolos usados en las VPNs, que permiten alcanzar en general niveles bastante satisfactorios, principalmente en las áreas de seguridad y compatibilidad.

Los protocolos de enrutamiento punto a punto o de *tunneling*, se clasifican en términos de los niveles OSI. Los protocolos de enrutamiento punto a punto de nivel 2 operan en el nivel de Enlace de datos del modelo OSI. Ejemplos de estos protocolos son: PPTP (*Point-to-Point Tunneling Protocol)*, L2TP (*Layer 2 Tunneling Protocol*) y L2F (*Layer 2 Forwarding*), protocolos que se estudiarán más adelante. Estos protocolos encapsulan el paquete del emisor en una trama PPP, ver la figura 1.11, que se envía a través de la red intermedia.

Los protocolos de nivel 3 operan en el nivel de Red del modelo de referencia OSI. Un ejemplo de estos protocolos de nivel 3 es IPSec.

El establecimiento y terminación de los canales punto a punto se denomina mantenimiento del canal punto a punto. Al contrario que los protocolos de enrutamiento punto a punto de nivel 2, los protocolos de enrutamiento punto a punto de nivel 3 no tienen una fase de mantenimiento, debido a que éstos asumen que el túnel está listo para ser utilizado.

1.9.1 PROTOCOLO PUNTO A PUNTO

Hay un gran número de propuestas de estándares que especifican el funcionamiento de PPP sobre distintas clases de enlaces punto a punto, PPP permite el uso simultáneo de múltiples protocolos de red, además se diseñó para enviar datos a través de conexiones punto a punto dedicadas, como líneas telefónicas, enlaces entre *routers* y enlaces entre computadoras.

PPP cumple los requisitos para la creación de una VPN, debido a que una VPN es un circuito virtual punto a punto. PPP es un protocolo de nivel 2, por lo tanto encapsula a los protocolos de nivel superior, como IP, IPX y NetBEUI (*NetBios Extended User Interface*)[7] y transmite los paquetes a través del enlace punto a punto. El protocolo PPP tiene tres componentes principales:

1. Un método para encapsular datagramas sobre enlaces serie.
2. Un Protocolo de Control de Enlace (LCP, *Link Control Protocol)* para establecer, configurar y probar la conexión.
3. Una familia de protocolos de control de red (NCP, *Network Control Protocol)* que establecen y configuran distintos protocolos de red. El NCP es distinto para cada capa de red. Así, el protocolo IPCP (IP *Control Protocol*) es el NCP para IP y es responsable de configurar, habilitar y deshabilitar el protocolo IP en ambos extremos del enlace. La secuencia de negociación de opciones es la misma que en LCP, lo que da la posibilidad de reutilizar el código.

Antes de que un enlace se considere apto para que los protocolos de red lo utilicen, debe producirse una secuencia específica de eventos. El LCP proporciona un método para establecer, configurar, mantener y terminar la conexión. LCP consta de las siguientes fases:

---

[7] NetBEUI: Protocolo de red sencillo y rápido creado para ser utilizado junto con el protocolo NetBIOS (*Network Basic Input/Output System*) de Microsoft e IBM en redes pequeñas.

1. Establecimiento del enlace y negociación de la configuración: En esta fase, se intercambian paquetes de control del enlace y se negocian opciones de configuración. Una vez que hay acuerdo sobre las opciones, el enlace se *abre*, pero no está necesariamente listo para que los protocolos de red comiencen a funcionar.
2. Determinación de la calidad del enlace: Esta fase es opcional. PPP no especifica una política para determinar la calidad, pero proporciona herramientas de bajo nivel, tales como "*echo request*" y "*echo reply*".
3. Autentificación: Esta fase es opcional. Cada extremo del enlace se autentifica con el otro extremo empleando métodos de autentificación acordados durante la fase 1.
4. Negociación de la configuración del protocolo de red: Una vez que LCP ha terminado la fase anterior, los protocolos de la capa de red se pueden configurar por separado con el NCP apropiado.
5. Terminación del enlace: LCP puede terminar el enlace en cualquier momento. Esto se hará normalmente a petición de un usuario, aunque puede ocurrir debido a un evento físico.

El formato de la trama PPP se escogió de modo que fuera muy parecido al formato de la trama HDLC (*High Level Data Link Control*). En particular PPP, utiliza relleno de caracteres en las líneas por discado con módem, por lo que todas las tramas tienen un número entero de *bytes*. No solo puede mandarse tramas PPP a través de líneas telefónicas de discado, sino que también pueden enviarse por ejemplo a través de SONET[8]. El formato de la trama de PPP se muestra en la figura 1.11.

1 byte	1 byte	1 byte	1 ó 2 bytes	Variable	2 ó 4 bytes	1 byte
Delimitador 01111110	Dirección 11111111	Control 00000011	Protocolo	Datos	CRC	Delimitador 01111110

Figura 1.11: Trama del protocolo PPP

[8] SONET (*Synchronous Optical Network*): La red óptica sincrónica es un estándar definido por el ANSI (*American National Standards Institute*) para la transmisión óptica digital a alta velocidad y de alta calidad.

La trama PPP comienza con el *byte* delimitador estándar de HDLC (01111110). El campo dirección al cual siempre se asigna el valor binario 11111111 para indicar que todas las estaciones deben aceptar a la trama. El campo de control, cuyo valor predeterminado es 00000011. En otras palabras, PPP no proporciona por omisión transmisión confiable usando números de secuencia y acuses. El cuarto campo es el de protocolo, su tarea es indicar la clase de paquete que está en el campo de datos. Se definen códigos para LCP, NCP, IP, IPX y otros protocolos. El campo de datos es de longitud variable, hasta algún máximo negociado, cuando no se negocia la longitud, su valor predeterminado es de 1500 *bytes*. El campo CRC normalmente es de 2 *bytes*, pero puede negociarse a 4 *bytes*.

El protocolo PPP puede operar sobre una gran variedad de interfaces físicas, como RS-232, RS-422 y V.35.

1.9.2 PPTP, L2F y L2TP

1.9.2.1 PPTP (*Point-to-Point Tunneling Protocol*) [4], [8]

PPTP es un protocolo de red creado por Microsoft que permite la realización de transferencias seguras desde clientes remotos a servidores emplazados en redes privadas, empleando para ello tanto líneas telefónicas conmutadas como Internet. En el escenario típico de PPTP, el cliente establecerá una conexión *dial-up* con el servidor de acceso a red (NAS[9]) del proveedor del servicio, empleando para ello el protocolo PPP. Una vez conectado, el cliente establecerá una segunda conexión con el servidor PPTP, el cual estará situado en la red privada. Dicho servidor será utilizado como intermediario de la conexión, recibiendo los datos del cliente externo y transmitiéndolos al correspondiente destino en la red privada. En la figura 1.12, se muestra el camino o canal punto a punto a seguir por un paquete PPTP.

[9] NAS: Servidor de acceso a la red. Es el ejecutor de la autentificación y de la autorización del cliente; el servidor de seguridad solo se encarga de la configuración de los usuarios. Por consiguiente, debe haber un conjunto de reglas que indique que el NAS y el servidor de seguridad puedan comunicarse entre sí. Por lo general este conjunto de reglas se llaman protocolos de autentificación.

Figura 1.12: Canal punto a punto a través de una red intermedia [4]

PPTP encapsula los paquetes PPP en datagramas IP. Una vez que los datagramas llegan al servidor PPTP, son desensamblados con el fin de obtener el paquete PPP y descifrados de acuerdo al protocolo de red transmitido. Por el momento, PPTP únicamente soporta los protocolos de red IP, IPX, y NetBEUI. El protocolo PPTP especifica además una serie de mensajes de control con el fin de establecer, mantener y terminar el túnel PPTP. Los paquetes de control de conexión PPTP consisten de una cabecera IP, una cabecera TCP, el mensaje de control PPTP y los *trailers* apropiados.

La autentificación PPTP está basada en el sistema de acceso de Windows NT, en el cual todos los clientes deben proporcionar un par *login/password*. La autentificación remota de clientes PPTP es realizada empleando los mismos métodos de autentificación utilizados por cualquier otro tipo de servidor de acceso remoto (RAS). En el caso de Microsoft, la autentificación utilizada para el acceso a los RAS soporta los protocolos CHAP[10], MS-CHAP, y PAP[11]. Los accesos a los recursos NTFS (*New Technology File System*), precisa de los permisos adecuados, para lo cual resulta recomendable utilizar el sistema de ficheros NTFS para los recursos de ficheros a los que deben acceder los clientes PPTP. En cuanto al cifrado de datos, PPTP utiliza el proceso de cifrado de secreto compartido en el cual sólo los extremos de la conexión comparten la clave. Dicha clave es generada empleando el estándar RSA RC-4 a partir del *password* del

[10] Protocolo CHAP (*Challenge Handshake Authentication Protocol*): Es un protocolo que utiliza una función de transformación de código de un solo sentido para proporcionar la autentificación de los usuarios.
[11] Protocolo PAP (*Password Authentication Protocol*): Protocolo de autentificación que utiliza contraseñas de texto simple y un reconocimiento en doble sentido.

usuario. La longitud de dicha clave puede ser 128 *bits* (para usuarios de Estados Unidos y Canadá) o 40 *bits* (para el resto de usuarios).

Por último, PPTP puede ser utilizado conjuntamente con *firewalls* y *routers*, para lo cual deberá habilitarse el paso del tráfico destinado al puerto TCP 1723 (tráfico PPTP) y protocolo 47 (IP).

1.9.2.2 L2F (*Layer 2 Forwarding*) [4]

El protocolo L2F tiene como objetivo proporcionar un mecanismo de *tunneling* para el transporte de tramas a nivel de enlace (HDLC, PPP, SLIP[12], etc.). El proceso de *tunneling* involucra tres protocolos diferentes: Protocolo pasajero, protocolo encapsulador, y protocolo portador. El protocolo pasajero representa el protocolo de nivel superior que debe encapsularse (PPP, SLIP, etc.). A continuación, el protocolo encapsulador indica el protocolo que será empleado para la creación, mantenimiento y terminación del túnel de comunicación. En este caso, el protocolo encapsulador será L2F. Por último, el protocolo portador será el encargado de realizar el transporte de todo el conjunto. Por lo general, este protocolo suele ser IP dadas sus capacidades de enrutamiento, su acople a los diferentes medios y su estandarización dentro del ámbito de Internet.

Entre las principales ventajas que ofrece el protocolo L2F cabe destacar el soporte multiprotocolo, la multiplexación de múltiples sesiones remotas (minimizando el número de túneles abiertos en un momento dado) y la gestión dinámica de los túneles, en la cual los recursos de los servidores de acceso a la red se minimizan al iniciar los túneles únicamente cuando existe tráfico de usuario. Además, por cada túnel L2F establecido, el proceso de seguridad genera una clave aleatoria como medida de prevención ante posibles ataques basados en *spoofing*[13]. A su vez, en el interior de los túneles, cada una de las sesiones

---

[12] SLIP (*Serial Line Internet Protocol*): es un protocolo punto a punto, predecesor de PPP. Sin embargo tienen formas similares de funcionamiento y son protocolos que en general trabajan juntos.

[13] *Spoofing*: Es una técnica de ataque a una red de computadoras, que funciona de tal manera que se actúa como un usuario propio de la red o en nombre de otro usuario de red.

multiplexadas mantendrá un número de secuencia para evitar problemas debidos a la duplicidad de paquetes.

1.9.2.3 L2TP (*Layer 2 Tunneling Protocol*) [4]

Creado como combinación de los protocolos L2F y PPTP, permite el establecimiento de túneles a través de una gran variedad de redes (IP, SONET, ATM) para el transporte de tráfico PPP.

L2TP es un protocolo de nivel 2 que encapsula tramas PPP para ser enviadas sobre IP, X.25, Frame Relay o redes ATM. Cuando se configura para utilizar IP como su protocolo de transporte de información, L2TP se puede usar como un protocolo de enrutamiento punto a punto sobre Internet.

Dado que el protocolo pasajero es PPP, L2TP hereda el mecanismo de autentificación de éste, al igual que los protocolos empleados para el control de la encriptación (ECP[14]) y la compresión (CCP[15]), además de incluir un soporte propio de autentificación que podrá ser empleado en ambos extremos del túnel. La figura 1.12, muestra el canal punto a punto que debe seguir un paquete L2TP a través de una red intermedia.

Los túneles L2TP pueden llevarse a cabo tanto en redes públicas IP como no IP. Esto provoca, que los paquetes de control y los paquetes de datos sean vulnerables frente a posibles ataques tales como *snooping*[16], denegaciones de servicio, modificaciones, o incluso interceptación de los procesos de negociación de la encriptación (ECP) y de la compresión (CCP) con el fin de provocar la supresión de los mecanismos de confidencialidad o en su caso, obtener el acceso a los *passwords* de los usuarios. Para evitar todas estas posibles situaciones, el

---

[14] ECP (*Encryption Control Protocol*): es responsable de la configuración y habilitación de los algoritmos de cifrado o encriptación en ambos extremos del enlace. ECP usa el mismo mecanismo de intercambio de paquetes que LCP.

[15] CCP (*Compression Control Protocol*): Es un protocolo usado para el control de compresión, además tiene un *bit* que se usa para negociar el cifrado.

[16] *Snooping*: Mecanismo de ataque a una red de computadoras, que tiene por objetivo, obtener información sin modificarla.

protocolo de seguridad deberá proporcionar autentificación así como mecanismos para asegurar la integridad y la protección de los paquetes de control, además de la confidencialidad de todos los paquetes. Para poder alcanzar este nivel, es necesario implementar IPSec- ESP.

En L2TP, el canal se crea mediante mensajes L2TP específicos. Los extremos finales del canal se identifican utilizando números de puerto UDP. La porción de datos (carga) de las tramas PPP encapsulados puede opcionalmente cifrarse y comprimirse.

PPTP y L2TP encapsulan el paquete original en una trama PPP y luego añaden cabeceras a la trama PPP para su transmisión a través del canal. Aunque PPTP y L2TP son similares en muchos aspectos, tienen diferencias importantes, entre las que se incluyen las siguientes:

- En PPTP, la red de tránsito debe ser una red IP. En L2TP puede ser IP, circuitos virtuales permanentes (PVC) FR, circuitos virtuales (CV) X.25 o circuitos virtuales ATM. El único requisito de L2TP es que la red física para el canal debe proporcionar conexiones punto a punto orientadas a paquetes.
- PPTP está limitado a un único canal entre dos computadoras. En L2TP se pueden utilizar varios canales y cada canal puede tener una calidad de servicio diferente.
- En L2TP se puede comprimir la cabecera a 4 *bytes,* mientras que en PPTP se puede comprimir la cabecera a 6 *bytes.*
- L2TP tiene mecanismos de autentificación. Por lo mismo, PPTP no ofrece mecanismos de autentificación. Se necesita utilizar otro protocolo como IPSec para ofrecer autentificación. IPSec se puede utilizar en PPTP y L2TP para ofrecer autentificación en el canal. Si IPSec se utiliza con L2TP, la autentificación del canal en el nivel 2, utilizada normalmente en L2TP, se puede reemplazar con el mecanismo de autentificación más robusto de IPSec.

1.9.3 PROTOCOLO DE SEGURIDAD EN INTERNET (IPSec) [4], [9]

IPSec es un protocolo de Capa 3 resultando totalmente transparente a las aplicaciones; IPSec se puede usar directamente entre las máquinas que se comunican, o bien a través de un túnel entre los dispositivos periféricos, denominados *gateways* de seguridad, que las conectan a través de Internet.

IPSec representa un conjunto de mecanismos de seguridad de alta calidad basada en claves criptográficas. Proporciona un canal seguro para los datos a través de la red ofreciendo para ello un control de acceso, así como una integridad en los datos transmitidos además de mecanismos de autentificación y confidencialidad. Los servicios IPSec se apoyan sobre el nivel IP lo que conlleva además un mecanismo de protección para el protocolo IP.

Los protocolos que componen IPSec son: ESP (*Encapsulating Security Protocol*), AH (*Authentication Header*) e IKE (*Internet Key Exchange*). Los dos primeros componen los servicios de seguridad de IPSec, mientras que IKE básicamente administra las claves. IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios: ISAKMP (*Internet Security Association and Key Management Protocol*) y Oakley (*Oakley Key Determination Protocol*). ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

El protocolo AH [10] proporciona únicamente mecanismos de autentificación y dispone de dos modos de operación diferentes: modo transporte y modo túnel. El modo transporte proporciona una protección a los protocolos de niveles superiores y a ciertos campos de la cabecera IP. En este modo, los datos AH son insertados entre la cabecera IP y los datos referentes al paquete de nivel superior (TCP, UDP, ICMP) o bien antes de otro tipo de cabeceras IPSec que ya hubieran sido incluidas (como por ejemplo ESP). En el modo túnel, AH protege la totalidad del datagrama IP, incluyendo la cabecera IP. En cuanto al proceso de inserción,

es totalmente análogo al realizado en modo transporte. El protocolo de autentificación empleado se encuentra especificado de acuerdo a la Asociación de Seguridad (SA, *Security Association*) e incluye códigos de autentificación de mensajes (MAC) basados en algoritmos simétricos como DES y funciones *hash* tales como MD5 y SHA-1.

El protocolo ESP[11], en cambio, proporciona mecanismos de cifrado y autentificación y, como AH, dispone de dos modos de uso: modo transporte y modo túnel. En modo transporte, y al igual que sucede con el protocolo AH, ESP es insertado entre la cabecera IP y los datos de niveles superiores (TCP, UDP, ICMP) o bien antes de otro tipo de cabeceras IPSec que ya hubieran sido incluidas. En el modo túnel, ESP protege la totalidad del datagrama IP interno incluyendo la cabecera IP. En este modo, la cabecera IP interna transporta las direcciones fuente y destino mientras que la cabecera IP externa puede contener direcciones distintas tales como las direcciones de los *gateways* de seguridad. En cuanto al proceso de inserción, es totalmente idéntico al realizado en el modo transporte. El protocolo ESP hace uso de una amplia variedad de algoritmos de criptografía, entre los cuales cabe destacar: DES, 3DES, CAST128 y *Blowfish*[17].

1.9.3.1 Asociación de Seguridad (SA)

La Asociación de Seguridad (SA), es una conexión IPSec entre dos *hosts*, o entre dos *gateways* VPN, o incluso entre un *host* y un *gateway* extremo de un túnel IPSec, utilizada para llevar a cabo la autentificación. Es decir, representa una conexión unidireccional para la cual se definen todos los servicios de seguridad que deben ser aplicados al tráfico de red. Cada SA se define mediante tres componentes:

- Índice de parámetros de seguridad (SPI, *Security Parameter Index*). Es un valor de 32 *bits* usado para identificar diferentes SAs con la misma dirección de destino y protocolo de seguridad.

[17] 3DES, CAST128 y *Blowfish*: Son algoritmos de cifrado. Cuya diferencia entre otras cosas, es que trabajan sobre diferentes bloques de *bits* así: 3DES (168 bits), CAST128 (40-128 *bits*) y *Blowfish* (40-446 *bits*).

- Dirección IP de destino. Puede ser *unicast*, *multicast* o *broadcast* y define el *host*, *gateway* o *router* que va a recibir y procesar la información de la SA.
- Protocolo de seguridad (AH o ESP). Representa el protocolo de seguridad que utiliza la SA. Solo se puede utilizar un protocolo de seguridad para la comunicación definida por una sola SA.

Una implementación de IPSec mantiene dos bases de datos relacionadas a las SAs:

- Base de datos de políticas de seguridad (SPD, *Security Policy Database*). La SPD especifica los servicios de seguridad que se ofrecen al tráfico IP, dependiendo de factores tales como: fuente, destino, si es tráfico saliente o entrante, etc. La SPD contiene una lista ordenada de políticas de entrada, separada para el tráfico entrante y/o saliente. Cada entrada incluye información acerca del tipo de paquetes al cual se debe aplicar la política, como la dirección de origen y destino.
- Base de datos de asociaciones de seguridad (SAD, *Security Association Database*). La SAD define los parámetros asociados a las SAs individuales, tales como: protocolos y claves, números de secuencia y tiempo de vida de la SA. Para el procesamiento saliente, un entrada SPD apunta a una entrada en la SAD. Es decir, la SPD determina qué SA será usada para un paquete dado. Para el procesamiento entrante, la SAD es consultada para determinar cómo el paquete debe procesarse.

Las SAs pueden ser creadas tanto automáticamente como manualmente, empleando para ello el protocolo IKE. Este protocolo presenta tres características principales:

- Asegura que la comunicación IPSec y el intercambio de claves se lleve a cabo entre las partes autentificadas.
- Negocia los protocolos, algoritmos y claves que serán utilizados en la comunicación IPSec.

- Proporciona un método seguro para actualizar y renegociar asociaciones una vez que éstas han expirado.

1.9.3.2 Protocolo IKE

El IETF (*Internet Engineering Task Force*) ha definido el protocolo IKE [12] para realizar tanto la función de gestión automática de claves como el establecimiento de las SAs correspondientes. Una característica importante de IKE es que su utilidad no se limita a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos, como por ejemplo: OSPF o RIPv2.

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

a) La fase uno o fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro y autentificado. Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo de autentificación de mensajes. Las claves necesarias se derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de los nodos, para ello es necesario un paso adicional de autentificación.

   Existen varios métodos de autentificación, así:

   - El *primer* método de autentificación se basa en el conocimiento de un secreto compartido o claves precompartidas que, como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones *hash* cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentifican mutuamente. Para no debilitar la seguridad de este mecanismo de autentificación, debe

configurarse un secreto distinto para cada par de nodos, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de nodos. Por esta razón en entornos en los que se desea interconectar muchos nodos IPSec la gestión de claves es muy complicada. En este caso no se recomienda el uso de autentificación mediante secreto compartido, sino autentificación basada en certificados digitales.

- En los estándares IPSec está previsto el uso de un método de autentificación que se basa en utilizar certificados digitales especificados por la norma X.509v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública.

En la fase uno están definidos dos modos de funcionamiento de IKE:

- *Modo Principal* (Obligatorio). Este modo proporciona varios mensajes a autentificar. Los dos primeros mensajes determinan una política de comunicaciones. Los dos mensajes siguientes intercambian datos públicos de Diffie-Hellman. Los dos últimos mensajes autentifican el intercambio de Diffie-Hellman.
- *Modo Agresivo* (Optativo). Proporciona más información con menos mensajes y confirmaciones. Los dos primeros mensajes determinan una política de comunicaciones e intercambian datos públicos de Diffie-Hellman. A continuación, un tercer mensaje autentifica a la entidad que responde, con lo que termina el proceso de negociación.

b) En la fase dos, el canal seguro IKE es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, en este caso IPSec. Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El

sistema receptor aceptará la primera opción que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

En la fase dos, existen dos modos:

- *Modo Rápido.* El modo Rápido ocurre después de que IKE ha establecido el túnel en la fase uno. El modo Rápido se utiliza para establecer las SAs por cuenta del protocolo de seguridad subyacente.
- *Modo Grupo Nuevo.* El servicio proporcionado por el modo Grupo Nuevo es la creación de SAs adicionales.

1.10 LAS VPNs Y SUS BENEFICIOS [5], [6]

Las redes privadas virtuales implican costos, requisitos organizacionales y cargas de trabajo, también permiten que una compañía obtenga ahorros en el costo al utilizar una red pública en vez de una instalación de línea arrendada.

Respecto a las VPNs se pueden citar varias ventajas:

a) **Ahorro con la implementación de VPNs:** Al abreviar muchos de los dispositivos asociados con la infraestructura de telecomunicaciones de las líneas arrendadas y el equipo de acceso remoto costoso, se puede reducir los costos del servicio telefónico de larga distancia, también se reduce el tiempo que el personal de la corporación invierte en la administración y en el mantenimiento de estos dispositivos.

b) **Beneficios en el diseño de red:** El diseño de red es un área donde la tecnología VPN realmente puede ser benéfica desde el punto de vista de diseño arquitectónico, flexibilidad y mantenimiento. La necesidad de un diseño de una red WAN compleja, con cálculos de desempeño del enlace, ajustes en el tamaño del ancho de banda y redundancia, ya no representa un problema para una organización. En este punto, la principal preocupación es la conexión

a Internet con un proveedor ISP local, quien manejará todos los problemas asociados con la conexión.

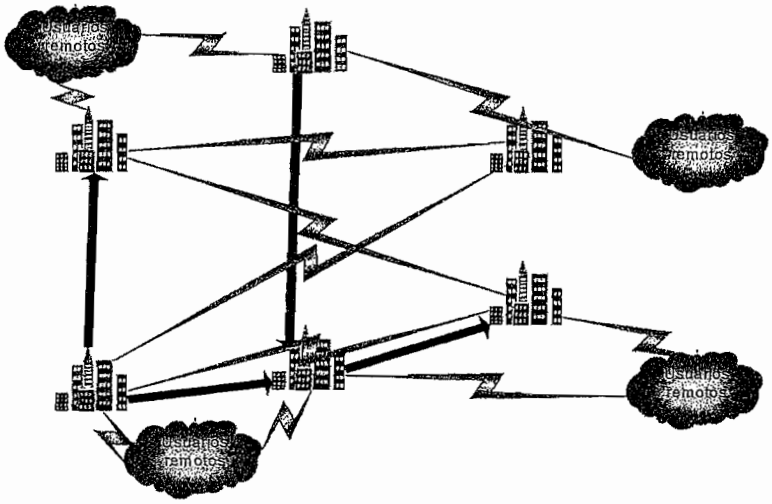


Figura 1.13: WAN sobre líneas arrendadas [6]

La figura 1.13, ilustra lo que tiene que enfrentar un administrador de una red típica cuando diseña una WAN sobre líneas arrendadas. El administrador de red debe preocuparse por el flujo de tráfico entre departamentos ubicados en distintos puntos geográficos, edificios y ciudades, y crear el tamaño del conducto adecuado para este tráfico.

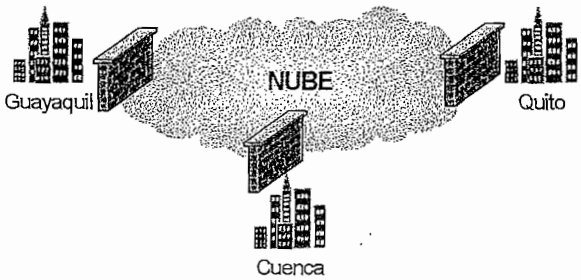


Figura 1.14: Conexión a un ISP para la conectividad de una WAN [6]

Con la tecnología VPN, todo el trabajo se reduce; como se muestra en la figura 1.14, todo lo que se requiere es una conexión a Internet y el ISP se encarga del transporte. La principal consideración que se debe tener, es

seleccionar el ancho de banda correcto para el ISP. Será necesario que se examinen los patrones de tráfico en las redes y que se estime el porcentaje de este tráfico que necesitará acceso a Internet.

c) **Pagar sólo lo necesario:** Además de los costosos cargos telefónicos de larga distancia en los que se incurre, están los costos de las sucursales y las oficinas remotas. Con líneas arrendadas, retransmisión de tramas u otra infraestructura, se tiene que pagar por el tiempo de inactividad. Aun si no se está utilizando el servicio, se está cobrando. En el caso de Internet, sólo paga por el tiempo en línea, lo cual generalmente consiste de una llamada local además de una cuota mensual.

d) **Acceso a datos:** En un escenario normal, un proveedor necesita una propuesta, un contrato u otro documento como presentación ante el cliente. Comúnmente se debe marcar a la red corporativa y acceder a alguna Intranet. Con la VPN instalada puede establecer una conexión directa al servidor en cuestión y transferir la información apropiada, eliminado la necesidad de preguntarle al cliente potencial si tiene una línea al exterior que pueda utilizar para establecer una conexión por marcación.

e) **Asignación de prioridades de tráfico:** Varios proveedores ofrecen asignación de tráfico a través de la tecnología VPN. Esto añade gran flexibilidad a la utilización de tráfico de una compañía mediante su enlace con Internet. Ya que las VPNs ofrecen acceso a una Extranet, a una Intranet o servidores internos de una organización, es posible decidir que sólo se permita pasar libremente cierto tipo de tráfico, con el fin de conservar el ancho de banda, mientras que otro tipo de tráfico queda en cola de espera, según su importancia. En las instalaciones de ciertas topologías se puede dirigir todo el tráfico de la VPN a través de un enlace y todo el tráfico que no es de la VPN a través de otro.

f) **Beneficios para los ISP:** Los ISPs pueden beneficiarse de la tecnología VPN. Serán capaces de proporcionar a sus clientes todos los tipos de servicios que

demandan los negocios actuales. En un futuro próximo, las compañías telefónicas cobrarán por el paquete. Los ISPs harán lo mismo, es decir cobrarán a sus clientes una cuota basada en paquetes.

g) **Ancho de Banda:** El ancho de banda puede tener diferentes significados: el ancho de banda del medio físico hacia el proveedor, o el ancho de banda disponible sobre el *backbone* del ISP. Este último, por lo general es bastante grande y comúnmente se ubica en el rango de *terabits* por segundo. Esta increíble disponibilidad de ancho de banda se ha vuelto posible gracias a la tecnología de Red óptica sincrónica (SONET).

h) **Latencia:** Es el concepto relacionado con el retraso en el establecimiento inicial del enlace en la comunicación entre dos puntos. Las conexiones de la red atravesarán dos, tres o varios *backbone*s del ISP. Entonces es probable que se obtenga una garantía de latencia únicamente a través del *backbone* del ISP.

BIBLIOGRAFÍA – CAPÍTULO 1

[1] KOSIUR Dave, "*Building and Managing Virtual Private Networks*", 1era edición, Editorial Wyley, 1998.

[2] TANENBAUM Andrew, "Redes y Ordenadores", Editorial Prentice Hall, 1996.

[3] STALLINGS William, "Comunicaciones y Redes de computadoras", 5ta edición, Editorial Prentice Hall PTR.

[4] KARANJIT Siyan, "Microsoft Windows 2000 TCP/IP", Editorial Prentice Hall PTR, Madrid.

[5] MURHAMMER Martin W, "*A guide to Virtual Private Networks*", Editorial Prentice Hall PTR, 1998.

[6] BROWN Steven, "Implementación de Redes Privadas Virtuales", Editorial McGraw-Hill, 2000.

[7] RIVEST R., "*The MD5 Message - Digest Algorithm*", RFC 1321, Abril 1992.

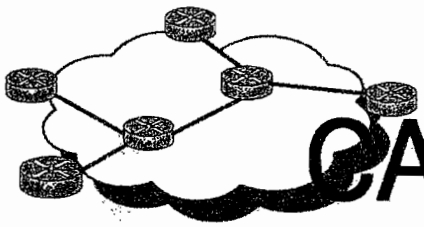
[8] MICROSOFT CORPORATION, "*Understanding Point-to-Point Tunneling Protocol (PPTP)*", http://www.microsoft.com

[9] KENT S., ATKINSON R., "*Security Architecture for the Internet Protocol*", RFC 2401, Noviembre 1998.

[10] KENT S., ATKINSON R., "*IP Authentication Header*", RFC 2402, Noviembre 1998.

[11] KENT S., ATKINSON R., "*IP Encapsulating Security Payload* (ESP)", RFC 2406, Noviembre 1998.

[12] HARKINS D., CARREL D., "*The Internet Key Exchange* (IKE)", RFC 2409, Noviembre1998.



CAPÍTULO 2

ARQUITECTURA MPLS

2.1 INTRODUCCIÓN

Con el advenimiento del *World Wide Web* (WWW), el Internet ha visto el enorme crecimiento de sus raíces. Miles de usuarios corporativos y millones de usuarios residenciales han ido integrándose en los últimos años, haciendo de Internet una verdadera red pública de datos. Este acelerado crecimiento en la suscripción ha conducido a una oleada de datos en el *backbone* de Internet. Para mantener la creciente demanda en el servicio y ancho de banda, todos los ISPs han aumentado sus redes en tamaño y ancho de banda.

Internet, fue diseñado para transportar aplicaciones tolerantes en el tiempo; es decir, aplicaciones como correo electrónico, FTP, Telnet, HTTP, donde el tiempo de envío y respuesta no es un problema importante. De allí que el actual Internet ofrece un servicio básico conocido como el mejor esfuerzo, "*best effort*", donde la red no hace ninguna distinción entre cada aplicación.

Con la aparición de nuevas aplicaciones de tiempo real, como telefonía o voz sobre IP (VoIP), el uso de teléfonos móviles con acceso a Internet (*WAP, Wireless Application Protocol*), telecontrol, videoconferencias, teleducación, entre otros; ha incitado a proponer y desarrollar nuevos modelos para que el Internet del futuro asegure una buena calidad de servicio (QoS[1]) dependiendo de la importancia de los datos que se envían a la red.

Recientemente, se propuso un nuevo enfoque para no solo ofrecer QoS en redes IP, sino para optimizar la QoS en redes como ATM y Frame Relay, este enfoque es denominado MPLS (*Multiprotocol Label Switching*). Es así como se define esta arquitectura, donde los paquetes de datos en lugar de ser enrutados en la capa 3 (IP *routing*) ahora son conmutados en la capa 2 (IP *switching*).

---

[1] Desde una perspectiva comercial, la QoS es esencial para asegurar que las aplicaciones críticas tengan garantizados los recursos de red que ellas necesitan; para mayores detalles, ver los capítulos 3 y 5.

2.2 ORÍGENES [7]

MPLS nace de los numerosos esfuerzos a mediados de los años 90, por combinar las tecnologías IP y ATM. Uno de los primeros esfuerzos que llegó al mercado fue IP *Switching*, desarrollado por **Ipsilon**. Para competir con esta oferta, numerosas compañías anunciaron sus propios productos, entre éstos: **Cisco** (*Tag Switching*), **IBM** (*ARIS, Aggregate Route-based IP Switching*) y **Cascade** (*IP Navigator*). La meta de todos estos productos era mejorar el *throughput* y la demora en el funcionamiento de IP y todos tomaron el mismo enfoque básico: Usar un protocolo estándar de enrutamiento tal como OSPF (*Open Shortest Path First*), para definir caminos entre puntos terminales, distribuyendo paquetes cuando ingresen a la red y usar *switches* ATM para trasladar los paquetes a lo largo de los caminos. Cuando estos productos salieron, los *switches* ATM eran mucho más rápidos que los *routers* IP.

En respuesta a estas iniciativas, el IETF (*Internet Engineering Task Force*), organizó el grupo de trabajo MPLS en 1997 para desarrollar un estándar común. El grupo de trabajo entregó su primera serie de estándares en el 2001. Sin embargo el mercado no se detenía. A finales de los años 90, se introdujeron *routers* tan rápidos como los *switches* ATM, eliminando la necesidad de proveer ambas tecnologías IP y ATM en la misma red.

No obstante, MPLS tiene un fuerte papel que desempeñar. MPLS reduce la cantidad de procesamiento por paquete, requerido en cada *router* en una red basada en IP, aumentando el desempeño de un *router* cada vez más. Más aún, MPLS provee nuevas capacidades significativas en cuatro áreas que han asegurado su popularidad: soporte de calidad de servicio (QoS), Ingeniería de Tráfico, Redes Privadas Virtuales (VPNs) y un soporte multiprotocolo.

MPLS nace con la idea de integrar las mejores características de la capa 2 y la capa 3, sustituyendo a las actuales técnicas de túneles (*tunneling*) para encaminar tráfico IP sobre ATM. Además surge para consensuar diferentes soluciones de conmutación multinivel.

Las principales premisas a la hora de definir el estándar, han sido las siguientes:

- Debe funcionar sobre cualquier tecnología de transporte, no sólo sobre ATM.
- Soportar envíos tanto *Unicast* como *Multicast.*
- Compatible con RSVP (*Resource ReSerVation Protocol*) y los servicios integrados del IETF.
- Compatible con los actuales modos de funcionamiento de redes IP existentes.
- Debe admitir herramientas de soporte, administración y mantenimiento al menos tan fiables como las que soportan las actuales redes IP.
- Permitir un crecimiento constante de Internet, ampliando su capacidad para convertirse en un medio universal para el transporte de datos, no sólo para la distribución de contenidos.

2.3 COMPONENTES DE MPLS [1]

MPLS emplea nuevas mejoras al enrutamiento IP para el envío de paquetes. Los componentes de MPLS permiten que funcione a un grado más alto de desempeño e inteligencia que las tecnologías actuales. También proporcionan una manera más eficaz de enviar los paquetes de la fuente al destino que la basada en el modo *hop by hop*, usada en el enrutamiento tradicional. Muchos de sus componentes simplemente son extensiones de tecnologías ya existentes tales como las extensiones agregadas a los protocolos de enrutamiento actuales. Adicionalmente, la funcionalidad de los *routers* MPLS simplemente puede agregarse por ejemplo actualizando el *software* de los *switches* ATM.

La arquitectura MPLS diferencia dos tipos de *routers*:

2.3.1 LER (*LABEL EDGE ROUTER*)

Los LERs o *routers* de etiqueta de borde, son equipos que están situados en la periferia de la red MPLS (ver figura 2.1). Los LERs unen diferentes subredes

(Ethernet, Frame Relay, ATM) a la red MPLS y además son los encargados de asignar y retirar las etiquetas, a la entrada o salida de la red MPLS. Su conmutación se basa en FECs (*Forwarding Equivalence Classes*).

2.3.2 LSR (*LABEL SWITCHING ROUTER*)

Los LSRs o *routers* de conmutación de etiquetas (ver figura 2.1), son equipos de conmutación (por ejemplo: *routers* IP o *switches* ATM) habilitados para MPLS. Este componente trabaja en el núcleo de la red MPLS, por tanto su conmutación es directa.

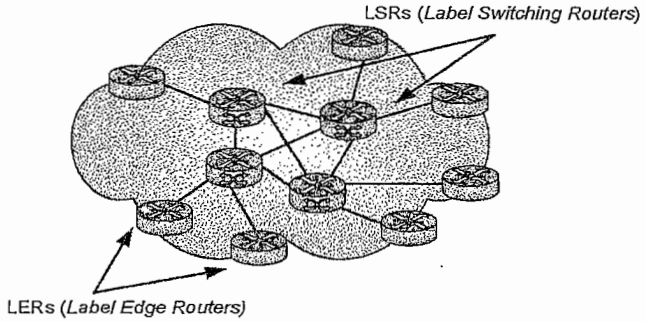


Figura 2.1: LERs y LSRs

Usan un protocolo de distribución de etiquetas, que no necesariamente es el mismo en todos los LSRs y su función es encaminar los paquetes, basados únicamente en la etiqueta de dicho paquete. Cuando los paquetes llegan a los LSRs, éstos intercambian las etiquetas existentes por otras, y envía el paquete al siguiente LSR, y así sucesivamente.

2.3.3 FEC (*FORWARDING EQUIVALENCE CLASS*)

La Clase Equivalente de Envío es una representación de un grupo de paquetes que comparten los mismos atributos: el mismo destino, la misma VPN, etc. y/o requieren el mismo servicio: flujo, *multicast*, QoS. Paquetes de un mismo flujo de datos generalmente pertenecen a una misma FEC. Todos los paquetes en el grupo tienen el mismo tratamiento en la ruta al destino. En oposición al envío convencional IP, en MPLS, la asignación de un paquete particular a una FEC particular se hace solo una vez, cuando el paquete ingresa a la red. Las FECs son

usualmente construidas mediante información aprendida a través de un IGP (*Interior Gateway Protocol*), como es el caso de OSPF (ver Anexo A).

Una FEC es representada por una etiqueta en cada LSP (*Label Switched Path*), un LSP es un camino especifico a través de una red MPLS (ver la sección 2.3.5). Al recibir un paquete el LER verifica qué FEC le pertenece y lo encamina por el LSP correspondiente (ver figura 2.2).

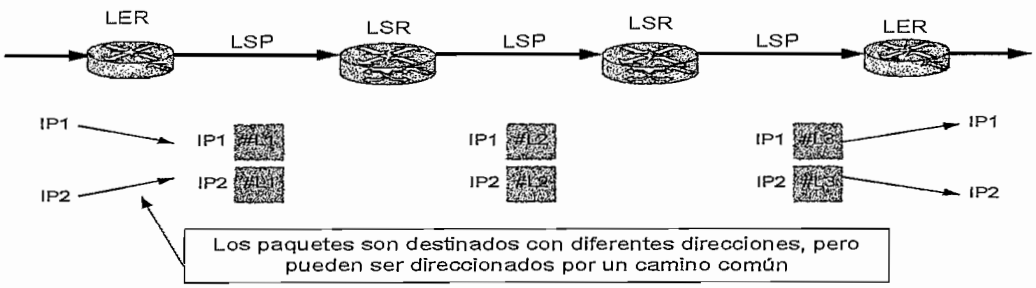


Figura 2.2: FEC (Forwarding Equivalence Class)

2.3.4 ETIQUETA

Una etiqueta es un conjunto pequeño de *bits* de longitud fija, que lleva el paquete en su cabecera para identificar una FEC. Una etiqueta es análoga al identificador de conexión usado en ATM, como son los VPI/VCI o los DLCI (*Data Link Connection Identifier*) usados en FR. La validez de una etiqueta es local, solo entre un par de nodos, y es reemplazada en cada salto en el LSP (ver figura 2.2).

Las decisiones de asignación de etiquetas pueden estar basadas en criterios de envío tales como: ingeniería de tráfico, *multicast*, redes privadas virtuales (VPNs), QoS. Las etiquetas son asociadas a un flujo específico de datos unidireccional. Las etiquetas son asociadas a una FEC como resultado de algún evento o política que indica una necesidad para tal asociación. Estos eventos pueden ser manejados por el flujo de datos (*data-driven bindings* [2]) o manejados por el tráfico de control (*control-driven bindings* [3]).

---

[2] *Data-driven bindings*: Asociación dinámica de una etiqueta a una FEC basada en el flujo de datos.
[3] *Control-driven bindings:* Esta es una forma estática de asociación. Se usan mensajes de control (como el Protocolo de distribución de etiquetas) o comandos específicos predeterminados y parámetros para asociar una etiqueta a una FEC.

2.3.4.1 Asignación de etiquetas

Se tienen dos casos para la asignación de etiquetas:

- La asignación de etiquetas normalmente ocurre en forma dinámica según la situación presente en el "tráfico de datos", lo que se conoce como ***asignación de etiquetas derivada del tráfico***. La asignación se inicia con una nueva comunicación que demande el uso de etiquetas, el LSP se establece bajo demanda solamente cuando hay tráfico por enviar.
- El establecimiento de etiquetas es ordenado, mediante señalización (es decir, se deriva del tráfico de control) entre nodos de la red. Por ejemplo, un LSR puede en cierto momento decidir actualizar sus tablas de envío y cambiar las etiquetas que venía manejando para sus entradas. Esto puede suceder ante situaciones anormales que pueden presentarse en la red o en un nodo.

  El LSR procederá a informar las nuevas etiquetas a sus nodos vecinos, esto es lo que se conoce como ***asignación de etiquetas derivada de la topología***. Otro caso de señalización es cuando la capa Internet usa protocolos de QoS propios de IP como RSVP, el cual reserva recursos en la red para determinado servicio, lo cual a su vez puede conllevar a cambios de etiquetas en las tablas de envío del LSR, esto es lo que se conoce como ***asignación de etiquetas derivada por solicitud.***

La asignación de etiquetas derivada de la topología y asignación de etiquetas derivada por solicitud son ejemplos de *control-driven bindings*, mientras que la asignación de etiquetas derivada del tráfico es un ejemplo de *data-driven bindings*.

La escalabilidad es significativamente mejor en el modelo *control-driven*, porque el número de LSPs es proporcional al número de entradas en la tabla de envío y no al número de flujos de tráfico individuales. En una topología estable, el *overhead* por la asignación y distribución de etiquetas es más baja que en el modelo *data-driven* porque los LSP son establecidos solamente después de un cambio en la

topología o por la llegada del tráfico de control y no cuando llega un nuevo flujo de tráfico de datos. MPLS usa el modelo *control-driven*.

2.3.4.2 Asignación y distribución de etiquetas

Si se considera el caso de paquetes fluyendo del LSR **A** hacia el LSR **B**. **A** es el LSR *upstream* (**Ru**) y **B** es el LSR *downstream* (**Rd**). En la arquitectura MPLS, la decisión para asociar una etiqueta particular a una FEC particular es realizada por el LSR, el cual es *downstream* con respecto a esa asociación. El LSR *downstream* entonces informa al LSR *upstream* de tal asociación. Siempre el LSR *downstream* garantiza la unicidad de las etiquetas recibidas de todo Ru.

La asignación puede ser local o remota:

- **Local:** se elige y se asigna localmente una etiqueta.
- **Remota:** se recibe de otro LSR información de la asignación de otro *router*.

A su vez, la asignación puede ser *Downstream* o *Upstream*.

- ***Downstream:*** etiquetas de asignación local se usan como etiquetas de entrada. Etiquetas de asignación remota se usan como etiquetas de salida.
- ***Upstream:*** etiquetas de asignación local se usan como etiquetas de salida y etiquetas de asignación remota se usan como etiquetas de entrada.

2.3.4.2.1 Asignación de etiquetas Downstream.

La asignación ***Downstream*** (ver figura 2.3) se denomina así debido a que la asociación entre una etiqueta que lleva el paquete y una FEC particular a la cual pertenece el paquete, es creada por el LSR que es *downstream* (respecto al flujo de paquetes) con respecto del LSR que pone la etiqueta en el paquete. Se puede observar que los paquetes que llevan una etiqueta particular fluyen en la dirección opuesta al flujo de información de la asignación respecto a la etiqueta.

2.3.4.2.2 Asignación de etiquetas Upstream.

La asignación ***Upstream*** (ver figura 2.3) se denomina así debido a que la asociación entre una etiqueta que lleva un paquete y una FEC particular a la cual pertenece el paquete, es creada por el mismo LSR que pone la etiqueta en el paquete, es decir, el creador del enlace es *upstream* respecto al flujo de paquetes. Se puede observar que los paquetes que llevan una etiqueta particular fluyen en el mismo sentido que la información de la asignación respecto a la etiqueta.

La mayoría de las aplicaciones usan asignación *downstream* con dos variantes: *Downstream* No solicitado y *Downstream* Bajo Demanda.

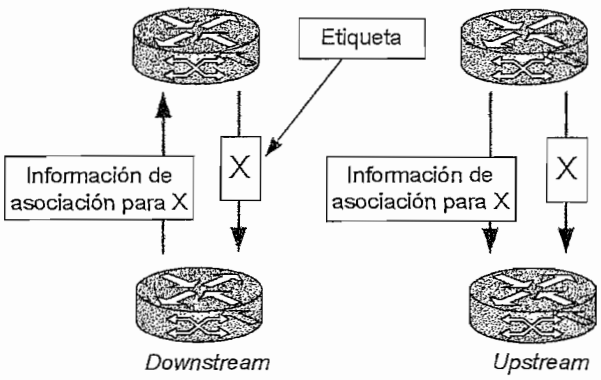


Figura 2.3: Asignación Downstream y Upstream

2.3.4.2.3 Downstream No solicitado versus Downstream Bajo Demanda

La arquitectura MPLS permite a un LSR hacer una solicitud específica de asociación de etiqueta para una determinada FEC y completar el siguiente salto, esto es conocido como distribución de etiquetas mediante *Downstream* bajo demanda; es decir el *router upstream* hace una petición de etiqueta para una determinada FEC al *router downstream*, el *router downstream* comunica dicha asociación al *router upstream* y apunta la etiqueta recibida en la tabla de etiquetas como salida (ver figura 2.4 a).

La arquitectura MPLS también permite a un LSR la distribución de asociaciones etiqueta/FEC a LSRs que no tienen solicitudes explícitas. Esto es conocido como

distribución de etiquetas mediante *Downstream* No solicitado, es decir un LSR toma la decisión de asignar una etiqueta a una FEC y comunica la asociación a los *routers upstream* (ver figura 2.4 b).

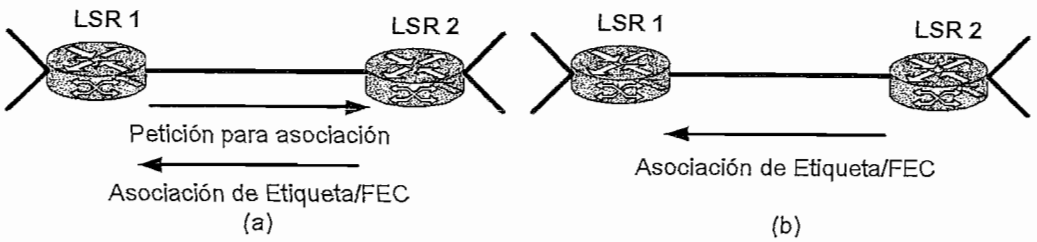


Figura 2.4: Downstream Bajo Demanda vs. Downstream No solicitado

Algunas implementaciones de MPLS proveen solamente *downstream* bajo demanda y otras implementaciones proveen solamente *downstream* no solicitado, pero también hay algunas implementaciones que pueden proveer ambas, todo dependerá de las características de las interfaces y del tipo de implementación que se realice. Sin embargo, estas dos técnicas de distribución de etiquetas pueden ser usadas en la misma red y al mismo tiempo. Para cualquier distribución de etiqueta adyacente dada, el LSR *upstream* y el LSR *downstream* pueden ponerse de acuerdo en la técnica a ser usada.

2.3.4.3 Control de la distribución de etiquetas

MPLS define modos para el control de la distribución de etiquetas a los LSRs vecinos. Se definen los siguientes modos:

Independiente: En este modo, un *router* MPLS envía una nueva etiqueta al LSR *upstream* aun cuando no tenga una etiqueta para esa FEC. Se lo comunica a los LSRs *upstream* y la apunta en su tabla de etiquetas como entrada.

Ordenado: En este modo, un LSR no anuncia una nueva etiqueta al LSR *upstream* hasta que una etiqueta para esa FEC llega desde el LSR *downstream*, la apunta en la tabla de etiquetas como salida; por consiguiente, el *router* de borde en la salida de la red MPLS es el primer *router* en anunciar una etiqueta. Entonces

realiza la asignación de la FEC a una etiqueta local y la apunta en la fila de entrada y comunica la asociación a los LSRs *upstream.*

2.3.4.4 Modo de retención de etiquetas

Un LSR puede recibir (o ha recibido) la asignación de etiqueta para una FEC dada desde un Rd, aunque Rd no sea el próximo salto de Ru para esa FEC (ver figura 2.5). Ru entonces tiene la opción de conservar el rastro de tal asignación o descartarla.

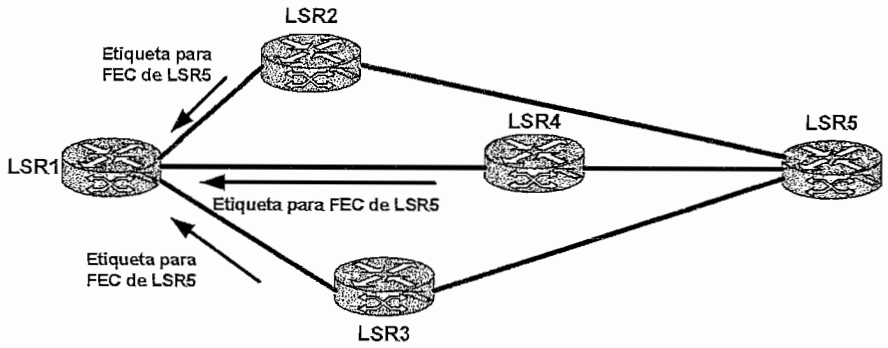


Figura 2.5: Modo de retención de etiquetas [9]

Si el Ru mantiene la asignación, entonces éste puede inmediatamente empezar a usar la asignación otra vez, si Rd finalmente llega a ser su próximo salto para la FEC en cuestión. Si Ru descarta la asignación, entonces si Rd más tarde llega a ser el siguiente salto, la asignación tendrá que ser requerida nuevamente. Así, se definen dos modos:

Modo de retención de etiqueta Liberal: en este modo, las asociaciones entre una etiqueta y una FEC que se reciben de LSRs que no son el próximo salto para una FEC dada, se retienen. Este modo permite una adaptación rápida a cambios de topología y permite la conmutación de tráfico a otros LSPs en caso de cambios.

Modo de retención de etiquetas Conservador: en este modo, las asociaciones entre una etiqueta y una FEC que se reciben de LSRs que no son el próximo salto

para una FEC dada, se desechan; es decir, un LSR sólo retiene las etiquetas asignadas a una FEC por medio de sus vecinos *downstream* actuales.

2.3.4.5 Formato de la cabecera MPLS

La cabecera MPLS es un identificador de 32 *bits* (ver figura 2.6), que consiste de los siguientes campos:

Etiqueta: 20 *bits*, valor de etiqueta que localmente representa a la FEC durante el envío. La tabla 2.1, muestra los valores de etiquetas reservadas.

Etiqueta	Descripción
0	Etiqueta nula explícita IPv4. Una etiqueta que simplemente tiene un valor EXP. Un valor de cero (0) representa la etiqueta nula explícita. Esta etiqueta sólo puede estar en el fondo de la pila de etiquetas. Indica que la pila de etiquetas debe ser removida y el envío del paquete debe hacerse basado en la cabecera IPv4. A veces puede haber requisitos de tener una etiqueta en la pila cuando ninguna etiqueta es requerida.
1	Etiqueta Alerta de *Router*. Esta etiqueta es análoga al uso de la opción "Alerta de *Router*" en paquetes IP. Este valor de etiqueta es lícito en cualquier parte de la pila de etiquetas excepto en el fondo.
2	Etiqueta nula explícita IPv6. Un valor de cero (0) representa la etiqueta nula explícita. Esta etiqueta sólo puede estar en el fondo de la pila de etiquetas. Indica que la pila de etiquetas debe ser removida y el envío del paquete debe hacerse basado en la cabecera IPv6.
3	Etiqueta nula implícita. Esta es una etiqueta que un LSR puede asignar y puede distribuir, pero que nunca aparece realmente en la encapsulación. Cuando un LSR debería reemplazar la etiqueta en la cima de la pila con una nueva etiqueta, pero la nueva etiqueta es "Nula Implícita", el LSR removerá la pila en lugar de hacer el reemplazo. Esta es usada para PHP (*Penultimate Hop Popping*) [4].
4 - 15	Reservadas para su uso futuro.

Tabla 2.1: Valores de las Etiquetas Reservadas

EXP: 3 *bits*, para identificar la clase de servicio en el campo EXP experimental, (anteriormente llamado CoS, *Class of Service*) o Clase de Servicio, siendo usado para la prioridad de tráfico y QoS.

[4] PHP (*Penultimate Hop Popping*) u omisión del penúltimo salto, es necesario solo para subredes directamente conectadas; ya que la información del paquete saliente de capa 2 (por ejemplo: la dirección física) está disponible en la tabla de envío.

S (*Stack*): 1 *bit*, se utiliza para indicar una pila de etiquetas jerárquica (S), el campo S toma el valor de 1 en la etiqueta que se encuentra en la cima de la pila y cero en todas las etiquetas restantes.

TTL: 8 *bits* para indicar el TTL (*Time To Live*) que sustenta la funcionalidad estándar TTL de las redes IP. Número de saltos que puede hacer un paquete antes de llegar al destino dentro de un dominio MPLS. Un campo importante en la cabecera del paquete IP es el campo TTL (IPv4) o *Hop Limit* (IPv6). Como en un paquete IP, un paquete MPLS tiene un campo TTL, el campo es decrementado en cada *router* y el paquete es excluido si la cuenta cae a cero. Esto es para evitar lazos o que el paquete permanezca demasiado tiempo en la red debido a un enrutamiento defectuoso. Un LSR no examina la cabecera IP, el campo TTL es incluido en la etiqueta para que la función TTL todavía sea soportada. Hay que notar que ATM y Frame Relay no usan el concepto de TTL.

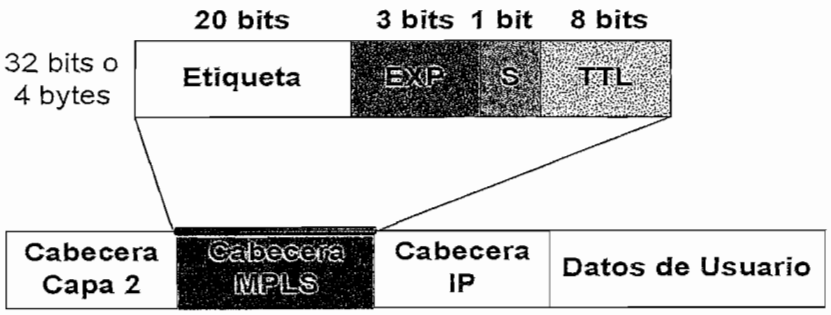


Figura 2.6: Estructura de la cabecera genérica MPLS

2.3.4.6 Pila de etiquetas o etiquetas en *stack*

Uno de los aspectos más poderosos de MPLS es la pila o acumulamiento de etiquetas. Un paquete etiquetado puede llevar muchas etiquetas, organizado como una pila LIFO de etiquetas (último en entrar primero en salir). El procesamiento está siempre basado en la etiqueta de la cima. En cualquier LSR, la etiqueta puede ser añadida a la pila (operación *push*) o removida de la pila (operación *pop*). El apilamiento de etiquetas (ver figura 2.7) permite la agregación de LSPs en un solo LSP para una porción de la ruta a través de una red, creando un túnel.

Al principio del túnel, un LSR asigna la misma etiqueta a los paquetes de un número de LSPs colocando la etiqueta sobre la pila de cada paquete. Al final del túnel, otro LSR extrae el elemento de la cima de la pila de la etiqueta, mostrando la etiqueta interna. Esto es similar a ATM que tiene un nivel de pila (canales virtuales dentro de caminos virtuales), pero MPLS soporta una pila ilimitada. La pila de etiquetas proporciona una considerable flexibilidad en la transmisión de la información.

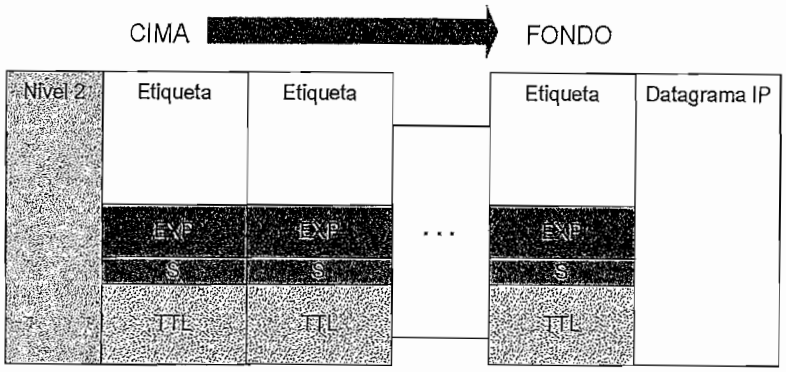


Figura 2.7: Pila de Etiquetas [9]

Aunque, como se verá más adelante, MPLS soporta una jerarquía, el proceso de etiquetación de un paquete es completamente independiente del nivel de jerarquía. Este proceso está basado en la etiqueta de más alta numeración, sin contemplar la posibilidad de que algún número de otra etiqueta haya sido anteriormente la más alta o que otro número de alguna etiqueta haya estado por debajo de esa.

Un paquete sin etiquetar puede pensarse como un paquete cuya pila de etiqueta está vacía (e.d cuya pila de etiqueta tiene una profundidad 0 (*depth* 0)). Si la pila de la etiqueta de un paquete es de profundidad m, se referirá a la etiqueta en el fondo de la pila como la etiqueta de nivel 1, a la etiqueta sobre él (si existe) como la etiqueta de nivel 2 y a la etiqueta en la cima de la pila como la etiqueta de nivel m. La utilidad de etiquetas en pila llega a ser muy buena cuando se introduce la noción de túnel LSP y de jerarquía en MPLS.

2.3.4.7 Encapsulación de Etiquetas

La pila de etiquetas aparece después de la cabecera de capa enlace, pero antes de la cabecera de capa red. El paquete de capa red sigue inmediatamente a la entrada de la pila de etiquetas que tiene el *bit* S puesto a 1. En una trama de capa enlace como para PPP (*Point-to-Point Protocol*) la pila de etiquetas aparece entre la cabecera IP y la cabecera de capa enlace (figura 2.8 a). Para una trama IEEE 802 la pila de etiquetas aparece entre la cabecera IP y la cabecera LLC (*Logical Link Control*), figura 2.8 b.

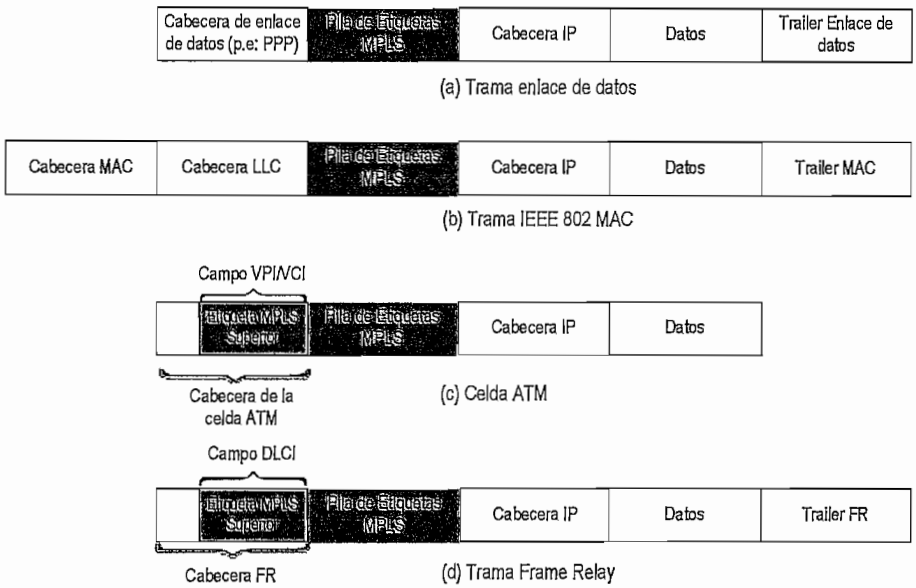


Figura 2.8: Encapsulación ATM, Frame Relay y IEEE 802

Si MPLS es usada sobre una red de servicios orientada a conexión, puede asumirse un enfoque ligeramente diferente, como se muestra en las figuras 2.8 c y d. Para celdas ATM, el valor de la etiqueta que se encuentra en la cima de la pila es colocada en el campo del identificador de camino y canal virtual (VPI/VCI) en la cabecera de la celda ATM. La etiqueta más alta permanece en la cima de la pila, la cual es insertada entre la cabecera de la celda y la cabecera IP.

Colocando el valor de la etiqueta en la cabecera de la celda ATM facilita la conmutación por un *switch* ATM, el cual solo necesita mirar la cabecera de la

celda. Similarmente, el valor de la etiqueta que se encuentra en la cima de la pila es colocado en el campo DLCI de una cabecera FR. Se debe notar que en estos dos casos, el campo TTL no es visible al *switch* y éste no es decrementado.

Con la cabecera de la pila de etiquetas MPLS insertada entre la cabecera de la capa 2 y la carga útil (*payload*) de la capa 3, el *router* emisor debe tener algunos medios para indicar al *router* receptor que el paquete que se transmite no es un paquete IP, sino un paquete etiquetado (un paquete MPLS). Para facilitar esto, se han definido nuevos tipos de protocolos definidos sobre la capa, así:

- En ambientes LAN, los paquetes etiquetados que transportan paquetes de capa 3 *unicast* y *multicast* usan valores 0x8847 y 0x8848. Estos valores *ethertype* pueden usarse directamente en medios Ethernet (incluyendo Fast Ethernet y Gigabit Ethernet) y también como parte de la cabecera SNAP en otro medio LAN (incluyendo Token Ring y FDDI).
- En los enlaces punto a punto que emplean la Encapsulación PPP, se introdujo un nuevo protocolo de control de red (NCP, ver sección 1.9.1), denominado Protocolo de Control MPLS (MPLSCP, *MPLS Control Protocol*). Los paquetes MPLS están marcados con el protocolo PPP, cuyo valor de campo es 0x8281.
- Los paquetes MPLS transmitidos a través de un DLCI FR entre un par de *routers* se marcan con el ID del protocolo de capa de red Frame Relay SNAP (NLPID) seguido de una cabecera SNAP con el valor *ethertype* 0x8847.
- Los paquetes MPLS transmitidos entre un par de *routers* por un circuito virtual ATM se encapsulan con una cabecera SNAP que utiliza valores *ethertype* iguales a los utilizados en el ambiente LAN.

2.3.5 LSP (*LABEL SWITCHED PATH*)

Un LSP se forma con la concatenación de varios LSRs, los cuales forman para un paquete etiquetado, un camino por el cual viajarán los paquetes hasta alcanzar el LSR de salida, es decir es el camino lógico que un paquete MPLS toma a través

de la red. Un LSP es funcionalmente equivalente a un circuito virtual, porque define un camino de entrada y salida a través de la red, este camino es el mismo para paquetes de la misma FEC, entonces un LSP es un camino unidireccional de origen a destino (ver figura 2.9). Para el retorno de tráfico se tomará otro camino.

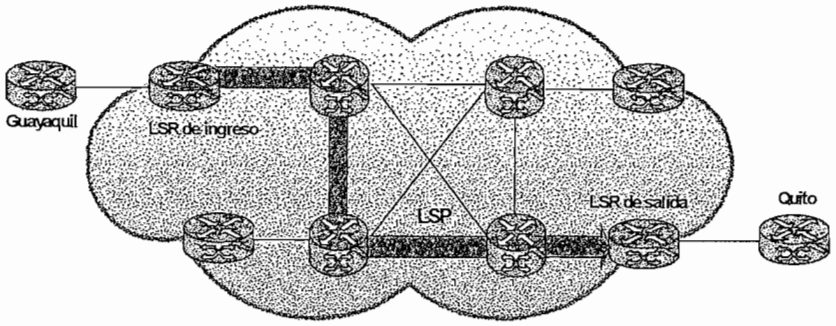


Figura 2.9: LSP (Label Switched Path)

En el interior de la red, los conmutadores de etiquetas ignoran la cabecera de la capa red de los paquetes y simplemente envían el paquete usando el algoritmo de etiquetas. Así los proveedores de servicio pueden diseñar LSPs personalizados que soporten aplicaciones y requerimientos específicos. Los LSPs pueden ser asignados a un mínimo de saltos, reunir ciertos requerimientos para el ancho de banda, requerimientos de apoyo precisos, *bypass* para los puntos de congestión, tráfico directo fuera del camino dado por el IGP (*Interior Gateway Protocol*) o simplemente forzar el tráfico a cruzar ciertos enlaces o nodos en la red.

La arquitectura MPLS soporta dos opciones para seleccionar una ruta o LSP para una FEC particular: enrutamiento *hop by hop* y enrutamiento explícito.

Con el **enrutamiento *hop by hop***, cada LSR independientemente escoge el próximo *salto para* cada FEC. Esta opción hace uso de un protocolo de enrutamiento ordinario, como OSPF. Además esta opción proporciona algunas de las ventajas de MPLS, incluyendo rápida conmutación de las etiquetas, y tratamiento diferencial de paquetes de diferentes FECs que siguen la misma ruta.

Sin embargo, debido al uso limitado del desempeño de la métrica en protocolos de enrutamiento típicos, el enrutamiento *hop by hop* no soporta fácilmente

ingeniería de tráfico[5] o políticas de enrutamiento (definición de rutas basadas en algunas políticas relacionadas a la QoS, seguridad).

Con el **enrutamiento explícito (ER-LSP)**, usualmente un LSR de ingreso o salida, especifica algunos o todos los LSRs en el LSP para una FEC dada. Para un **enrutamiento explícito estricto**, un LSR especifica todos los LSRs en un LSP, es decir especifica una lista de nodos usando la dirección real de cada nodo a recorrer. Para un **enrutamiento explícito libre**, solo algunos LSRs son especificados, es decir se especifica una lista de nodos para actuar como uno de los nodos "abstractos" a recorrer.

El enrutamiento explícito proporciona todos los beneficios de MPLS, incluyendo la capacidad de hacer ingeniería de tráfico y políticas de enrutamiento. Las rutas explícitas pueden ser seleccionadas por configuración o dinámicamente[6]. Para el enrutamiento explícito dinámico, el LSR que prepara el LSP, necesita información sobre la topología del dominio MPLS, así como la información relacionada con la calidad de servicio (QoS) en el dominio MPLS. Una especificación de ingeniería de tráfico, sugiere que la información relacionada con la calidad de servicio (QoS), cae dentro de dos categorías:

- Una serie de atributos asociados con una FEC o una colección de FECs similares que colectivamente especifican sus características de comportamiento.
- Una serie de atributos asociados con los recursos (nodos, enlaces) que restringen la colocación de LSPs a través de ellos.

---

[5] Se define Ingeniería de Tráfico (*Traffic Engineering*), como el proceso de controlar cómo el tráfico fluye a través de la red con el fin de optimizar el uso de los recursos y mejorar el rendimiento de la red.

[6] Configuraciones de enrutamiento:

- Estático: En una red con un número limitado de *routers* para comunicarse con otras redes, las entradas en la tabla pueden ser introducidas manualmente.
- Dinámico: Para usarse en una red donde haya más de una ruta para llegar a otra estación/red. La tabla de rutas es llenada utilizando una aplicación para comunicarse con otros *routers* y determinar la mejor ruta. Los protocolos de enrutamiento actualizan cualquier cambio que se dé en las condiciones de la red.

2.4 DISTRIBUCIÓN DE TAREAS [1]

La implementación de MPLS en los *routers* se divide en dos planos o partes bien diferenciadas (ver figura 2.10): plano de control (llamado también componente de control) y plano de datos (llamado también componente de envío).

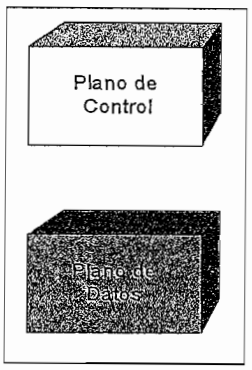


Figura 2.10: Plano de control y de datos

2.4.1 PLANO DE CONTROL

Este plano es el responsable de la generación y mantenimiento de tablas de enrutamiento que establecen los LSPs, así como la distribución de la información sobre las etiquetas a los LSRs. Las tablas de enrutamiento se calculan utilizado bases de datos de estado de enlace así como políticas de control de tráfico (topología, características de los enlaces, patrón de tráfico, etc). Los protocolos de enrutamiento más extendidos en este ámbito son OSPF e IS-IS (ambos de estado de enlace) reforzados para transportar información de políticas y recursos. Los principales componentes de este plano son:

Tabla de enrutamiento: calculada usando los estados de enlace de la base de datos y políticas de ingeniería de tráfico. En MPLS, la tabla de enrutamiento IP proporciona información sobre la red de destino y prefijos de subred usados para la asociación de etiquetas.

***Label Information Base* (LIB):** Tabla donde se guardan las etiquetas que se usan como índice para asignar a las FECs. Es decir, la LIB contiene todas las

etiquetas asignadas por el nodo MPLS local y las asignaciones de estas etiquetas a las etiquetas recibidas de sus vecinos MPLS. Por lo tanto los LSRs requieren un protocolo de distribución de etiquetas (LDP, RSVP-TE, CR-LDP o BGP) para informar a otros *routers* que han realizado una asociación "Etiqueta/FEC". Así, MPLS crea un LSP para cada "ruta IP" a base de concatenar las etiquetas de entrada/salida en cada tabla de los LSRs. Para ello utiliza la LIB.

2.4.2 PLANO DE DATOS

Su función se limita a conmutar los paquetes MPLS entrantes en base a las tablas de enrutamiento ofrecidas por el plano de control. Este plano usa dos fuentes de información:

- Tabla de enrutamiento mantenida en el LSR (LFIB).
- La etiqueta transportada por el paquete.

Los LSRs internos intercambian las etiquetas según una tabla de envío (LFIB, *Label Forwarding Information Base*) que se construye a partir de la información de enrutamiento proporcionada por el plano de control.

***Label Forwarding Information Base* (LFIB):** Contiene toda la información requerida para la conmutación de etiquetas, esto es: etiquetas entrantes y salientes, FEC, las interfaces entrantes y salientes y su encapsulación y la dirección del próximo salto. La LFIB utiliza un subconjunto de las etiquetas contenidas en la LIB para el envío del paquete, es decir guarda solo las etiquetas que en ese momento está usando el plano de datos.

La figura 2.11, muestra los planos de MPLS con sus respectivos componentes.

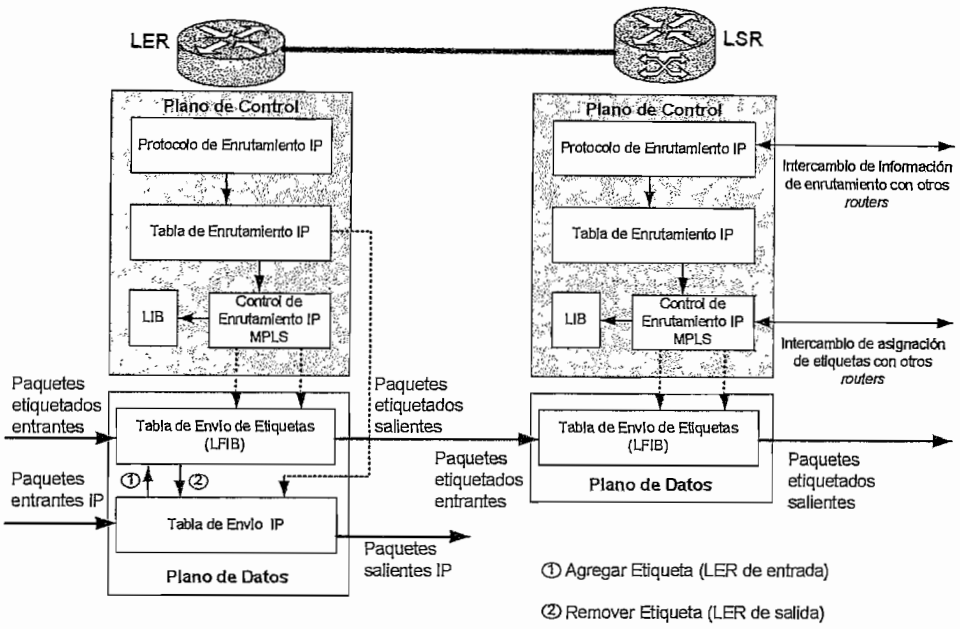


Figura 2.11: Componentes del plano de control y de datos

Puesto que los *routers* no tienen en cuenta los encabezados originales del paquete, MPLS puede utilizarse para transportar protocolos de distintas capas. No obstante, en la práctica se utiliza casi exclusivamente para transportar paquetes IP. Tanto los paquetes etiquetados como los enrutados convencionalmente pueden seguir los mismos trayectos de tráfico. Los *routers* se encargan de enviar de la manera más eficiente ambos tipos de tráfico y por tanto mantienen tablas de enrutamiento diferenciadas para cada uno de ellos.

2.5 FUNCIONAMIENTO DE MPLS [1]

Una red MPLS (ver figura 2.12) consiste en una serie de nodos, denominados LSRs (*Label Switching Routers*), que son capaces de conmutar y enviar los paquetes en base a una etiqueta que se ha añadido a cada paquete. Las etiquetas definen un flujo de paquetes entre dos puntos terminales (*endpoints*) o, en el caso de *multicast*, entre un punto terminal de la fuente y un grupo *multicast* de los puntos terminales del destino. Para cada flujo diferente, denominado FEC, se define un camino específico a través de la red de LSRs.

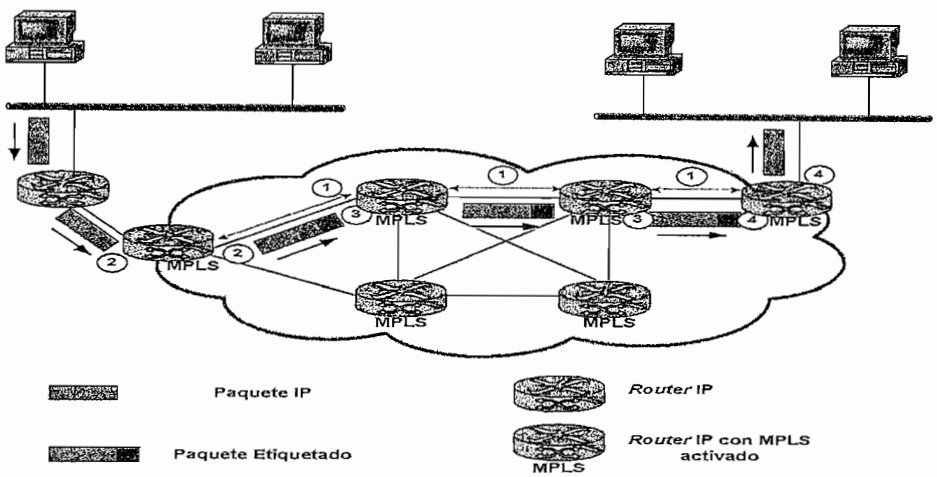


Figura 2.12: Funcionamiento de MPLS

Así, MPLS es una tecnología orientada a conexión. Asociado con cada FEC está una descripción de tráfico que define los requisitos de calidad de servicio (QoS) para dicho flujo. Los LSRs no necesitan examinar o procesar la cabecera IP, sino más bien simplemente enviar cada paquete basado en el valor de su etiqueta. Por tanto el proceso de envío es más simple que con un *router* IP. A continuación se describe el funcionamiento de la red MPLS:

1. Previo al envío y reparto de paquetes en una FEC dada, se debe definir un camino a través de la red, conocido como LSP, y se deben establecer los parámetros de calidad de servicio (QoS) a lo largo de dicho camino. Los parámetros de QoS determinan (1) cuántos recursos se entrega al camino, y (2) qué prioridades en colas y políticas de descarte son establecidas en cada LSR para los paquetes en la FEC. Para lograr estas tareas, se usan dos protocolos para intercambiar la información necesaria entre los *routers*:

    a. Un protocolo de enrutamiento interno, como OSPF, es usado para intercambiar información de accesibilidad y de enrutamiento (información sobre la topología y el retardo del conjunto de las redes).
    b. Las etiquetas deben ser asignadas a los paquetes para una FEC particular. Dado que el uso de una única etiqueta global impondría una carga en la administración y limitaría el número de etiquetas utilizables, las etiquetas solo tienen significado local. Un operador de

red puede especificar las rutas explícitas manualmente y asignar los valores apropiados de etiqueta. Alternativamente se usa un protocolo para determinar la ruta y establecer los valores de etiqueta entre LSRs próximos. Cualquiera de los siguientes protocolos puede ser usado para este propósito: el LDP (*Label Distribution Protocol*) o una versión mejorada de RSVP (*Resource ReSerVation Protocol*).

2. Un paquete entra al dominio MPLS a través de un LSR de borde en el ingreso del dominio MPLS (LER), donde éste es procesado para determinar qué servicios de capa red son requeridos, definiendo su calidad de servicio (QoS). El LSR asigna este paquete a una FEC particular y por tanto a un LSP particular, añade la etiqueta apropiada al paquete y envía el paquete. Si ningún LSP existe todavía para esta FEC, el LER debe cooperar con los otros LSRs, definiendo un nuevo LSP.

3. Dentro del dominio MPLS, cuando cada LSR recibe un paquete etiquetado, éste:

    a. Remueve la etiqueta del paquete entrante y adhiere la etiqueta apropiada al paquete saliente.
    b. Envía el paquete al próximo LSR a lo largo del LSP.

4. El LSR de borde en la salida del dominio MPLS (LER), remueve la etiqueta, lee la cabecera del paquete IP y envía el paquete a su destino final.

Varios aspectos claves del funcionamiento de MPLS, pueden notarse en estos puntos:

1. Un dominio MPLS consiste de un conjunto de *routers* MPLS contiguos o asociados. El tráfico puede entrar o salir del dominio de un punto terminal en una red directamente conectada, como se muestra en la esquina superior derecha de la figura 2.12. El tráfico también puede arribar de un

router ordinario que conecta a una porción de la red que no usa MPLS, como se muestra en la esquina superior izquierda de la figura 2.12.

2. La FEC para un paquete puede determinarse por uno o más parámetros, especificados por el administrador de red. Entre los posibles parámetros se tienen:

   - Direcciones IP de origen o destino, o direcciones IP de red.
   - Números de puerto de origen o destino.
   - Identificador del protocolo IP.
   - Punto de código de Servicios Diferenciados (ver la sección 3.5.2).
   - Flujo de etiquetas IPv6.

3. Se realiza el envío por ejecución de una simple búsqueda en una tabla predefinida (LFIB) que asigna los valores de las etiquetas para el siguiente salto de dirección. No hay necesidad de examinar o procesar la cabecera IP o hacer una decisión de enrutamiento basado en la dirección IP de destino.

4. Se puede definir un PHB (*Per-Hop Behavior*) particular en un LSR para una FEC dada. El PHB define niveles de prioridades a cada paquete para esta FEC, para que cada *router* asigne un determinado comportamiento por salto y además defina una política de descarte. Un PHB puede equivaler a niveles concretos de prioridad de servicio (qué paquete se atiende primero) o de prioridad de descarte (en caso de congestión, qué paquetes se descartan primero).

5. Los paquetes enviados entre los mismos puntos terminales pueden pertenecer a FECs diferentes. Así, ellos se etiquetarán de manera diferente, experimentarán diferente PHB en cada LSR y pueden seguir diferentes caminos a través de la red.

En la figura 2.13 se muestra el funcionamiento del manejo y envío de etiquetas con más detalle. Cada LSR mantiene una tabla de envío para cada LSP que pasa a través del LSR. Cuando un paquete etiquetado llega, el LSR usa el valor de la etiqueta como un índice dentro de la tabla de envío (LFIB), que especifica el siguiente destino y la nueva etiqueta a ser utilizada, así el LSR remueve la etiqueta entrante del paquete y adhiere la etiqueta saliente, antes de enviar el paquete. El LSR de borde en el ingreso del dominio MPLS determina la FEC para cada paquete entrante sin etiquetar y, en base a la FEC, asigna al paquete a un LSP particular, adhiere la correspondiente etiqueta y envía el paquete.

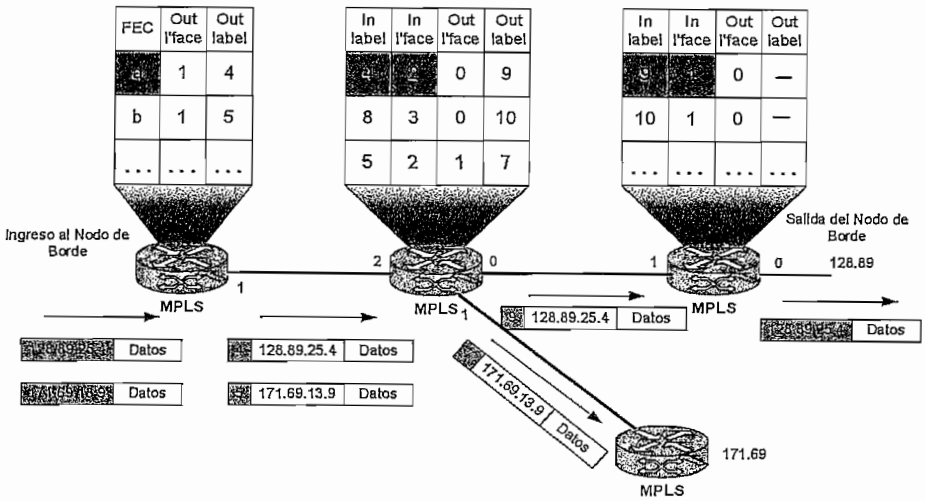


Figura 2.13: Funcionamiento del manejo y envío de etiquetas

2.6 PROTOCOLOS DE DISTRIBUCIÓN DE ETIQUETAS [2], [3], [5], [8]

Para que un paquete etiquetado pueda avanzar por los LSRs necesita que un protocolo previo prepare las tablas. Este protocolo puede ser uno de varios, denominados como: LDPs (*Label Distribution Protocols*) y se encargan de propagar de *router* a *router* la información necesaria para establecer el LSP, es decir son un conjunto de procedimientos por el que un LSR informa a otros que ha realizado una asociación "Etiqueta/FEC".

Dos LSRs que utilizan conjuntamente un protocolo LDP se denominan: "LDP *peers*". Dos LSRs pueden ser pares (*peers*) con respecto a algún conjunto de asociaciones pero no con respecto a otros conjuntos de asociaciones.

La arquitectura MPLS no asume la existencia de un protocolo específico. En efecto diferentes protocolos de distribución de etiquetas, han comenzado a ser estandarizados, existiendo una lista de protocolos de distribución de etiquetas, como se muestra a continuación:

- Protocolos Existentes:
  - De enrutamiento con nuevas funciones
    - BGP (*Border Gateway Protocol*), ver sección 3.4.1.6 y el Anexo A
    - PIM (*Protocol Independent Multicast*).
  - De señalización
    - RSVP-TE: RSVP con funcionalidad añadida de ingeniería de tráfico
- Nuevos protocolos:
  - LDP (*Label Distribution Protocol*)
    - Mismas rutas que el enrutamiento IP convencional
  - CR-LDP (*Constraint Routing*)
    - LDP con funcionalidad añadida de ingeniería de tráfico

A continuación se estudiarán los principales protocolos de distribución de etiquetas que pueden ser utilizados en los dispositivos MPLS.

2.6.1 PROTOCOLO LDP (*LABEL DISTRIBUTION PROTOCOL*)

LDP (Protocolo de Distribución de Etiqueta) es un nuevo protocolo que define una serie de procedimientos y mensajes por los cuales un LSR informa a otro de la asociación Etiqueta/FEC que ha realizado y es usado para el establecimiento de un LSP. Dos LSRs que utilizan conjuntamente el protocolo LDP para intercambiar la información de *label mapping* son conocidos como: "LDP *peers*" y éstos tienen una sesión LDP entre ellos. LDP permite a un LSR distribuir etiquetas a sus pares (*peers*) LDP usando el puerto TCP 646. En una sola sesión, cada par o vecino es capaz de aprender sobre otros *label mappings*, en otras palabras, el protocolo es bidireccional.

Existen cuatro tipos de mensajes:

- Descubrimiento (*Discovery*): Para señalizar la presencia de *routers* MPLS sobre UDP y, usa mensajes *Hello* por difusión para aprender sobre otros LSRs con los cuales tiene una conexión LDP directa.
- Sesión (*Session*): Para establecer y mantener sesiones LDP sobre TCP.
- Anuncio (*Advertisement*): Para crear, cambiar y borrar las asociaciones Etiqueta/FEC. Para anunciar las asociaciones entre FECs y etiquetas se usa mensajes *Label Mapping*. Para revertir el proceso de asociación se usa los mensajes *Label Withdrawal*. Los mensajes *Label Release* son usados por LSRs que han recibido la información de los *label mapping* y han requerido librar la etiqueta porque ya no tienen una necesidad por ésta.
- Notificación (*Notification*): Para indicar errores. Existen dos tipos de mensajes de notificación:

    1. Notificaciones de error; estas señales de errores fatales causan la terminación de la sesión.
    2. Notificaciones de asesoría; éstas se usan para comunicar en la información del LSR acerca de la sesión LDP o el estado de algunos mensajes previos recibidos del LSR par.

2.6.1.1 Detalles de LDP

2.6.1.1.1 Espacios de Etiquetas

Las etiquetas usadas por un LSR para la asociación Etiqueta/FEC son asignadas de un conjunto de posibles etiquetas denominado espacio de etiqueta (*label space*). La noción de "*label space*" es útil para discutir la asignación y distribución de etiquetas. LDP soporta dos tipos de *label spaces*:

Por interfaz: Los rangos de la etiqueta están asociados con interfaces. Los valores de la etiqueta proporcionados en diferentes interfaces podrían tener el

mismo valor, es decir el LSR *downstream* está usando un espacio de etiquetas diferente para las etiquetas distribuidas a los LSR *upstream*, ver figura 2.14.

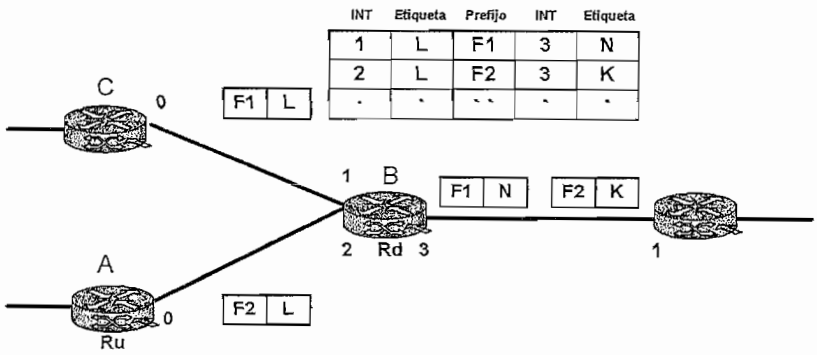


Figura 2.14: Espacio de etiquetas por interfaz

Por plataforma: Los valores de la etiqueta son únicos sobre el LSR que los asignó. Ninguna de dos etiquetas en interfaces diferentes tienen el mismo valor, ver figura 2.15.

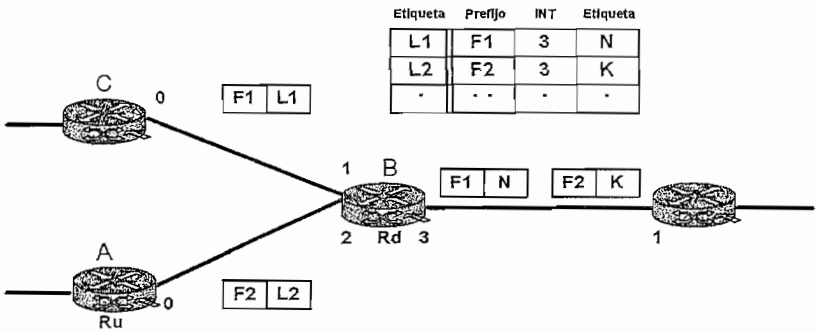


Figura 2.15: Espacio de etiquetas por plataforma

2.6.1.1.2 Identificadores LDP

Un identificador LDP es un valor de seis octetos, usado para identificar el espacio de etiquetas de un LSR. Los primeros cuatro octetos identifican el LSR y deben ser globalmente de un solo valor. Los últimos dos octetos identifican un espacio de etiquetas específico dentro del LSR. Se utiliza la siguiente nomenclatura para los identificadores LDP: **<LSR id>: <*label space* id>**, por ejemplo: lsr19:2, donde 19 representa el identificador del LSR y 2 representa el identificador del espacio

de etiquetas. Un LSR que maneja y anuncia múltiples espacios de etiquetas, usa un identificador LDP diferente para cada espacio de etiquetas. Una situación donde un LSR necesitaría anunciar más de un espacio de etiquetas a un par (*peer*) y usar más de un identificador LDP ocurre cuando el LSR tiene dos enlaces al par y ambos son ATM (y usa etiquetas por interfaz). Otra situación es donde el LSR tiene dos enlaces al par uno de los cuales es Ethernet (y usa etiquetas por plataforma) y el otro es ATM.

2.6.1.1.3 Sesión LDP

Son sesiones entre LSRs para respaldar el intercambio de información entre ellos. LDP usa TCP como un transporte confiable para las sesiones. Una sesión es solo para un espacio de etiquetas.

2.6.1.2 Mecanismo LDP

2.6.1.2.1 Descubrimiento LDP

El descubrimiento LDP es un mecanismo que permite a un LSR descubrir "LDP *peers*" potenciales (por interfaz LSR). Los mensajes *Discovery* se envían periódicamente usando UDP. Existen dos variantes del mecanismo *Discovery* (en las dos variantes, los mensajes transportan identificadores LDP):

- Un mecanismo de descubrimiento básico es usado para descubrir vecinos LSR que están conectados directamente al nivel de enlace. Un LSR envía periódicamente mensajes *Hello*. Los mensajes *Hello* son enviados como paquetes UDP dirigidos a "todos los *routers* de esta subred" es decir a una dirección *multicast*, haciendo que el descubrimiento del LSR vecino sea automático.
- Las sesiones LDP entre LSRs que no están conectados directamente son soportadas por el descubrimiento extendido LDP. Un LSR envía periódicamente "*Targeted Hello*" a una dirección específica, la cual puede ser suministrada por la parte administrativa.

2.6.1.2.2 Establecimiento de la Sesión LDP

El intercambio de mensajes *Hello* entre dos LSRs activa el establecimiento de la sesión LDP.

El establecimiento de la sesión es un proceso de dos pasos:

1. **Establecimiento de la conexión TCP:** El establecimiento de la conexión TCP es llevado a cabo por el LSR "activo" (identificador LSR más alto) determinado por los parámetros de dirección en el mensaje "*Hello*".

2. **Iniciación de la Sesión:** Después de que se establece una conexión TCP, se negocian los parámetros de la sesión intercambiando mensajes de Inicialización (*Initialization*). Los parámetros negociados incluyen: la versión protocolar, el método de distribución de etiquetas, valores del temporizador, el espacio de etiquetas a ser usadas en el enlace entre dos LSRs. Si un LSR es activo, comienza la negociación de parámetros de la sesión enviando un mensaje de Inicialización a otro LSR. Si el LSR es pasivo, espera por otro LSR para comenzar la negociación de los parámetros.

   Dos LSRs pueden enviar mensajes de Inicialización, el LSR que recibe el mensaje, contesta con un mensaje *KeepAlive* si los parámetros son aceptados. Si los parámetros de la sesión son inaceptables, el LSR envía un mensaje de Notificación de error rechazando la sesión y cierra la conexión.

LDP incluye mecanismos para supervisar la integridad de la sesión LDP. LDP utiliza el regular recibimiento de PDUs en la sesión de conexión para supervisar la integridad de la sesión. Un LSR mantiene un temporizador *KeepAlive* para cada sesión con el par, el cual es reiniciado siempre que reciba una PDU de LDP del par (*peer*) en la sesión. Si el temporizador *KeepAlive* expira sin el recibimiento de una PDU de LDP del par, el LSR concluye que la conexión es mala o que el par ha fallado, y termina la sesión LDP cerrando la conexión. En circunstancias donde un

LSR no tiene otra información que comunicar a su par, envía un mensaje *KeepAlive*. Un LSR puede elegir terminar una sesión LDP cuando quiera con un par. Si lo hace, informa al par con un mensaje de *Shutdown*.

2.6.1.2.3 Distribución de Etiquetas

Como se mencionó, en la sección 2.3.4.2.3, la arquitectura MPLS utiliza dos posibles variantes de distribución de etiquetas, éstas son: *Downstream* No solicitado y *Downstream* Bajo Demanda.

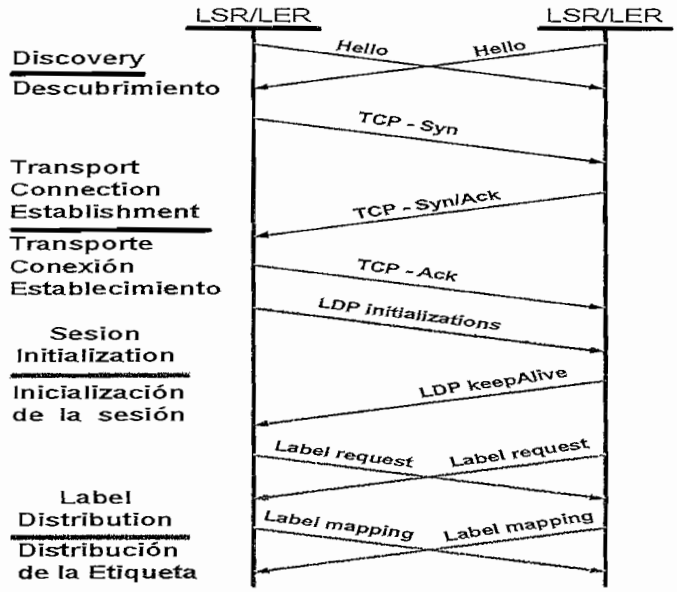


Figura 2.16: Intercambio de mensajes de LDP

En la distribución de etiquetas *downstream* bajo demanda, un LSR requiere de su vecino *downstream* una etiqueta para una cierta FEC, para esto un LSR usa mensajes *Label Request* (Petición de etiqueta) para solicitar una etiqueta de su vecino *downstream* para que pueda asociar a una FEC específica. Este mecanismo puede emplearse a lo largo de la cadena de LSRs hasta el LER de salida. El mensaje *Label Request Abort* es usado para eliminar el mensaje *Label Request* durante o antes de la finalización de la petición. En respuesta a una petición de etiqueta un LSR *downstream* enviará una etiqueta al iniciador *upstream* usando el mecanismo *label mapping*.

En la distribución de etiquetas *downstream* No solicitado las etiquetas son distribuidas sin peticiones.

En la figura 2.16, se muestra los procedimientos anteriormente detallados.

2.6.1.3 PDUs de LDP

Los mensajes son enviados como PDUs (*Protocol Data Unit*) de LDP. Cada PDU puede contener más de un mensaje LDP. Cada PDU de LDP es una cabecera LDP seguido por uno o más mensajes LDP. La estructura de la cabecera LDP se muestra en la figura 2.17.

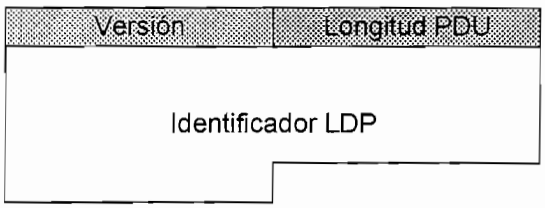


Figura 2.17: Estructura de la cabecera LDP [2]

Versión: Campo de 16 *bits*. El número actual de la versión del protocolo LDP es uno.

Longitud del PDU: Campo de 16 *bits*. Específica la longitud total del PDU excluyendo los campos de la versión y la longitud del PDU.

Identificador LDP: Campo de 48 *bits*. Este campo únicamente identifica el espacio de etiquetas del LSR. Los primeros cuatro octetos identifican el LSR y debe ser globalmente de único valor. Los últimos dos octetos identifican un espacio de etiquetas dentro del LSR.

2.6.1.4 Mensajes de LDP

Todos los mensajes de LDP tienen el siguiente formato (ver figura 2.18):

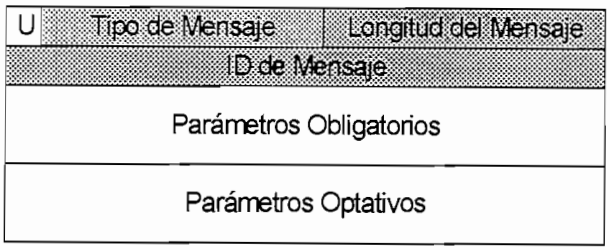


Figura 2.18: Formato de los mensajes de LDP [2]

Bit U: 1 *bit*. Define la acción a ser tomada después de recibir un mensaje desconocido. Si U = 0, una notificación se devuelve al creador del mensaje. Si U = 1, el mensaje desconocido se ignora.

Tipo de Mensaje: Campo de 15 *bits*. Identifica el tipo de mensaje.

Longitud del Mensaje: Campo de 16 *bits*. Especifica la longitud acumulativa en los octetos del ID de Mensaje, los Parámetros obligatorios y los Parámetros Optativos.

ID de Mensaje: Campo de 32 *bits*, se utiliza para identificar el mensaje.

Parámetros: Campo de longitud variable. Los parámetros contienen los TLVs (*Type-Length-Value*), ver la siguiente sección. Existen parámetros obligatorios y optativos. Los parámetros optativos se usan para la detección de lazos. Así se tiene los siguientes parámetros: vectores de camino (*path vectors*) y contadores de saltos (*hop count*).

2.6.1.5 Codificación TLV

Todos los mensajes LDP tienen una estructura común que usa un esquema de codificación TLV (Tipo-Longitud-Valor). Este código TLV es usado para codificar mucha de la información transportada en los mensajes LDP. La parte de Valor de un objeto codificado TLV, puede contener por sí mismo uno o más TLVs. En la figura 2.19, se muestra la cabecera TLV.

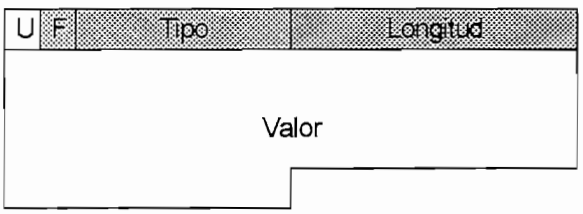


Figura 2.19: Cabecera TLV [2]

Bit U: 1 *bit*. El *bit* U es un *bit* TLV desconocido.

Bit F: 1 *bit*. El *bit* F es un *bit* TLV desconocido de reenvío.

Tipo: Campo de 14 *bits*. Codifica cómo el campo Valor será interpretado.

Longitud: Campo de 16 *bits*. Especifica la longitud del campo Valor dado en octetos.

Valor: Campo de longitud variable. Codifica la información para ser interpretada como se específica en el campo Tipo.

LDP usa vectores de camino y contadores de saltos para detectar los lazos. El vector de camino consiste en un vector que transporta las identificaciones LSRs de todos los LSRs en el LSP. Los lazos se descubren cuando un LSR recibe un mensaje con su identificación dentro del vector de camino.

Los contadores de saltos son usados para limitar la cantidad de recursos que pueden consumirse cuando se crean los lazos. Cuando el contador de saltos alcanza un cierto umbral, el sistema actúa como si un lazo se hubiera encontrado en el vector de camino. El LSP no se establece. Los LSRs intercambian *label mappings* con la información del contador de saltos. Los Protocolos de Distribución de Etiquetas pueden usar los valores del contador de saltos. Cada nodo sabe el número de saltos para alcanzar el fin del LSP.

2.6.2 PROTOCOLO CR-LDP

El protocolo LDP, no puede satisfacer las necesidades de QoS. Existen algunos casos donde hay una necesidad de crear LSPs de enrutamiento explícito a través de un dominio de MPLS. Hay también una necesidad de asegurar que los LSPs puedan soportar CoS (Clase de Servicio) y requerimientos de ingeniería de tráfico. Para esto se crearon protocolos como: CR-LDP y RSVP-TE.

CR (*Constraint-based Routing*), es un algoritmo de enrutamiento restringido que calcula los trayectos basándose en los recursos reservados, sin considerar la carga instantánea de los enlaces. CR-LDP es una ampliación de LDP, el cual ya es parte de MPLS. Usa los mensajes existentes de LDP, pero define TLVs adicionales para los mensajes. Aunque CR-LDP no es tan maduro como RSVP,

CR-LDP no requiere la implementación de un protocolo adicional. Usa estructuras de mensajes existentes y sólo se extiende como requisito para implementar ingeniería de tráfico. CR-LDP soporta rutas explícitas LSP (estricta y libre). UDP se usa para descubrir *peers* MPLS y se usa TCP para el control, la administración, petición de etiqueta (*label request*) y *label mapping*.

En la figura 2.20, se establece un CR-LDP LSP entre un LER de entrada y uno de salida en una red. El camino es predeterminado para el ingreso y la salida y está limitada a dos LSRs específicos. Las peticiones de etiqueta son pasadas hacia abajo a cada dispositivo *downstream* de una manera *hop by hop* al LER de salida y la asignación de etiqueta es pasada hacia arriba de manera similar al LER de ingreso. En la red, el establecimiento del CR-LDP LSP es referido como "*hard state*"; esto significa que toda la información se intercambia en el momento del arreglo inicial y ninguna información adicional se intercambia entre los *routers* hasta que el LSP se ha dado de baja.

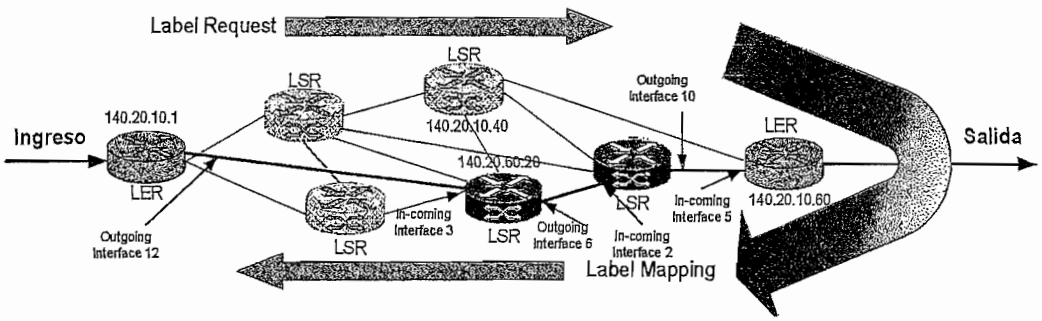


Figura 2.20: CR-LDP LSP [10]

Como se muestra en la figura, el camino de enrutamiento explícito puede ser tan preciso como para estipular las direcciones IP específicas a ser usadas por el LER y el LSR. Esto es ventajoso para un tipo particular de tráfico, como la voz o de VPN, que pueden ser asociados al camino óptimo influyendo en el ancho de banda y/o en la prioridad.

2.6.3 PROTOCOLO RSVP-TE

RSVP es un protocolo de señalización para reservar recursos en las aplicaciones antes de empezar a transmitir información. RSVP permite reservar recursos para

flujos que se agreguen, configurar *routers* explícitos (basándose en una calidad de servicio determinada) y, además realizar otro tipo de señalizaciones.

El uso de RSVP-TE no significa que se requiera una implementación completa de RSVP para correr en cada LER ó LSR dentro de una red MPLS. Un LER o un LSR solo requieren las extensiones para ser capaz de soportar enrutamiento explícito. RSVP-TE es referido como un protocolo *"soft state"*. Después de un proceso inicial de establecimiento de un LSP, se deben intercambiar periódicamente mensajes de refresco entre los pares para notificar a éstos que la conexión todavía se desea. RSVP-TE usa datagramas UDP, como el mecanismo de señalización para establecer el LSP, incluyendo el descubrimiento del par, petición y asignación de etiquetas y administración.

En este ejemplo (ver figura 2.21), haciendo uso de BGP para descubrir el LER apropiado de salida, a fin de enrutar el tráfico a otro sistema autónomo (AS), el LER de ingreso inicializa un mensaje PATH al LER de salida a través de cada LSR *downstream* a lo largo del camino.

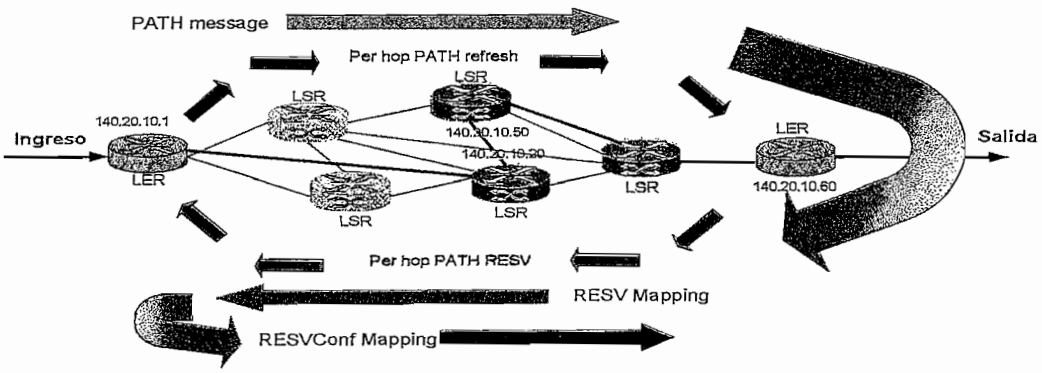


Figura 2.21: RSVP-TE LSP [10]

Cada nodo recibe un mensaje *PATH* para recordar que el mensaje está pasando, creando así una sesión. El LER de salida usa el mensaje RESV para reservar recursos con el tráfico y parámetros de QoS en cada LSR *upstream* a lo largo del camino de la sesión. Una vez que se recibe el mensaje en el LER de entrada, un mensaje RESVConf es devuelto al LER de salida confirmando el establecimiento del LSP.

Después que el ER-LSP ha sido establecido, mensajes de refresco atraviesan los LERs y LSRs para mantener el camino y los estados de reservación. Debe notarse que, ninguno de los mensajes *downstream*, *upstream* o de refresco entre los LERs y LSRs se consideran fiables, porque UDP o los datagramas IP son usados como los mecanismos de comunicación. RSVP-TE proporciona capacidades significativas para proveer ingeniería de tráfico en MPLS.

2.7 TUNELIZACIÓN Y JERARQUÍAS EN MPLS [1]

MPLS puede controlar el camino entero de un paquete sin especificar explícitamente los *routers* intermedios. MPLS hace esto creando túneles a través de los *routers* intermedios que pueden extenderse por múltiples segmentos. Este concepto es utilizado por MPLS para proveer VPNs. Es posible implementar un túnel como un LSP y usar una conmutación de etiquetas en lugar de la encapsulación de capa red para motivar al paquete a viajar a través del túnel. El túnel es un LSP <R1,..., Rn>, donde: R1 es el punto terminal transmisor del túnel y Rn es el punto terminal receptor del túnel. Esto se denomina túnel LSP.

El criterio para asignar un paquete particular a un túnel LSP es una cuestión del punto terminal transmisor del túnel; éste coloca un paquete dentro de un túnel LSP, el punto terminal transmisor coloca una etiqueta para el túnel sobre la pila de etiquetas y envía el paquete etiquetado al próximo salto. En el punto terminal receptor del túnel se remueve la etiqueta de la pila.

MPLS tiene jerarquía, permitiendo los túneles LSP dentro de LSPs, pero el paquete que se procesa en un *router* es completamente independiente del nivel de jerarquía. Se procesa siempre la etiqueta de la cima, como ya se mencionó anteriormente.

Considerando el escenario mostrado en la figura 2.22. Se considera un LSP (LSP1) <R1, R2, R3, R4, R5, R6>. R1 recibe un paquete sin etiquetar, añade en su pila de etiquetas una etiqueta que permita seguir el camino trazado. R3 y R4, no están directamente conectados, pero son "vecinos", en virtud de ser puntos

terminales de un túnel LDP. Así que la real secuencia a seguir por el paquete es: <R1, R2, R3, R31, R32, R4, R5, R6>.

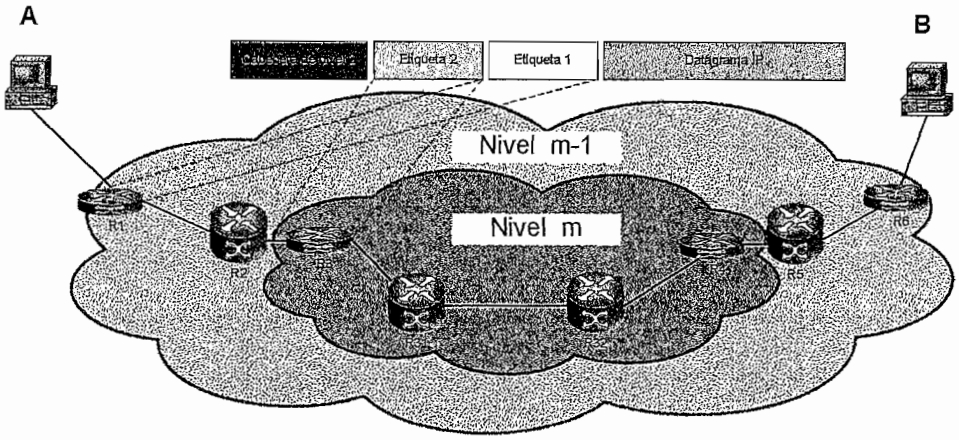


Figura 2.22: Jerarquía MPLS [9]

Cuando el paquete viaja de R2 a R3 tendrá una pila de etiquetas con profundidad 1 (*depth* 1), R3 recibe la etiqueta y determina que el paquete debe ingresar al túnel. R3 en primer lugar reemplaza la etiqueta entrante con una etiqueta que es significativa a R4. Entonces, R3 añade una nueva etiqueta. Esta etiqueta de nivel 2 tiene un valor que es significativo a R31. R3 enviará información a R4, la cual debe ir a través de varios LSRs, por consiguiente, un LSP (LSP2) separado es creado entre R3 y R4, que se extiende a través de R31 y R32. Esto, en efecto, representa un túnel entre R3 y R4. En otras palabras habrá una etiqueta para LSP1 y otra para LSP2 y el paquete transporta las dos etiquetas a la vez.

En general, un paquete puede transportar múltiples etiquetas organizadas en una pila LIFO de etiquetas. R4, remueve la etiqueta de la pila de etiquetas para LSP2 y cambia la etiqueta para LSP1 dentro del paquete con la etiqueta del próximo salto, antes de enviar el paquete a R5. Cuando R5 recibe el paquete, éste solo tiene una etiqueta de nivel 1. R6 removerá la etiqueta antes de enviar el paquete al destino.

2.8 MPLS *MULTICAST* [7]

Aunque MPLS ha hecho un notable progreso recientemente, varios problemas permanecen pendientes, los cuales merecen una extensa investigación. Algunos

problemas están dirigidos a: la QoS, manejo de recursos y un soporte de movilidad en un ambiente *multicast*[7].

MPLS se diseñó originalmente para tráfico *unicast* IP y todavía no existe una definición completa para el soporte de tráfico *multicast* IP. Algunos mecanismos de MPLS *Multicast* apuntan hacia aplicar a MPLS, técnicas *multicast* de IP para optimizar el desempeño de la red sin modificación alguna en el ambiente del usuario final, o a los protocolos *multicast* de IP existentes. Para *multicast* en MPLS, en general se utiliza el protocolo de enrutamiento PIM-SM (*Protocol Independent Multicast - Sparse Mode*). Este protocolo es diseñado para enviar eficazmente datagramas *multicast* IP a los grupos de una área extensa escasamente distribuidos.

Para soportar *multicast* en MPLS, debe establecerse un LSP punto a multipunto a lo largo del árbol *multicast*. Existen varias maneras de lograr esto: superposiciones en los mensajes de control del protocolo *multicast*, usando LDP o un protocolo separado. Cuando se establecen los árboles *multicast* con los mensajes de control, las etiquetas pueden distribuirse con los mensajes superpuestos (*piggybacking*). Por ejemplo, las etiquetas pueden ser incluidas en el protocolo PIM-SM junto con los mensajes para que los LSPs se construyan a lo largo del camino hacia el punto de reunión (RP, *Rendezvous Point*). Sin embargo, este modelo requiere extensiones para cada protocolo *multicast*. Por consiguiente, también es deseable poder usar LDP para establecer un LSP *multicast*.

2.9 BENEFICIOS DE MPLS

Respecto a MPLS se pueden citar varias ventajas:

- Fácilmente aplicable a los *routers* actuales mediante actualización de *software*.

[7] *Multicast* es el hecho de enviar un paquete desde un origen a dos o más receptores específicos. *Multicast* es usado en aplicaciones como las teleconferencias.

- MPLS soporta cualquier tipo de tráfico en una red IP sin depender de los protocolos de enrutamiento, capa de transporte y esquemas de direccionamiento.

- La determinación del siguiente salto dentro de la red MPLS es realizada sólo analizando la etiqueta en lugar de analizar la cabecera del paquete IP.

- La ruta que seguirá un flujo de datos determinado puede: (1) establecerse dinámicamente por los protocolos de distribución de etiquetas, (2) especificarse explícitamente y (3) reservarse mediante una extensión del protocolo RSVP.

- Es posible forzar un camino dentro de la red MPLS, teniendo en cuenta aspectos de QoS como ancho de banda y disponibilidad de *buffer*, en lugar de los algoritmos de enrutamiento actuales que consideran básicamente la menor distancia. Esto último es una ventaja importante, ya que no siempre el camino más corto es el menos congestionado y el óptimo para ofrecer una mejor QoS a una aplicación en general.

- Uno de los beneficios más importantes de MPLS es que permite a los SPs (*Service Provider*), tales como portadores (*carriers*), ISPs, etc, entregar nuevos servicios que no pueden darse con técnicas de enrutamiento IP convencionales. La separación de la componente de control de la componente de datos, proporciona a MPLS la flexibilidad para desarrollar la funcionalidad de control sin cambiar el mecanismo de envío permitiendo así, a MPLS soportar el despliegue de capacidades reforzadas de envío que se necesitará para que el Internet continúe con su crecimiento explosivo.

BIBLIOGRAFÍA – CAPÍTULO 2

[1] ROSEN E., VISWANATHAN A., CALLON R., "*Multiprotocol Label Switching Architecture*", RFC 3031, Enero 2001.

[2] ANDERSSON L., DOOLAN P., FELDMAN N., FREDETTE A., y THOMAS B., "LDP *Specification*", RFC 3036, Enero 2001.

[3] REKHTER Y., LI T., "*A Border Gateway Protocol 4* (BGP-4)", RFC 1771, Marzo 1995.

[4] BATES T. y Otros, "*Multiprotocol Extensions for BGP-4*", RFC 2858, Junio 2000.

[5] AWDUCHE D. y Otros., "RSVP-TE: *Extensions to RSVP for LSP Tunnels*", RFC 3209, Diciembre 2001.

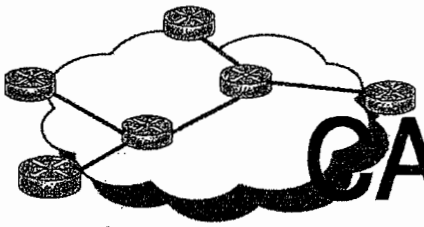
[6] BRADEN R. y Otros, "*Resource ReSerVation Protocol* (RSVP) -- *Version 1 Functional Specification*", RFC 2205, Septiembre 1997.

[7] VISWANATHAN A., FELDMAN N., WANG Z., CALLON R., "*Evolution of Multiprotocol Label Switching*", *IEEE Communications Magazine,* Vol. 36, No. 5, Mayo 1998.

[8] JAMOUSSI B. y Otros, "*Constraint-based LSP Setup Using LDP*", RFC 3212, Enero 2002.

[9] FIM LSIIS, "MPLS. INGENIERÍA DE TRÁFICO Y RPV DE PROVEEDOR", 2002.

[10] PULLEY R. y CHRISTENSEN P., "*A Comparison Of MPLS Traffic Engineering Initiatives*", NETPLANE Systems, http://www.netplane.com.



CAPÍTULO 3

REDES PRIVADAS VIRTUALES BASADAS EN MPLS

3.1 INTRODUCCIÓN

El concepto de Red Privada Virtual (VPN) no es nuevo, las tecnologías como ISDN, Frame Relay (FR) o ATM han sido usadas durante las últimas décadas como una base para la aplicación de este concepto. Independientemente de la tecnología usada, una VPN proporciona un servicio funcionalmente equivalente a una red privada que usa recursos de una red pública. Como resultado de la amplia definición de una VPN, muchas tecnologías de comunicaciones contemporáneas pueden dar el soporte de VPNs de diferentes maneras.

Las VPNs pueden ser implementadas con la tecnología predominante y con los propios objetivos de los usuarios. Así, hasta no hace demasiado tiempo, las VPNs basadas en servicios portadores de nivel 2 (como ATM o FR) constituían el elemento clave en los catálogos de productos de los proveedores de servicio en este segmento. Este tipo de soluciones permite la provisión de servicios de conectividad entre diferentes ubicaciones gracias a la constitución de una topología entre ellas mediante circuitos virtuales sobre una red FR o ATM (o mixta, con una capa de acceso FR y un núcleo ATM, como es el caso de la mayor parte de los operadores), garantizan los parámetros de calidad de servicio asociados a estas tecnologías, y dado que se trata de tecnologías orientadas a conexión donde se crean circuitos virtuales, limitan los problemas de intrusión.

Adicionalmente, dado que se basan en protocolos de nivel 2, de acuerdo al modelo de referencia OSI (*Open System Interconnection*), es posible la transmisión de diferentes protocolos de nivel de red (IP, IPX, ..) o capa internet de acuerdo al modelo TCP/IP. Como desventajas se encuentran una escalabilidad comprometida en el caso de necesitar proveer una topología completamente mallada (*full mesh*) entre un gran número de ubicaciones.

En el presente capítulo, se describe la arquitectura VPN MPLS, en las primeras secciones se introducirá el concepto de IP-VPNs y los tipos básicos, los modelos

overlay y *peer to peer*, se estudiarán las VPNs MPLS de Capa 3 (VPNs BGP/MPLS), seguidamente las VPNs MPLS de Capa 2 (*drafts* Martini y Kompella) y finalmente la calidad de servicio (QoS) en las VPNs.

Antes de describir los diferentes tipos de VPNs basadas en MPLS, es necesario revisar dos términos importantes.

Dispositivos CE y PE: Para tener acceso al *backbone* de IP, debe existir al menos un dispositivo en el borde de cada sitio del cliente que se conecte a la red del proveedor de servicios[1] (SP, *Service Provider*). Éstos son denominados dispositivos CE (*Customer Edge*). Aunque estos dispositivos son parte de la red del cliente, en lugar de ser parte del *backbone* de IP, estos dispositivos son en algunos casos administrados por el proveedor del servicio.

Similarmente, el dispositivo o dispositivos, que conectan a los dispositivos CE a la red del proveedor del servicio se denominan dispositivos PE (*Provider Edge*).

Los *routers* en la red del proveedor de servicio que envían los datos, pero no están proporcionando la funcionalidad de VPN a un dispositivo CE, se denominan dispositivos P (*Provider*).

Capa 2/Capa3: Una diferencia principal entre los tipos de VPNs es el servicio que se proporciona al usuario de la VPN. Por ejemplo, un servicio de VPN podría ser una solución de Capa 2 ("L2VPN"), proporcionando a los clientes servicios parecidos a Ethernet, Circuitos Virtuales ATM/FR ("VC"s, *virtual circuits*) o líneas arrendadas, o podría ser una solución de Capa 3 ("L3VPN"), proporcionando a los clientes conectividad IPv4 o IPv6 entre los sitios de la VPN.

La amplia difusión alcanzada por IP, fundamentalmente gracias a la explosión del fenómeno Internet, es el principal promotor de la aparición de otro concepto de VPN, articulada en torno a IP, denominadas IP-VPNs.

---

[1] Un Proveedor de Servicio es una entidad que proporciona servicios a sus subscriptores en una base contractual y es responsable por los servicios ofrecidos. La misma entidad puede actuar como Operador de Red y Proveedor de Servicio. Un Operador de Red es una entidad que es responsable por el desarrollo, provisión y mantenimiento de servicios de telecomunicaciones y de operar las redes correspondientes.

3.2 DEFINICIÓN DE UNA IP-VPN Y LOS TIPOS BÁSICOS [1]

En los recientes años, con el éxito del Internet, el panorama de las telecomunicaciones ha cambiado radicalmente y el protocolo IP ha sido desplegado enormemente en las redes corporativas. Una VPN basada en IP (IP-VPN) puede definirse como una implementación de una VPN que usa o comparte los recursos de una red pública IP para emular las características de una red privada IP.

Usualmente se identifican dos tipos de IP-VPNs [1]:

- VPNs basadas en dispositivos CE
- VPNs basadas en dispositivos PE o VPN basadas en Red

Las VPNs basadas en dispositivos CE, se refieren a un enfoque en el cual los dispositivos PE no saben nada sobre el enrutamiento o direccionamiento de las redes del cliente. Los dispositivos PE ofrecen un simple servicio de IP, y esperan recibir paquetes IP cuyas cabeceras sólo contienen direcciones IP globalmente únicas. Es común para un SP ser el responsable del manejo y provisión de los dispositivos CE para reducir los requerimientos de administración del cliente. Esto produce las VPNs basadas en dispositivos CE proporcionadas por el proveedor.

En este modelo, el *backbone* de la red del cliente es un conjunto de túneles cuyos puntos terminales (*endpoints*) son los dispositivos CE. Pueden usarse varios tipos de túneles (por ejemplo: GRE, IP-IP, IPSec, L2TP, MPLS), el único requisito es que cuando se envía un paquete a través del túnel se requiere encapsulamiento con una nueva cabecera IP cuyas direcciones sean globalmente únicas.

Una VPN basada en dispositivos PE, es aquella en la cual los dispositivos PE de la red del SP proporcionan la VPN. Esto permite ocultar la existencia de la VPN de los dispositivos CE, la cual puede operar como si fuera parte de una red normal del cliente.

En las VPNs basadas en dispositivos PE, la red del cliente es soportada por túneles, los cuales son establecidos entre los dispositivos PE. Existen dos tipos básicos de VPNs basadas en PE: de capa 2 y de capa 3, las cuales se estudiarán en la sección 3.4.

En adición, el IETF define el concepto de *Provider Provisioned VPN* (PPVPN). Una PPVPN es un tipo de VPN, la cual es manejada por el SP y no por el cliente final. La alternativa para la PPVPN es una VPN manejada por el usuario en la cual la red del proveedor de servicio no participa en el manejo y provisión de la VPN y normalmente no es consciente de la existencia de la VPN. Aunque la mayoría de PPVPNs serán VPNs basadas en dispositivos PE, los dos conceptos no son completamente equivalentes, por ejemplo: una PPVPN puede ser una VPN basadas en dispositivos CE manejada por el proveedor de servicio.

3.3 MODELO DE VPNs *OVERLAY* Y *PEER TO PEER* [2]

Otra clasificación común de las VPNs está basada en: si el dispositivo CE del cliente y el proveedor de servicios intercambian información de enrutamiento de capa 3. Pueden definirse dos modelos de implementaciones de VPN basados en este criterio [2]:

- El Modelo *Overlay*, donde el servicio VPN es funcionalmente equivalente a las líneas arrendadas emuladas y el proveedor de servicio y el cliente no intercambian información de enrutamiento de capa 3. Este modelo proporciona una separación clara entre las responsabilidades del cliente y del proveedor.
- El Modelo *Peer to Peer*, donde el proveedor de servicio y el cliente intercambian información de capa 3. Tales implementaciones normalmente simplifican el enrutamiento del cliente y proporcionan una provisión más fácil del servicio VPN.

La figura 3.1, ilustra la distinción básica entre los dos modelos.

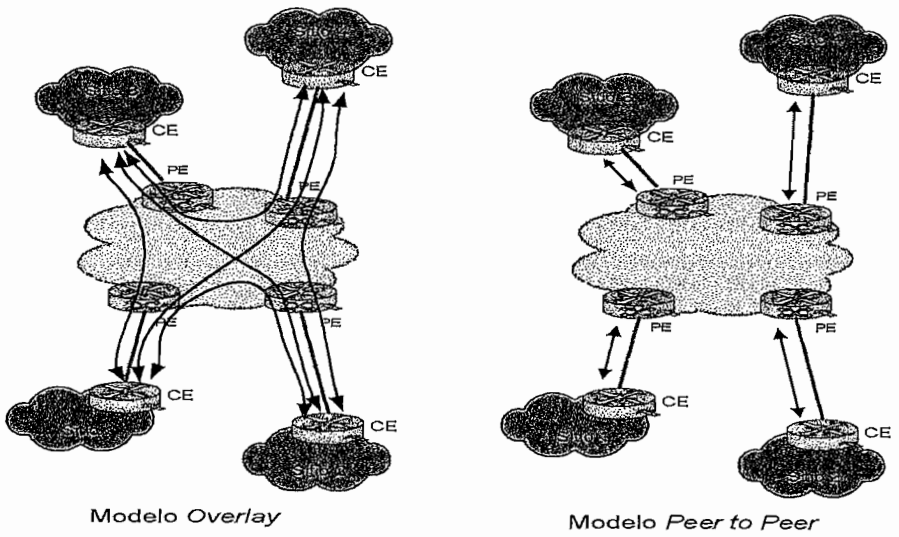


Figura 3.1: Modelo Overlay y Modelo Peer to Peer [10]

3.3.1 MODELO *OVERLAY*

Las VPNs en este modelo pueden implementarse con varias tecnologías WAN conmutadas de capa 2, incluyendo X.25, FR o ATM. Estas redes también se han implementado con tunelización IP sobre IP (IP-IP), en *backbones* IP privados y sobre el Internet público. Los dos métodos más usados de tunelización IP sobre IP son: GRE (*Generic Route Encapsulation*)[2] y el modo túnel de IPSec. Sin embargo, el modelo *overlay* tiene varios inconvenientes:

- Su comportamiento es bueno en configuraciones con pocos sitios centrales y muchos sitios remotos, pero se vuelve difícil manejar en una configuración más compleja.
- La provisión apropiada de las capacidades del circuito virtual requiere de un conocimiento detallado de los perfiles de tráfico de sitio a sitio, los cuales no están fácilmente disponibles.
- Cuando se implementa con tecnologías de capa 2, dicho modelo de VPN introduce otra capa innecesaria de complejidad e incrementa los costos operacionales.

[2] GRE es un protocolo de *tunneling* que puede encapsular una variedad de tipos de paquetes protocolares dentro de túneles IP, creando un enlace virtual punto a punto a los *routers* en puntos remotos.

3.3.2 MODELO *PEER TO PEER*

El modelo *Peer to Peer*, se introdujo para aliviar los inconvenientes del anterior modelo de VPN. En este modelo, el *router* localizado en el borde de la red del proveedor intercambia directamente información de enrutamiento con el *router* CE. El modelo *Peer to Peer* proporciona varias ventajas sobre el modelo tradicional *overlay*:

- El enrutamiento se vuelve simple, cuando el *router* del cliente intercambia información de enrutamiento con un solo *router* localizado en el borde de la red del proveedor, mientras que en la red VPN *overlay* el número de *routers* vecinos depende del número de sitios remotos, lo cual significa que puede crecer en un número grande.
- El añadir un nuevo sitio es más simple, porque el proveedor de servicio maneja solo un sitio adicional y cambia la configuración en el *router* PE conectado. En el modelo *overlay*, el proveedor de servicio debe proporcionar un conjunto entero de circuitos virtuales que conecta ese sitio a otros sitios del cliente de la VPN.

En la práctica, existe un criterio en base al cual se adopta un determinado modelo, este criterio es el tamaño. Para las implementaciones de pequeña escala, el modelo *overlay* es probablemente la manera más simple de construir una VPN. Para VPNs más grandes, el modelo *overlay* está claramente limitado en lo que se refiere a escalabilidad y el modelo *peer to peer* es la opción más apropiada.

Las VPNs basadas en MPLS usan un modelo *Peer to Peer*, en el cual la información de enrutamiento es intercambiada entre un dispositivo del cliente y un dispositivo del SP, y el SP es responsable por el establecimiento de los caminos a través del núcleo (*backbone*) y la propagación de las rutas entre los sitios del cliente.

Una ventaja de VPNs basadas en MPLS es que resultan ser mucho más escalables. Ellas están basadas en redes, no en conexiones, y consecuentemente

son fácilmente escalables. No hay necesidad de una topología completamente mallada de túneles o circuitos virtuales permanentes entre todos los sitios en la VPN. El despliegue y el mantenimiento en una VPN basada en MPLS resultan ser relativamente más fáciles que las opciones basadas en circuitos virtuales o tunelización IP.

La Seguridad y privacidad en las VPNs MPLS se logran limitando la información de enrutamiento a todos los miembros de la VPN. Las rutas de los sitios de la VPN son solamente notificadas a miembros de la misma VPN y no son compartidas con dispositivos fuera de la VPN.

3.4 VPNs MPLS [3], [4], [5], [6]

MPLS simplifica el enrutamiento de los paquetes y facilita la selección de caminos óptimos a través del Internet. Un beneficio importante adicional de MPLS es su soporte a las VPNs, permitiendo a los proveedores de servicio ofrecer servicios de red basados en Internet. MPLS también soporta calidad de servicio (QoS) permitiendo reservaciones de ancho de banda y prioridad de tráfico. MPLS está basado en el Protocolo de Internet (IP) existente y puede integrarse fácilmente con los protocolos de enrutamiento actuales (RIP, BGP-4, IS-IS, y OSPF).

Pueden actualizarse muchos *routers* existentes en el *backbone* de Internet para soportar MPLS simplemente agregando *software*. Los *routers* más recientes ya tienen capacidades opcionales de MPLS incluidas en su *software*.

MPLS sigue el paradigma contemporáneo de Internet de mover la mayoría de la complejidad de la red al borde. Esto significa que los servicios (VPNs, QoS, cifrado, autentificación, etc) se aplicarán a los paquetes y usuarios cuando ellos ingresen al Internet. Esto distribuye la carga asociada con el soporte de estas funciones complejas entre muchos *routers* de borde. Por consiguiente, no se requieren *routers* individuales para soportar todos estos servicios para todos los clientes del SP. Esto también significa que estos procesos adicionales no recargan a los *routers* del *backbone* de la red; ya que en cambio ellos pueden

permanecer enfocados en la tarea de enviar rápidamente los paquetes por el *backbone* de la red.

Las VPNs implementadas con MPLS (VPNs MPLS) solo se aplican al *backbone* del proveedor. Esto significa que el cliente solo tiene que solicitarla y el proveedor se encarga de proveerla y de hacerla activa sin afectar al cliente.

Esencialmente existen dos tipos de Redes Privadas Virtuales que pueden ser soportadas por MPLS:

VPNs MPLS de Capa 3: VPNs BGP/MPLS; éstas usan las extensiones al protocolo de enrutamiento existente del Internet (BGP – 4) para interconectar lugares remotos; este tipo de VPNs también se denominan "RFC 2547".

VPNs MPLS de Capa 2: la conectividad de capa 2 se extiende a clientes por una estructura MPLS; comúnmente llamadas "VPNs Martini/Kompella", ya que Luca Martini y Kireeti Kompella, ayudaron a desarrollar esta metodología.

Cabe destacar la existencia de otra clase de VPNs MPLS, que son consideradas como una tercera categoría de VPNs, las cuales utilizan métodos de *tunneling* sobre MPLS; y, emulan un circuito punto a punto de capa 2.

3.4.1 VPNs BGP/MPLS

Este es un modelo de capa 3 para crear VPNs basadas en MPLS. El estándar de facto para implementar tales VPNs se describe en el "RFC 2547", con una nueva versión, actualmente, bajo desarrollo referido como RFC 2547bis que se describe en el respectivo borrador (*draft*) [3].

Las VPNs BGP/MPLS son IP-VPNs basadas en dispositivos PE. El RFC 2547bis define un método que permite a los proveedores de servicio usar su *backbone* IP para proporcionar los servicios de una VPN a sus clientes. El cliente puede ser una empresa o un grupo de empresas, que necesiten una Extranet, un proveedor de servicio de Internet u otro proveedor de servicio de una VPN, usando el mismo

mecanismo para ofrecer VPNs a sus propios clientes. Las VPNs BGP/MPLS usan:

a. BGP para distribuir la información de enrutamiento de la VPN a través del *backbone* del proveedor, y
b. MPLS para enviar el tráfico de un sitio de la VPN a otro.

Estas VPNs son dependientes de los LSPs (*Label Switched Paths*), consecuentemente proveen todos los beneficios relacionados con esta tecnología. Así las ventajas en el desempeño, junto con la clasificación y segmentación de tráfico inherente a MPLS proveen un sólido fundamento sobre el cual las VPNs pueden ser construidas. Un beneficio adicional proporcionado por estas VPNs es la preservación del esquema de la dirección IP existente del cliente. Aún si un cliente del proveedor de servicios tiene solapamiento del espacio de direcciones IP (utiliza direccionamiento privado IP), estas direcciones serán efectivamente segmentadas para que el tráfico de datos y control permanezcan exclusivamente dentro de las respectivas VPNs.

3.4.1.1 Componentes de Red

En el contexto del RFC 2547bis, una VPN es una colección de políticas, las cuales controlan la conectividad entre un conjunto de sitios. Las VPNs solo existen en el borde de la red del proveedor de servicio. Los *routers* del *backbone* de la red no participan en las verdaderas VPNs, ellos mantienen el envío de paquetes sobre varios LSPs. Los *routers* del cliente tampoco participan en las VPNs, ellos mantienen el envío de paquetes IP de acuerdo a lo establecido en los esquemas de direccionamiento y enrutamiento del cliente.

Un sitio del cliente se conecta a la red del proveedor de servicio por uno o más puertos, un sitio es un conjunto de (sub)redes parte de la red bajo el control del cliente, donde el proveedor de servicio asocia cada puerto con una tabla de enrutamiento VPN. La figura 3.2, ilustra los componentes fundamentales de una VPN BGP/MPLS.

***Customer Edge* (CE) *Routers*:** éstos son los dispositivos localizados en el borde de la red del cliente y proporcionan al cliente acceso a la red del proveedor de servicios. Ellos ejecutan el(los) protocolo(s) de enrutamiento de elección del cliente, y soportan el esquema de dirección IP implementado por el cliente. Estos *routers* desconocen de la red MPLS o las VPNs. Sin embargo el próximo salto desde la perspectiva del dispositivo CE es el *router* PE. Los *routers* CE anuncian las rutas locales del sitio de la VPN al *router* PE, y aprenden rutas remotas de la VPN desde el *router* PE.

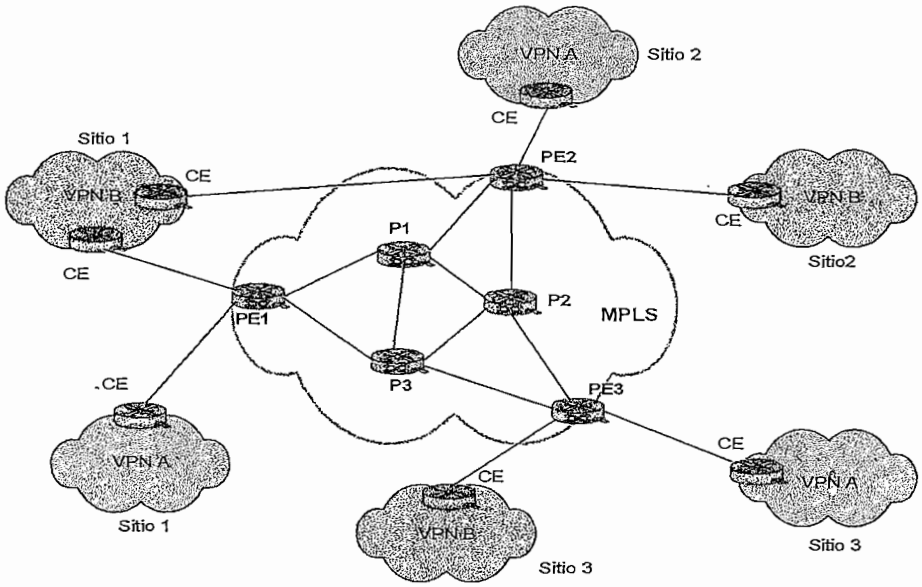


Figura 3.2: Componentes de red de una VPN BGP/MPLS

***Provider Edge* (PE) *Router*:** Todas las funciones asociadas con el establecimiento, mantenimiento y operación de las VPNs MPLS tienen lugar en los *routers* PE. Un *router* PE está conectado directamente con el *router* CE. Típicamente, un *router* PE estará conectado a múltiples *routers* CE soportando a diferentes clientes. El *router* PE se comunicará con el *router* CE mediante el protocolo de enrutamiento seleccionado por el cliente (RIP, OSPF, BGP, rutas estáticas, etc). Así, el *router* PE participará en las redes de Capa 3 de los clientes; aprenderá todas las rutas de los clientes y entregará paquetes derivados de esa información. Esto significa que si un *router* PE se conecta a una docena de clientes diferentes, necesitará participar en una docena de redes diferentes, cada

una de las cuales tendrá planes de direccionamiento y protocolos de enrutamiento únicos.

Este diseño refuerza la escalabilidad del modelo RFC 2547bis porque elimina la necesidad de que los *routers* PE mantengan todas las rutas de la VPN del proveedor de servicio. El *router* PE también debe comunicarse con otros *routers* PE para intercambiar información de accesibilidad. Por ejemplo, si un cliente en Quito tiene una sucursal en Guayaquil, el *router* PE en Quito necesitará comunicarse con el *router* en Guayaquil para establecer el túnel VPN apropiado. Para lograr esta tarea, los *routers* PE ejecutan Multiprotocolo BGP (MP-BGP) en sus enlaces de área extendida.

Los *routers* PE también necesitarán iniciar y terminar LSPs para que el tráfico MPLS sea enrutado a través del *backbone* (mediante *routers* P), es decir los *routers* PE actúan como los LSRs de borde (LERs).

***Provider* (P) *Router*:** Los *routers* P son los *routers* del proveedor en el *backbone* de la red. Éstos tienen la misma función que los LSRs, es decir conmutan los paquetes MPLS sobre LSPs establecidos. El tráfico es enviado a través del *backbone* MPLS usando una pila de etiquetas de nivel 2. Los *routers* P, no mantienen información de enrutamiento de VPN alguna, ya que nunca miran más allá de la etiqueta que se encuentra en la cima de la pila y desconocen completamente de la etiqueta localizada en el fondo de la pila o la etiqueta de la VPN transportada a través de la red MPLS.

Los *routers* P y PE comparten un IGP común y un protocolo de distribución de etiquetas. El IGP llena una tabla de enrutamiento global en todos los *routers* PE y P. El cliente es responsable del mantenimiento de los dispositivos CE.

3.4.1.2 Topologías de Redes Privadas Virtuales

Están disponibles diferentes topologías de VPNs. Probablemente la más común es la topología *hub and spoke*, también conocida como topología radial (ver figura

3.3), en la cual un número de sitios remotos (*spokes*) se conectan a un sitio central (*hub*); por ejemplo, una oficina central y un número de sucursales. Los sitios remotos no tienen una conectividad directa entre sí, solo a y desde el *hub*.

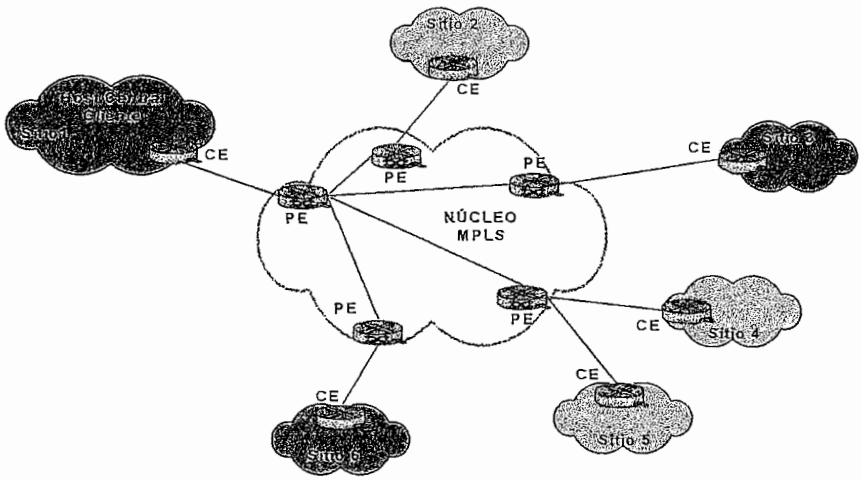


Figura 3.3: Topología Hub and Spoke o radial

Full mesh, es un término que describe una red en que los dispositivos son organizados en una topología de malla, en donde cada nodo de la red tiene una conectividad, mediante un circuito físico o circuito virtual, con cada uno de los otros nodos de la red (ver figura 3.4).

La topología *full mesh* (completamente mallada), proporciona mucha redundancia, pero debido a que puede ser prohibitivamente caro el implementarse, usualmente es reservada para los *backbones* de la red.

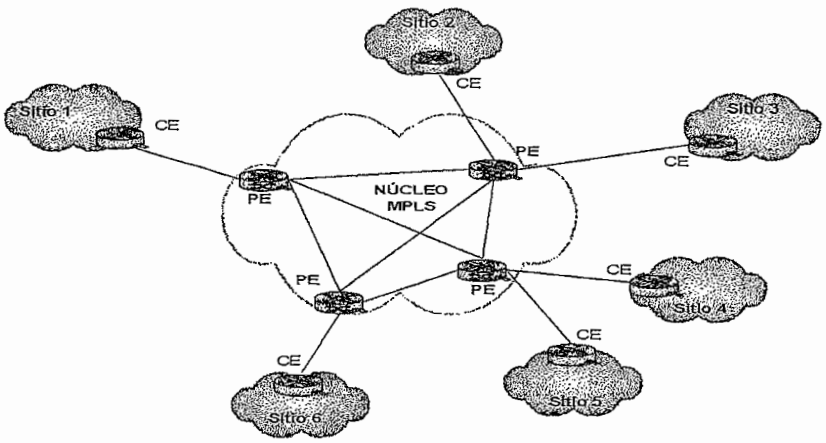


Figura 3.4: Topología Full Mesh o completamente mallada

3.4.1.3 Tablas VRF (*VPN Routing and Forwarding*)

Los *routers* PE participan en el enrutamiento y planes de numeración IP de todos y de cada uno de los clientes directamente conectados. Muchos de estos planes de numeración pueden solaparse (como el comúnmente usado espacio de direcciones 10.x.x.x). Los *routers* PE deben asegurar que el tráfico destinado para la red 10.x.x.x de la compañía A no se entregará inadvertidamente a la red IP 10.x.x.x de la compañía B. Esto se consigue, asegurando que las VPNs tengan sus propias tablas de enrutamiento y envío en el *router* PE, así un sitio del cliente que pertenece a una VPN puede acceder solamente a un conjunto de rutas contenidas en un dicha tabla.

En términos del RFC 2547bis, la tabla de enrutamiento y envío se denomina **VRF** (*VPN Routing and Forwarding*). Una tabla VRF puede ser considerada como un *router* virtual. La tabla VRF provee aislamiento entre VPNs y permite usar solapamiento y direcciones privadas IP. El *router* PE aprende las rutas del cliente de los *routers* CE conectados. Las rutas del cliente se distribuyen a otros *routers* PE usando MP-BGP.

Debe notarse que una tabla VRF no necesariamente corresponde a una VPN particular. Su propósito es guardar las rutas que están disponibles a un sitio particular conectado a un *router* PE. El *router* PE es configurado, de tal manera que cada una de sus VRFs es asociada con una o más interfaces en el *router* PE el cual conecta a los clientes del proveedor de servicios. Si un sitio dado contiene *hosts* que son miembros de múltiples VPNs, la VRF asociada con el sitio del cliente contiene las rutas para todas las VPNs de las cuales el sitio es un miembro, como se muestra en la figura 3.5. Esto es conocido como reuso de la VRF. Las tablas VRF deben ser propagadas a otros dispositivos PE, para esto se hace uso de elementos denominados atributos de comunidad extendida BGP, tema a tratarse en la sección 3.4.1.6.3.

Los métodos para llevar a cabo las VRFs varían de fabricante a fabricante. Éste es un componente altamente crítico de las VPNs RFC 2547 porque esta

implementación asegura la segmentación apropiada de tráfico del plano de datos y de control.

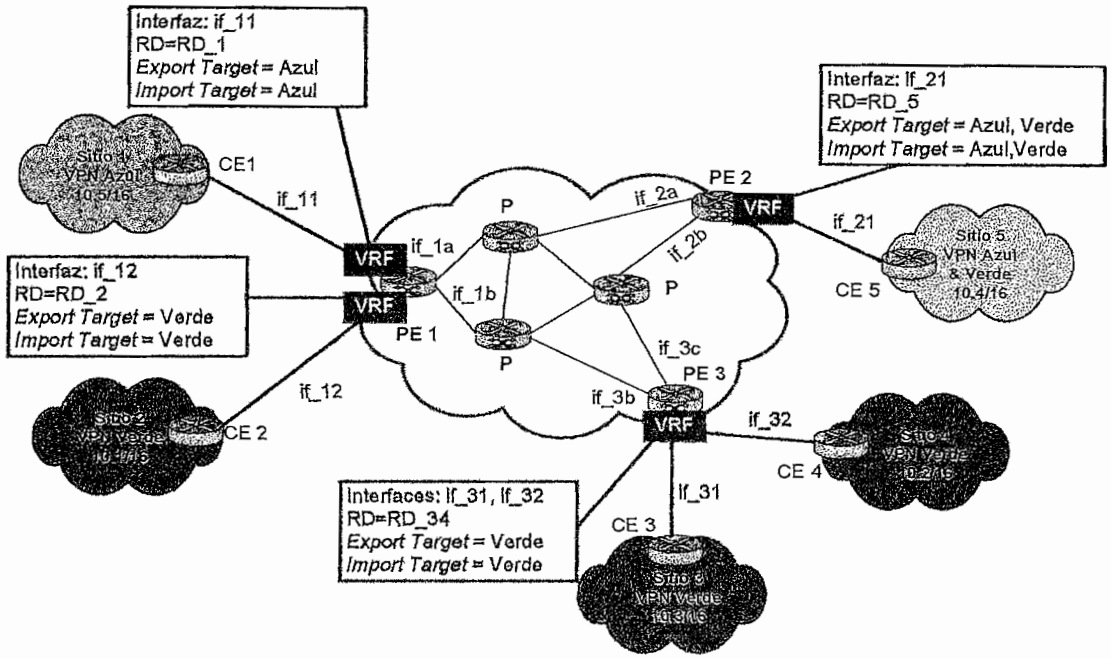


Figura 3.5: Tablas VRF

3.4.1.4 Solapamiento de los espacios de dirección del cliente

En las redes del cliente que no usan direcciones IP globalmente únicas (por ejemplo direcciones privadas definidas en el RFC 1918[3]), la misma dirección IPv4 puede usarse para identificar los diferentes sistemas en diferentes VPNs. Esto resulta en dificultades de enrutamiento ya que BGP asume que cada dirección IPv4 que transporta es globalmente única. Este problema se resuelve en las VPNs BGP/MPLS con el apoyo de un mecanismo que convierte direcciones IP que no son únicas en direcciones globalmente únicas usando la familia de direcciones VPN-IPv4 ó VPNv4, junto con las extensiones Multiprotocolo de BGP (MP-BGP).

---

[3] La "Autoridad de Números Asignados en Internet" (IANA, *Internet Assigned Numbers Authority*), ha reservado los tres siguientes bloques de direcciones IP para el uso en internets privadas:

10.0.0.0 - 10.255.255.255 (prefijo 10/8)
172.16.0.0 - 172.31.255.255 (prefijo 172.16/12)
192.168.0.0 - 192.168.255.255 (prefijo 192.168/16)

Así las VPNs MPLS permiten a las redes del sitio del cliente usar espacios de direcciones privadas, en lugar de las direcciones IP globalmente únicas. Esto se logra asegurando direcciones públicas únicas para el uso dentro de la VPN, por medio de los Distinguidores de Ruta (RDs, *Route Distinguishers*).

El Distinguidor de ruta no tiene ninguna semántica, da la información sobre el origen de la ruta. El único propósito es crear distintas rutas a una dirección común. Aunque el RD puede pensarse como un número identificador de sitio, éste realmente identifica la interfaz PE enlazada al sitio. Los RDs son bloques de 8 *bytes* colocados antes de la dirección IPv4 para identificar la VRF a la cual la ruta pertenece. Todas las VRFs deben tener un solo distinguidor de ruta, el proveedor de servicio debe asegurar que cada RD sea globalmente único.

Distinguidor de Ruta = Tipo + ASN + Número Asignado

Dirección VPN-IP = Distinguidor de ruta + Dirección IP

El uso del espacio público ASN o el espacio de dirección IP público garantiza que cada RD sea globalmente único. RDs únicos, proporcionan un mecanismo que permite a cada proveedor de servicio administrar su propio espacio de dirección y crear direcciones VPN-IPv4[4] globalmente únicas sin entrar en conflicto con las asignaciones de RD que son hechas por otros proveedores de servicios.

Un distinguidor de ruta contiene tres campos: El primer campo de 2 bytes indica el tipo de distinguidor de ruta que sigue. Según el campo tipo, los dos campos restantes muestran la estructura del distinguidor de ruta que puede ser ASN:nn o dirección IP:nn. Se recomienda el uso de ASN:nn con un número de sistema autónomo, que es asignado por el IANA para que sea único entre los proveedores de servicios. Se debe utilizar el formato dirección IP:nn sólo cuando la red VPN MPLS use un número de AS privado pero las direcciones VPN-IPv4 sean anunciadas más allá del AS privado.

[4] Para soportar VPN-IPv6, un *backbone* MPLS que soporta RFC 2547 VPN necesita actualizar los *routers* PE que están conectados a los clientes VPN IPv6. Esto significa que, desde el punto de vista de los proveedores de servicio, la migración del cliente de la VPN a IPv6 no requerirá la migración del *backbone* a IPv6. Pero el tema sigue en estudio.

Así, el segundo campo identifica el número del sistema autónomo (ASN) del ISP desde el cual el VRF se originó. Y el siguiente campo es un número asignado para la VPN dentro de dicho ISP. Por ejemplo, un distinguidor de ruta puede representarse como 101:1 (ver figura 3.6). En este ejemplo, 101 es el ASN del ISP y 1 es el número asignado para esa VRF particular. Este sistema de numeración asegura que todas las VRFs tengan universalmente identificadores únicos, aún cuando ellas crucen múltiples ISPs.

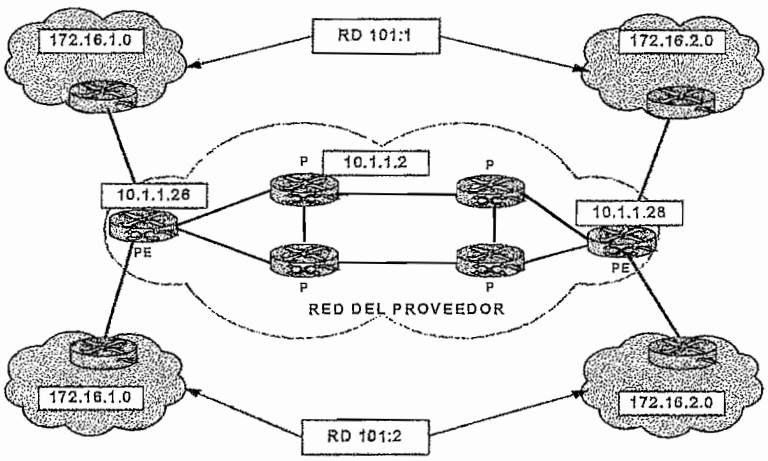


Figura 3.6: Distinguidor de ruta

Este identificador es exclusivamente para actualizaciones de enrutamiento, o tráfico de control y no afecta el tráfico de datos en lo absoluto. Las actualizaciones de enrutamiento son realizadas mediante una derivación de BGP. Todos los *routers* PE se comunican con otros mediante MP-BGP. El distinguidor de ruta se vuelve parte del campo NLRI (*Network Layer Reachability Information*) en una actualización de enrutamiento de MP-BGP, ver el Anexo A.

3.4.1.5 Opciones de conectividad PE a CE

Para proveer el servicio de VPN, el *router* PE necesita ser configurado de manera que cualquier información de enrutamiento aprendida de una interfaz del cliente de la VPN pueda asociarse con una VRF particular. Se puede hacer esto durante el proceso del protocolo de enrutamiento estándar, lo que se conoce como contexto de enrutamiento. Cada VRF usa un contexto de enrutamiento diferente.

Cualquier ruta aprendida a través de una interfaz que está asociada con el contexto del protocolo de enrutamiento particular es instalada en la VRF asociada. Cualquier ruta aprendida de una interfaz que *no* es parte de algún contexto de enrutamiento VRF, es colocada en la tabla de enrutamiento global. Esto permite la separación de la información de enrutamiento en diferentes contextos, aunque la información es aprendida por el mismo proceso del protocolo de enrutamiento. Esto crea efectivamente protocolos de enrutamiento conscientes de la VPN.

En el caso donde el dispositivo CE es un *host* o un *switch*, este conjunto de direcciones se configurará en el *router* PE conectado a ese dispositivo. En el caso donde el dispositivo CE es un *router*, existen varias maneras que un *router* PE pueda obtener este conjunto de direcciones.

El *router* PE traduce estas direcciones en direcciones VPN-IPv4, usando el RD configurado. El *router* PE entonces trata estas direcciones VPN-IPv4 como entradas de BGP. Las rutas de un sitio de la VPN no se filtran en el IGP del *backbone*.

Las posibles técnicas de distribución de rutas PE-CE, ver figura 3.7, son:

1. La primera opción es ejecutar el enrutamiento estático entre los *routers* PE y CE. La información del enrutamiento estático es *redistribuida* a BGP para ser anunciada a través de las sesiones MP-iBGP. Esta es una buena elección para el despliegue cuando el sitio tiene un punto de entrada a la red del SP porque existe muy poco que ganar por medio del aprendizaje dinámico de las rutas del cliente a través del enlace PE-CE.

   Una ruta estática para cada red (o ruta agregada) más allá del *router* CE debe ser configurada en la VRF del *router* PE que conecta el sitio (asumiendo que otros miembros de la VPN pueden acceder a la red). Éste es el mismo tipo de configuración para el enrutamiento IP normal.

2. Los *routers* PE y CE pueden ser pares (*peers*) RIP y el *router* CE puede usar RIP para decirle al *router* PE el conjunto de prefijos de dirección que son accesibles en el sitio del *router* CE. Cuando se configura RIP en el *router* CE, se debe tener cuidado de asegurar que los prefijos de dirección de otros sitios (es decir, prefijos de dirección aprendidos por el *router* CE del *router* PE) nunca sean anunciados al PE. Más precisamente si un *router* PE, (PE1), recibe una ruta VPN-IPv4 (R1), y como resultado distribuye una ruta IPv4 (R2) a un CE, entonces R2 no debe distribuirse nuevamente desde ese sitio del *router* CE a un *router* PE, (PE2), donde PE1 y PE2 pueden ser el mismo *router* o *routers* diferentes, a menos que PE2 asigne R2 a una ruta VPN-IPv4 que es diferente que (es decir, contiene un RD diferente) R1.

3. Los *routers* PE y CE pueden ser pares OSPF. Un *router* PE que es un par OSPF de un *router* CE aparece, al *router* CE, como un *router* de área 0. Si un *router* PE es un par OSPF de *routers* CE que están en VPNs distintas, el *router* PE debe estar ejecutando múltiples instancias de OSPF.

   Las rutas IPv4 que el *router* PE aprende del *router* CE mediante OSPF son redistribuidas en BGP como rutas VPN-IPv4. Se usan los atributos de comunidad extendida, ver sección 3.4.1.6.3, para transportar junto con la ruta, toda la información necesaria para permitir a la ruta ser distribuida a otros *routers* CE de la VPN en el tipo apropiado de OSPF LSA. La ruta OSPF etiquetada se usa para asegurar que las rutas recibidas del *backbone* BGP/MPLS no se envíen nuevamente al *backbone*.

4. Los *routers* PE y CE pueden ser pares BGP, y el *router* CE puede usar BGP (en particular eBGP) para decirle al *router* PE el conjunto de prefijos de dirección que están en el sitio del *router* CE. Esta técnica tiene varias ventajas sobre las otras:

a) Al contrario de las alternativas de IGP, ésta no requiere que el *router* PE ejecute múltiples instancias de algoritmos de enrutamiento para hablar con múltiples *routers* CE.
b) BGP es explícitamente diseñado para esta función: pasar la información de enrutamiento entre sistemas manejados por diferentes administradores.

Si el dispositivo CE es un *router*, también necesitará aprender las rutas desde un *router* PE. Por lo tanto, cualquier procedimiento usado para distribuir las rutas del *router* CE al *router* PE también será usado para distribuir las rutas del *router* PE al *router* CE.

3.4.1.6 Distribución de rutas mediante BGP

Varios *routers* dentro de la VPN se comunican usando BGP, un protocolo de enrutamiento IP que define cómo las rutas pueden ser distribuidas. BGP transporta la información acerca de los *routers* CE solamente a los miembros de la misma VPN, garantizando así seguridad.

3.4.1.6.1 El Protocolo BGP y Sistemas Autónomos

Un sistema autónomo [5] puede comprender una o muchas redes y cada red puede o no tener una estructura interna de subredes. La comunicación BGP que tiene lugar dentro de un sistema autónomo (es decir, entre *routers* PE dentro de la red del proveedor de servicios) es conocida como BGP Interno (iBGP). La comunicación BGP entre diferentes sistemas autónomos, es decir, entre un *router* PE y un *router* CE, es conocida como BGP Externo (eBGP), ver figura 3.7. Cada AS es identificado por un número de sistema autónomo (ASN), que se requiere cuando se ejecuta BGP.

[5] AS (*Autonomous System*): conjunto de *routers* (y redes) bajo una misma administración y con las mismas políticas de ruteo. Una AS se ve como una sola entidad y cada AS tiene asociado un número de 16 *bits*. Cada AS puede escoger su propio protocolo de enrutamiento y debe intercambiar información de enrutamiento con otros ASs. Los protocolos de enrutamiento internos de los ASs son denominados IGPs (*Interior Gateway Protocol*), por ejemplo: RIP y OSPF; y los protocolos de enrutamiento entre ASs son denominados EGPs (*Exterior Gateway Protocol*), por ejemplo: EGP y BGP.

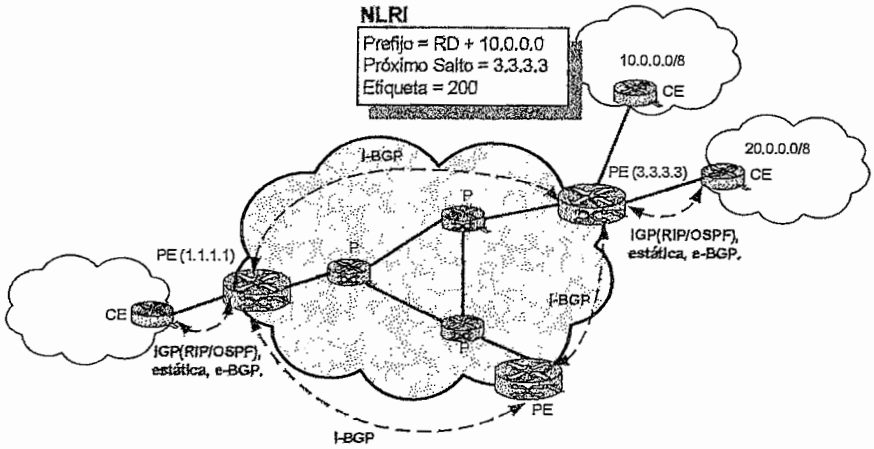


Figura 3.7: Protocolos de enrutamiento usados en una VPN BGP/MPLS

Las redes del proveedor de servicio normalmente usan BGP, así ellos ya tendrán un ASN asignado. Sin embargo si eBGP es usado como el protocolo de enrutamiento entre los *routers* PEs y CEs, un ASN debe asignarse a cada sitio del cliente en la red por separado.

3.4.1.6.2 Extensiones Multiprotocolo BGP

Una limitación de usar BGP-4 convencional para el soporte de las VPNs BGP/MPLS es que originalmente fue diseñado para transportar información de enrutamiento sólo para la familia de direcciones IPv4. Comprendiendo esta limitación, el IETF está trabajando para estandarizar las extensiones Multiprotocolo para BGP. Las extensiones permiten a BGP transportar información de enrutamiento para múltiples protocolos de capa red (IPv6, IPX, VPN-IPv4, etc). Por consiguiente, para desplegar las VPNs BGP/MPLS y apoyar la distribución de rutas de VPN-IPv4, se exige a los *routers* PE soportar las extensiones de MP-BGP y no simplemente BGP convencional.

Antes de intercambiar la información de enrutamiento VPN-IPv4, el RFC 2547bis requiere que las *capacidades* de negociación de BGP tengan lugar para asegurar que los vecinos BGP sean capaces de procesar la familia de direcciones VPN-IPv4. Se debe anotar que las extensiones MP-BGP son compatibles con las versiones anteriores de BGP de modo que un *router* que ejecuta estas

extensiones pueda interoperar con un *router* que no ejecuta dichas extensiones al usar BGP convencional (sin embargo, el BGP convencional no soporta las RFC 2547bis VPNs).

3.4.1.6.3 Atributos de la Comunidad Extendida BGP

La información de enrutamiento de la VPN es distribuida a través del uso de atributos de comunidad extendida BGP. Una comunidad extendida es un grupo de destinos que comporten alguna propiedad en común. Así una ruta BGP es descrita por:

- Atributos de comunidad BGP estándar, (por ejemplo: Preferencia_Local, *MED*, Siguiente_salto, Camino _AS, etc.), y
- Atributos de comunidad extendida BGP.

Los atributos de la comunidad extendida son usados para restringir la distribución de rutas de la VPN usando filtración de la ruta y son transportados en mensajes BGP como atributos de la ruta. Cada atributo debe ser globalmente único y solo puede usarse por una VPN. Ellos identifican la ruta que pertenece a una colección específica de rutas, todas las cuales son tratadas de la misma manera con respecto a la política de enrutamiento.

El RFC 2547bis puede usar tres tipos diferentes de atributos de comunidad extendida.

El atributo *route target*, identifica una colección de sitios (VRFs) a los cuales un *router* PE debe distribuir rutas. Un *router* PE usa este atributo para restringir la importación de rutas remotas en sus VRFs. Se tiene dos tipos de *Route Targets*:

- *Route Target* Exportada: Cada ruta VPN se etiqueta con uno o más *route targets* cuando se exporta de una VRF (para ser ofrecido a otras VRFs).

- *Route Target* Importada: Un conjunto de *route targets* pueden asociarse con una VRF, y todas las rutas etiquetadas con por lo menos una de esas *route targets* se insertarán en la VRF.

El atributo *VPN de origen*, identifica una colección de sitios que pertenece a la VPN.

El atributo *sitio de origen (SOO, Site of Origin)*, el propósito de este atributo es identificar el nodo desde el cual fue propagada originalmente una ruta. Este atributo es necesario para asegurar que una ruta aprendida de un sitio particular mediante una conexión PE/CE no sea distribuida nuevamente al sitio a través de una conexión PE/CE diferente.

Cada uno de los atributos de comunidad extendida están codificados como un valor de 8 octetos. Los dos primeros octetos definen el tipo de atributo, los siguientes seis octetos contienen el valor del atributo. Los tipos entre 0 y 0x7FFF son asignados por el IANA y los tipos entre 0x8000 y 0xFFFF son específicos del fabricante. La comunidad extendida *route target* tiene un código del tipo de 0x0002 ó 0x0102 y la comunidad extendida SOO tiene un código del tipo de 0x0003 ó 0x0103. La estructura del campo valor depende del *byte* de orden superior del campo de tipo.

Rutas locales son distribuidas a otros *routers* PE después que el *router* PE de ingreso une un atributo *route target* a cada ruta aprendida de los sitios directamente conectados.

3.4.1.6.4 Actualización de BGP

Las actualizaciones BGP están basadas en la importación y exportación de políticas de enrutamiento de cada *router*. Para que una VRF se establezca dentro de un *router* PE, se debe colocar una política explícita para aceptar (importación) y propagar (exportación) el distinguidor de ruta particular asociado con dicha VRF, ver figura 3.8.

La actualización de BGP consta de:

- Prefijo VPN-IPv4.
- Dirección del siguiente salto (dirección *loopback* del *router* PE).
- Atributos de Comunidad Extendida (*route target*, SOO).
- Otros atributos del BGP estándar (Preferencia_Local, MED, Camino_AS, Comunidad Estándar).
- Etiqueta MPLS, la cual representa: la interfaz saliente del *router* PE o la VRF donde una búsqueda tiene que ser hecha.

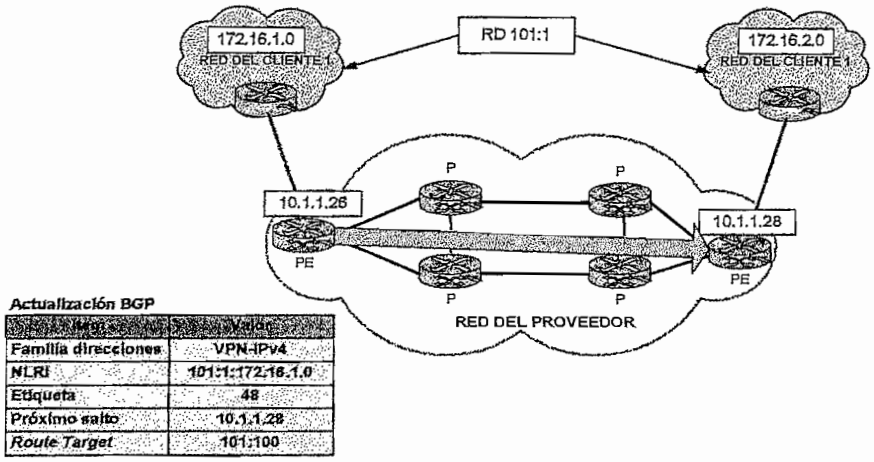


Figura 3.8: Actualización de BGP

3.4.1.6.5 Distribución de la Información de enrutamiento

Cada *router* PE es configurado para asociar una VRF con cada interfaz o subinterfaz sobre la cual aprende las rutas de cada *router* CE que se conecta al *router* PE. Cuando el *router* CE anuncia una ruta para un cierto prefijo al *router* PE, éste instala una ruta local en la VRF correspondiente. El *router* PE entonces anuncia la ruta para este prefijo a todos los otros *routers* PEs (los cuales conectan sitios que participan en la VPN). Antes de anunciar la ruta, el *router* PE selecciona una etiqueta MPLS para anunciarla junto con la ruta y asignar su dirección *loopback* como el próximo salto BGP para dicha ruta. El RFC 2547bis apoya el solapamiento de los espacios de dirección por el uso de distinguidores de ruta (RDs) y la familia de direcciones VPN-IPv4. Cuando una ruta VPN-IPv4 es creada por un *router* PE, ésta es asociada con una o más *Route Targets*.

La distribución de la información de enrutamiento se puede resumir en cinco pasos:

1. Del sitio (CE) al proveedor de servicio (PE) - por ejemplo: mediante RIP, enrutamiento estático, OSPF o BGP (ver figura 3.7).
2. En el *router* PE de ingreso, esta información se exporta en el BGP del proveedor.
3. Esta información es distribuida dentro del proveedor de servicio entre los *routers* PE usando BGP.
4. En el *router* PE de salida, la información de enrutamiento es importada del BGP del proveedor.
5. Del proveedor de servicio (PE) al sitio (CE) - por ejemplo: mediante RIP, enrutamiento estático, OSPF o BGP.

El RFC 2547bis restringe la distribución de la información de enrutamiento entre los *routers* PE por el uso de filtración de la ruta basada en los atributos de comunidad extendida BGP (*route targets*); esto es realizado por el *router* PE de ingreso en el paso 2. MP-BGP asigna una *Route Target* para que el *router* PE remoto inserte tales rutas en la adecuada VRF. Cuando un *router* PE recibe una ruta anunciada de otro PE, determina si debe instalar la ruta en una VRF particular realizando una filtración de la ruta basada en los atributos de comunidad extendida BGP transportados con la ruta; esto es realizado por el *router* PE de salida en el paso 4. Si la ruta se instala en la VRF, el *router* PE entonces anuncia la ruta al *router* CE asociado.

3.4.1.7 Envío de Datos

Para usar MPLS en el envío del tráfico de la VPN a través del *backbone* del proveedor de servicio, se deben establecer los LSPs entre los *routers* PE. Los LSPs se establecen y se mantienen a través de la red del proveedor de servicio usando el protocolo de distribución de etiquetas (LDP) o uno que soporte ingeniería de tráfico, como es el caso de RSVP. El proveedor usa LDP para establecer un LSP de mejor esfuerzo (*best effort*) entre dos *routers* PE o usa

RSVP para asignar ancho de banda al LSP o para usar ingeniería de tráfico para seleccionar un camino explícito para el LSP.

Con la introducción de MPLS, cada paquete de la VPN es etiquetado por el *router* PE de ingreso con una etiqueta que es identificada en el *router* PE de salida. Todos los *routers* en la red conmutan etiquetas sin mirar dentro de los paquetes. La preparación para este proceso es como sigue:

Cada *router* PE necesita un identificador único (una ruta *host*, usualmente se usa la dirección IP *loopback*), el cual es propagado a través de la red (*routers* P) usando un IGP. Esta dirección IP se usa también como el atributo de siguiente salto de BGP de todas las rutas de la VPN anunciadas por el *router* PE. Una etiqueta es asignada en cada *router* P para esa ruta *host* y es propagada a cada uno de sus vecinos. Finalmente, todos los otros *routers* PE reciben una etiqueta asociada con el *router* PE de salida a través de un proceso de distribución de etiquetas de MPLS. Después la etiqueta asignada por el *router* PE de salida es recibida por el *router* PE de ingreso, entonces el intercambio de paquetes VPN puede iniciar.

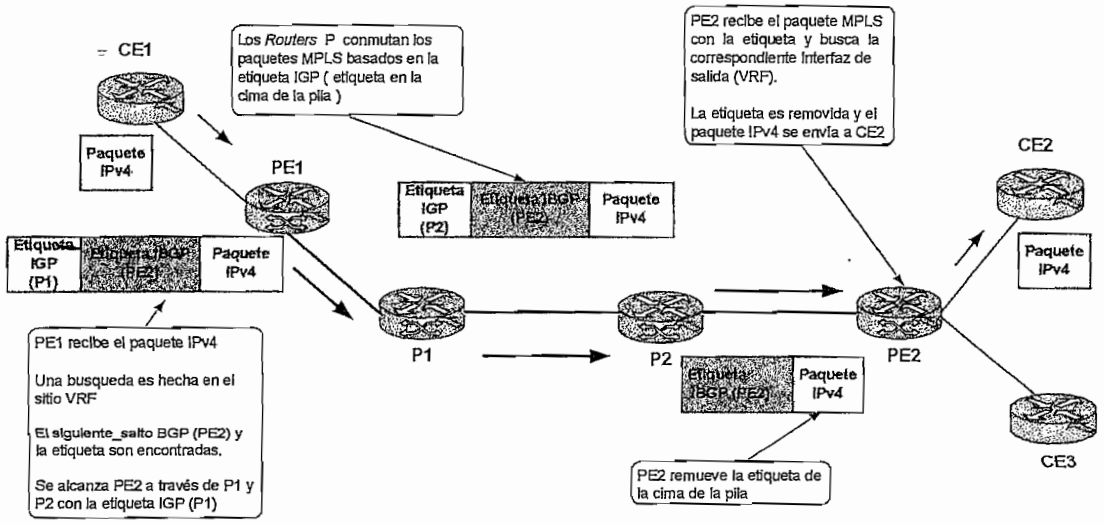


Figura 3.9: Envío de datos

Sin embargo, cuando el *router* PE de salida recibe el paquete de la VPN, no tiene información para determinar a que destino debe enviar el paquete. Para hacer

que la comunicación entre los sitios de la VPN sea única, se debe colocar una segunda etiqueta en la pila de etiquetas (ver figura 3.9).

Cada *router* PE asigna una única etiqueta para cada ruta en cada VRF. Estas etiquetas son propagadas junto con las rutas correspondientes a través de MP-BGP a todos los *routers* PE. Los *routers* PE reciben la actualización de MP-BGP e instalan las rutas recibidas en sus tablas VRF, también instalan la etiqueta asignada por el *router* de salida en sus tablas VRF.

Cuando un *router* PE de ingreso recibe un paquete de la VPN, examina la correspondiente VRF y busca la etiqueta que el *router* PE de salida ha asociado con la dirección de destino. Otra etiqueta, que apunta al *router* PE de salida, se obtiene de la tabla de envío global. Ambas etiquetas son combinadas en una pila de etiquetas MPLS, se adjuntan en la parte delantera del paquete de la VPN, y se envían hacia el *router* PE de salida.

Los *routers* P conmutan el paquete MPLS basado en la etiqueta que se encuentra en la cima de la pila de etiquetas, la cual apunta al *router* PE de salida. Al llegar al *router* PE de salida, éste recibe el paquete etiquetado, removerá la primera etiqueta y realiza una búsqueda en la segunda etiqueta, la cual identifica la VRF. La búsqueda se realiza en la VRF correspondiente, y el paquete es enviado hacia el *router* CE apropiado.

Para abreviar, la etiqueta exterior se usa para enviar el paquete a través del dominio MPLS al *router* de salida, es decir indica el túnel. Y la etiqueta interna se usa para entregar el paquete al cliente correcto, es decir diferencia las VPNs. El solapamiento y aislamiento de tráfico entre VPNs se realizan a través del mecanismo de envío de MPLS.

3.4.1.8 Seguridad en las VPNs BGP/MPLS

Las Redes Privadas Virtuales implican seguridad. Por consiguiente es muy importante que los usuarios de VPNs entiendan la tecnología de redes en las

cuales las conexiones seguras existen. Ellos pueden entonces juzgar por si mismos si una tecnología particular proporciona un nivel de seguridad y riesgo, o no.

Las VPNs RFC 2547 brindan seguridad mediante la separación y segmentación del tráfico. Cuando los *routers* del proveedor de servicio están todos correctamente configurados, cada cliente individual está representado por una sola VRF. El tráfico destinado para cada VRF transportará su propio valor de etiqueta interna. Por consiguiente el tráfico de datos de la compañía A será lógicamente y físicamente separado de la información de la compañía B.

Medidas adicionales pueden ser implementadas para complementar los aspectos básicos de seguridad con las VPNs RFC 2547. El cifrado es probablemente el método más deseable para asegurar los datos; la mayoría de los mecanismos de cifrado IP pueden residir transparentemente sobre una infraestructura MPLS. En términos de seguridad, las VPNs MPLS no proporcionan cifrado o algún mecanismo de seguridad específico. En todo caso, asumiendo que el proveedor de servicio sea fidedigno, la seguridad de la VPN está garantizada por el aislamiento de tráfico y dirección, y separación del enrutamiento, aspectos que la mayoría de las implementaciones de VPN MPLS pueden proporcionar.

En ciertos escenarios de las VPNs, puede usarse IPSec y MPLS como tecnologías complementarias. IPSec debe usarse en casos donde se requiere una autentificación fuerte y confidencialidad (típicamente, acceso remoto a VPNs a través del Internet público o algunas redes no confiables); mientras que MPLS proporciona funciones flexibles de control de la VPN y permite ingeniería de tráfico y diferenciación del tráfico requerido para las implementaciones de grandes VPNs.

3.4.2 VPNs MPLS DE CAPA 2

Tradicionalmente, la manera más común para las compañías de construir sus propias redes de área extendida (WAN) es colocar una infraestructura de capa 3

sobre varios enlaces punto a punto (basados en líneas arrendadas o circuitos virtuales) proporcionadas por un proveedor de servicios. Este modelo corresponde a lo que normalmente se conoce como "VPN de capa 2" ("L2 VPN").

Una de las soluciones recientemente presentadas son las VPNs de capa 2 basadas en MPLS, que mantienen los beneficios de una VPN tradicional de capa 2. Este enfoque de capa 2 proporciona una separación completa entre la red del proveedor y la red del cliente, es decir, no hay ningún intercambio de ruta entre los dispositivos PE y los dispositivos CE. La separación entre la red del proveedor y las redes del cliente proporcionan simplicidad. Así, la solución sigue el modelo *overlay* de VPNs (ver sección 3.3.1).

Las VPNs MPLS de capa 2 proporcionan servicios emulados capaces de transportar las tramas de capa 2 del cliente de un sitio a otro. Esto se hace de una manera que es totalmente transparente a los dispositivos CE. Por ejemplo un dispositivo CE puede ser configurado con un DLCI para poder "hablar" con otros CEs a través de la red del proveedor, lo cual aparece como una tradicional nube de capa 2 para el cliente. Dentro de la red del proveedor de servicio, los paquetes de capa 2 serán transportados en la red MPLS por los LSPs.

La meta de este tipo de VPNs es la extensión, en lugar del reemplazo, de los servicios de VPNs de capa 2 ya existentes. Las VPNs de capa 2 toman el tráfico de capa 2 existente y lo envían a través de túneles punto a punto en el *backbone* de la red MPLS. La fácil migración de VPNs tradicionales de capa 2 es una ventaja significativa de este modelo, ya que los dos tipos de VPN son indistinguibles desde el punto de vista del cliente.

En una VPN MPLS de capa 2, el *router* PE no es un par del *router* CE y no mantiene tablas de enrutamiento separadas. Más bien, simplemente asigna el tráfico de capa 2 entrante hacia el túnel punto a punto apropiado. El resultado se describe mejor como un modelo "*overlay*", opuesto al modelo "*peer to peer*" de capa 3 (ver sección 3.3.2).

3.4.2.1 Arquitectura L2 VPN

Las autoridades propusieron *drafts* para las L2 VPNs en dos grupos dentro del IETF: el grupo PWE3 (*Pseudo Wire Emulation Edge to Edge*) y el grupo PPVPN (*Provider-Provisioned VPN*). Los documentos relacionados con las VPNs de capa 2 emitidos por los grupos de trabajo PPVPN y PWE3 soportan tunelización usando IP, L2TP, pero la mayoría de los trabajos están alrededor de MPLS. Sin embargo todavía no existe estándar alguno para este tipo de VPNs. Algunos de los *drafts* actuales de Internet que han llamado la atención son los de Luca Martini y Kireeti Kompella.

Así, los esfuerzos del IETF por definir los mecanismos para crear VPNs MPLS de capa 2 están basados en dos tipos de conceptos. Primero, con MPLS, es posible crear un túnel como un LSP usando conmutación de etiquetas en lugar del encapsulamiento de capa 3. Segundo, es posible usar los protocolos de control, tales como LDP (*Label Distribution Protocol*) y BGP, para establecer los circuitos virtuales emulados (VCs) que transportan las PDUs (*Protocol Data Units*) de los protocolos de capa 2 por una red. Un número de tales circuitos emulados pueden transportarse en un solo túnel puesto que las PDUs son encapsuladas.

3.4.2.2 Martini L2 VPN [4], [5]

El establecimiento de circuitos virtuales emulados, también llamadas Líneas Virtuales Arrendadas (VLL, *Virtual Leased Line*) o conectividad punto a punto de capa 2 por un *backbone* MPLS, se especifica en los *drafts* del IETF que son conocidos como: "*drafts* Martini".

Existen dos *drafts* Martini: el primero, el *draft* de encapsulación, especifica el encapsulamiento del circuito virtual emulado para FR, ATM, Ethernet, HDLC y PPP; también define un campo demultiplexor, el cual se usa en un ambiente MPLS para distinguir circuitos virtuales emulados individuales dentro de un solo túnel. Además, este *draft* especifica una nueva Palabra de Control.

El segundo *draft*, define los procedimientos de distribución de etiquetas necesarios para transportar las PDUs encapsuladas a través de una red MPLS, es decir especifica la señalización para el establecimiento de los circuitos punto a punto de capa 2 sobre una red MPLS. Actualmente, Martini especifica LDP para establecer los túneles LSPs.

3.4.2.2.1 Encapsulación del paquete

En una red MPLS, es posible usar los protocolos de control para establecer los circuitos virtuales emulados que transportan las PDUs de protocolos de capa 2 a través de la red. Se puede transportar un número de estos circuitos virtuales emulados en un solo túnel. Esto requiere que las PDUs de capa 2 se encapsulen. Se puede distinguir tres niveles de encapsulación:

Cabecera del túnel: contiene la información necesaria para transportar la PDU por la red MPLS; ésta es la cabecera que pertenece al protocolo de tunelización, por ejemplo: MPLS, GRE, L2TP.

Campo demultiplexor: que se usa para distinguir los circuitos virtuales emulados individuales dentro de un solo túnel; este campo también debe ser entendido por el protocolo de tunelización; puede ser por ejemplo, una etiqueta MPLS.

Encapsulación del VC emulado: contiene la información acerca de la PDU de capa 2 encapsulada, la cual es necesaria para emular propiamente el protocolo de capa 2 correspondiente. Este tipo de encapsulación se denomina Palabra de Control.

Martini define las siguientes encapsulaciones sobre MPLS: FR, Ethernet, VLAN, ATM, PPP y HDLC. Además define un nuevo elemento VC FEC, para transportar información acerca del circuito virtual; y una Palabra de Control (ver figura 3.10), cuyas funciones incluyen la preservación de la secuencia de tramas, rellenar los paquetes pequeños para ser transmitidos en un medio donde la unidad de transporte mínima es más grande que el tamaño del paquete real y transportar los

bits de control de la cabecera original de la trama de capa 2. Puesto que no siempre es necesario para transportar el encapsulamiento de capa 2 por la red, un *router* en el ingreso puede quitar la cabecera original de capa 2 de una trama. El *router* de salida usa la Palabra de Control para reproducir la cabecera de capa 2 de la trama. Para algunos protocolos esta palabra es requerida, y para otros es optativa.

Rsvd	Bandera	0	0	Longitud	Número de Secuencia

Figura 3.10: Palabra de control [4]

En todos los casos el *router* de salida debe ser consciente de sí el *router* de ingreso enviará una palabra de control sobre un circuito virtual específico. La palabra de control se define como sigue:

En la figura 3.10, el primer campo es reservado para uso futuro, éste debe ponerse a 0 al transmitir, y debe ignorarse en el lado de recepción. La palabra de control transporta bits de bandera variable que dependen del encapsulamiento. El campo de longitud se requiere al rellenar las tramas pequeñas en enlaces que tienen un tamaño de trama mínimo. El campo de número de secuencia es optativo. Se usa para descubrir entregas defectuosas de tramas.

3.4.2.2.2 Transporte del paquete en una Martini L2 VPN

En una red MPLS, es posible transportar las PDUs de los protocolos de capa 2 usando una pila de etiquetas MPLS. Si se desea transportar las PDUs de capa 2 de un LSR de ingreso (PE1) a un LSR de salida (PE2), por una red MPLS y se asume que hay un LSP de PE1 a PE2, entonces se asume que ese PE1 puede hacer que un paquete sea entregado a PE2 colocando alguna etiqueta en el paquete. A esta etiqueta se la denomina etiqueta del túnel, y al LSP correspondiente el túnel LSP (ver figura 3.11).

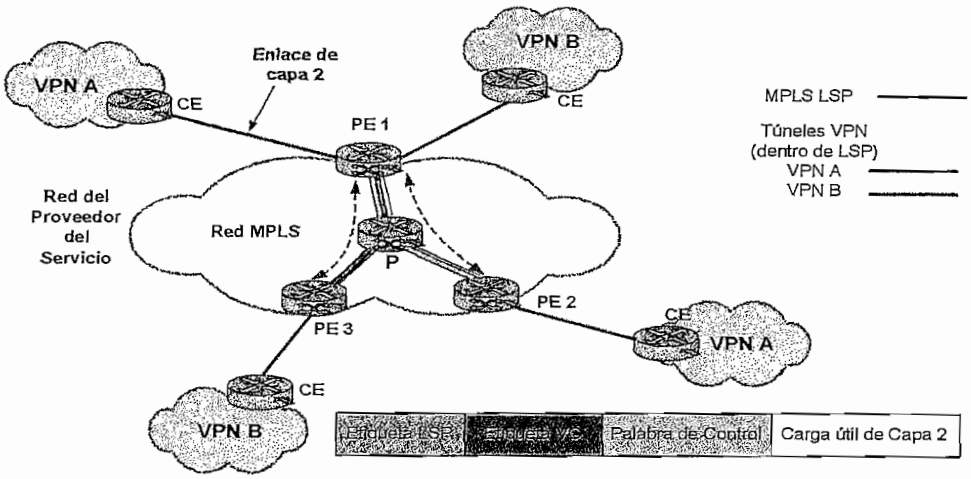


Figura 3.11: VPN de capa 2 basada en MPLS (Martini)

El túnel LSP envía meramente los paquetes de PE1 a PE2, la etiqueta correspondiente no le dice a PE2 qué hacer con el paquete. Así si la carga útil (*payload*) no es un paquete IP, debe haber una etiqueta, que sea visible a PE2, que le diga a PE2 cómo tratar el paquete recibido. A esta etiqueta se la denomina etiqueta del circuito virtual (VC).

Figura 3.12: Etiqueta del túnel y etiqueta del circuito virtual

En la figura 3.12, se nota que la etiqueta del VC se encuentra en el fondo de la pila de etiquetas, y la etiqueta del túnel, está inmediatamente anterior a la etiqueta del VC. Así cuando PE1 envía un PDU de capa 2 a PE 2, coloca una etiqueta del VC primero en su pila de etiquetas, y entonces coloca una etiqueta del túnel. La etiqueta del túnel pasa el paquete MPLS de PE1 a PE2; la etiqueta del VC no es visible hasta que el paquete MPLS alcanza PE2.

La etiqueta del VC debe distribuirse de PE2 a PE1 usando LDP en el modo *downstream* No solicitado; esto requiere que una sesión de LDP se cree entre PE1 y PE2. Los LSRs establecerán una sesión LDP que usa el mecanismo de Descubrimiento Extendido, para este propósito se define un nuevo tipo de elemento de FEC. Además, al usar LDP para distribuir la etiqueta del VC, se debe

usar el modo de retención de etiquetas liberal. Sin embargo, la operación de petición de etiqueta (*label request*), principalmente usado por el modo de retención de etiqueta conservativo, debe llevarse a cabo. Deben asignarse las etiquetas del VC del espacio de etiqueta (*label space*) por plataforma.

Resumiendo, el *draft* de Martini usa la pila de etiquetas MPLS para transportar etiquetas VC y etiquetas del túnel. La etiqueta VC identifica la VPN o conexión al punto terminal, mientras la etiqueta del túnel determina el camino que un paquete toma a través de la red. Los LSRs en el núcleo de una red usan la etiqueta del túnel para reenviar el paquete, y el LSR de salida usa la etiqueta VC para determinar cómo procesar la trama, ver figura 3.13.

Figura 3.13: Pila de etiquetas en una red MPLS (Martini)

Como fue anotado anteriormente, los grupos PPVPN y PWE3 del IETF definen las normas para las L2 VPNs. Hablando en términos generales, el grupo de PPVPN se enfoca en especificar las tecnologías de VPN multipunto que los proveedores de servicio pueden proveer para clientes empresariales. En contraste, el grupo PWE3[6] se enfoca en definir las tecnologías para enlaces punto a punto que se extiende de borde a borde en una red de un proveedor conocidas como tecnología *pseudo wire* (PW). Estas tecnologías dan la posibilidad de interconectar dos nodos con cualquier tecnología de capa 2.

3.4.2.3 Kompella L2 VPN [6]

Este modelo, combina autodescubrimiento de los sitios de la VPN con la señalización del campo demultiplexor para los PVCs de la L2VPN. Esto es

[6] El *draft* Martini precedió al grupo PWE3. Martini, espera publicar las características importantes de sus *drafts* en un futuro cercano como RFCs experimentales, para reflejar su aplicación real en el mercado. Además, los *drafts* Martini están sirviendo como punto de partida para nuevas extensiones.

posible porque el mecanismo usado para el autodescubrimiento (BGP) también es capaz de distribuir información de capa 2 así como el campo demultiplexor. Se introduce tres nuevos términos:

Etiqueta VPN: el campo demultiplexor que identifica un PVC de la L2 VPN en el borde de la red del SP.

Túnel: túnel que tiene sus extremos en los *routers* PE y es usado para transportar múltiples tipos de datos. Los *routers* P en el núcleo del SP envían estos datos basados en la cabecera del túnel.

Identificador del CE: constituye un número que únicamente identifica un dispositivo CE dentro de una L2 VPN. Más correctamente, el ID del CE identifica una conexión física del dispositivo CE al *router* PE. Por ejemplo, un dispositivo CE conectado a un PE sobre una línea DS-3 (44.736 Mbps) para un acceso Frame Relay; dicha DS-3 necesitaría un identificador CE. El CE también tendría N DLCIs sobre esta línea DS-3 para comunicarse con otros N sitios en la VPN.

3.4.2.3.1 Transporte del paquete en una Kompella L2 VPN

Cuando el paquete llega al dispositivo PE desde un dispositivo CE en una VPN de capa 2, la dirección de capa 2 del paquete identifica el CE al cual está destinado el paquete. Este procedimiento instala una ruta que asigna la dirección de capa 2 a un túnel (que identifica al PE al cual el CE destino está conectado) y a una etiqueta VPN (que identifica al CE destino). El paquete puede entonces ser modificado (dependiendo de la encapsulación de capa 2).

El tamaño de la MTU[7] de enlace de capa 2 debe ser escogido acorde al formato de las tramas más la cabecera de la L2 VPN, de tal forma que no exceda el MTU de la red. Las tramas de capa 2 que excedan el MTU después de la encapsulación serán desechadas.

[7] MTU: La MTU de una red es la mayor cantidad de datos que puede transportar su trama física. La MTU de las redes Ethernet es 1500 bytes y el de las redes Token Ring, 8192 bytes. Esto significa que una red Ethernet nunca podrá transportar un datagrama de más de 1500 bytes sin fragmentarlo.

3.4.2.3.2 Formato de la trama

La modificación a la trama de capa 2 depende del tipo de capa 2. Este enfoque requiere que los métodos de encapsulación usados en el transporte de tramas de capa 2 sobre los túneles sea el mismo que se describe en la referencia [4].

3.4.2.3.3 Señalización en las VPNs MPLS de Capa 2

BGP versión 4, se usa para el autodescubrimiento y protocolo de señalización para las VPNs de capa 2. Las extensiones Multiprotocolo (MP-BGP) se usan para transportar información de señalización L2 VPN. MP-BGP define el formato de dos atributos BGP, que pueden ser usados para anunciar y retirar la información de accesibilidad. Los proveedores configuran las VPNs con un atributo de BGP, la comunidad *Route Target*. Con BGP, los *routers* PE pueden aprender el número de miembros de la VPN, liberando a los proveedores de proporcionar toda la información a cada *router*. Los proveedores deben primero configurar los *routers* PE con una lista de los *routers* CE conectados localmente en cada VPN, la comunidad *Route Target* específica, y la interfaz física sobre la cual los clientes se conectan al *router* PE.

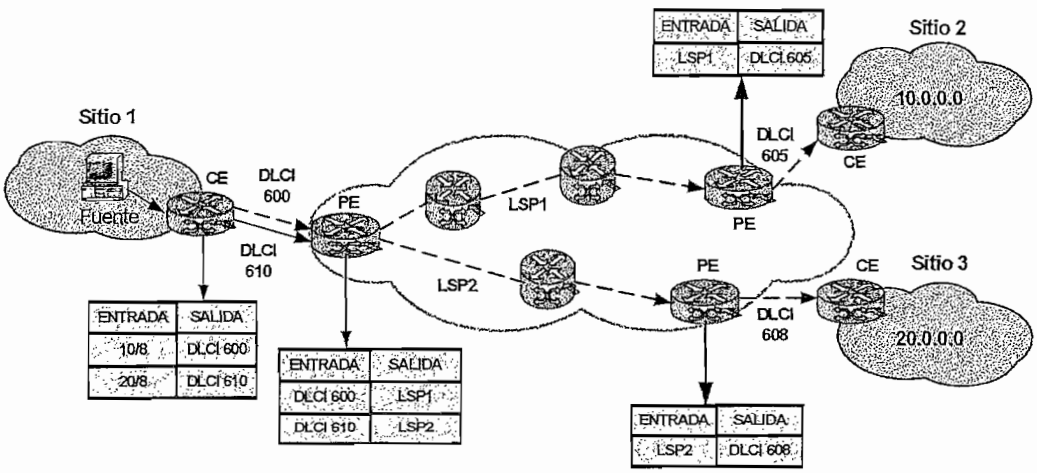


Figura 3.14: VPN de capa 2 basada en MPLS (Kompella) [10]

La figura 3.14 representa un ejemplo de una VPN de capa 2 basada en MPLS. La conexión entre los dispositivos CE de dos clientes está compuesta de tres segmentos: dos circuitos virtuales CE-PE "conectados" y un circuito virtual

emulado en el núcleo. Las tablas de enrutamiento del *router* fuente CE y los *routers* PE de ingreso y salida se indican en la figura. Básicamente, el primer *router* CE envía el tráfico por los DLCIs 600 y 610 a los sitios B y C respectivamente, como en una red FR normal, mientras que los *routers* PE de ingreso y salida realizan la asignación entre los DLCIs y los apropiados LSPs.

Debe notarse que las VPNs MPLS de capa 2 hacen que el suministro del servicio de VPNs sea mucho más fácil comparado con las VPNs convencionales de capa 2. En particular, si se añade un nuevo sitio a una VPN existente simplemente se requiere configurar el *router* PE que conecta al nuevo sitio, y no la reconfiguración de un alto número de dispositivos CEs.

Recientemente, el grupo PPVPN del IETF ha reutilizado el concepto de VPLS (*Virtual Private LAN Service*, siguiendo un término definido originalmente en el RFC 2764) como un servicio de capa 2 porque emula una LAN a través de una WAN [4]. El propósito básico de un VPLS es ofrecer conectividad de capa 2 a los múltiples sitios del cliente de una manera transparente a los dispositivos CE. El SP es responsable por transportar tramas de capa 2 del cliente y de conmutarlas a través de la red del SP entre los sitios del cliente. Desde el punto de vista del cliente, el servicio es equivalente a conectar los dispositivos CE mediante un conmutador (*switch*), es decir, todos en el mismo dominio *broadcast*/segmento LAN. En base a este concepto, una VPN de capa 2 puede ser ahora una de dos posibles variantes:

VPLS (*Virtual Private LAN Service*), es un SP que emula una LAN tradicional. Una VPLS hace posible interconectar varios segmentos LAN sobre una red conmutada de paquetes (PSN) y hace que los segmentos LAN remotos se comporten como una sola LAN. Por lo tanto tiene todas las características de escalabilidad de una LAN; los problemas podrían surgir en el número de puntos terminales que pueden ser soportados en un PE particular.

VPWS (*Virtual Private Wire Service*), corresponde a un servicio de VPN que proporciona un servicio de capa 2 punto a punto, conectando dos dispositivos

localizados en el borde del cliente. El CE en la red del cliente se conecta a un PE en la red del proveedor mediante un circuito; el circuito puede ser un circuito físico o un circuito lógico. Los problemas podrían aparecer en el número de puntos terminales que pueden ser soportados en un PE particular. Una VPWS difiere de una VPLS en que la VPLS es punto a multipunto, mientras la VPWS es punto a punto.

Además se incluye una tercera categoría:

IPLS *(IP-only LAN-like Service)*, IPLS es muy parecido a VPLS, excepto que se asume que los dispositivos CE son *hosts* o *routers*, y no *switches* y que el servicio solo transportará paquetes IP, y soporta paquetes tales como ICMP y ARP[8]; paquetes de capa 2 que no contengan IP no se soportan. Mientras este servicio es un subconjunto funcional de VPLS, éste es considerado separadamente, porque es posible proveer de IPLS, usando diferentes mecanismos, y además permite correr en diferentes plataformas de *hardware* que no soportan la completa funcionalidad de VPLS.

3.4.2.3.4 Diferencia entre los drafts de Kompella y Martini

Martini y Kompella tienen mucho en común en cuanto al formato del paquete y su habilidad para conectar clientes mediante el empleo de protocolos de capa 2 incluyendo FR, ATM, Ethernet y líneas arrendadas. Sus respectivas fortalezas y debilidades radican esencialmente en el empleo de: BGP, en el caso de Kompella, o LDP en el caso de Martini, para distribuir la información de la VPN.

El *draft* de Kompella podría argumentar que para configurar una red con el *draft* de Martini es más complicado por dos aspectos. Primero, el *draft* de Martini carece de un esquema de distribución para propagar la información a través de la red, demandando a los proveedores de servicio proveer ambos extremos del circuito. Las redes según Martini solamente soportan circuitos punto a punto, requiriendo de los proveedores configurar más circuitos en una red *full mesh*, de

[8] ARP (*Address Resolution Protocol*): Protocolo que realiza la conversión entre direcciones IP y direcciones físicas.

lo que requeriría hacerlo con Kompella. Kompella permite circuitos punto a multipunto y punto a punto.

Sin embargo, el *draft* de Martini señala que hay una pequeña diferencia en proveer sistemas que automatizarán el establecimiento del circuito bajo cualquier *draft*. Y con respecto al uso de circuitos punto a multipunto, puede ser una ventaja a medias. Hay que destacar que los *carriers* típicamente quieren redes parcialmente malladas y el establecimiento de *carriers* bajo Kompella, es muy complicado porque se necesita de *routers* PE que filtren los mensajes BGP.

Kompella indica que los problemas de las VPNs bajo su modelo son más simples que los que se tiene en Martini. Configurando ambos extremos, los enlaces introducen una complejidad operacional adicional en la red, especialmente si se necesita una red completamente mallada. Por ejemplo, una VPN con 40 sitios, en el *draft* de Martini requeriría 1600 configuraciones mientras que en Kompella se requeriría 40 configuraciones.

Martini indica que el número de tales configuraciones son irrelevantes porque esto solamente afecta al tiempo de actualización del *router*. Aún cuando se necesita identificar individualmente la configuración de la línea, muchos proveedores ofrecen herramientas que permiten un rápido vistazo a los puntos de configuración, dejando el número de configuraciones irrelevantes.

Finalmente, el *draft* Kompella usa BGP como un medio de habilitación para que una VPN pueda trabajar en ambientes ASs. Martini usa LDP, e indica que sí se puede trabajar entre ASs, las compañías escogen a LDP porque éste ofrece mejor protección para el tráfico de Internet contra los ataques en infraestructuras de capa 2 y además porque LDP reduce a la larga el tiempo de convergencia inherente en BGP.

3.4.3 MODELO DE CAPA 3 VERSUS MODELO DE CAPA 2

Las VPNs de capa 3 y capa 2 tienen puntos fuertes y débiles. En esta sección, se presenta un breve resumen de las ventajas y desventajas de cada modelo. Las

VPNs basadas en MPLS de capa 3 tienen varias ventajas cuando se comparan con las VPNs de capa 2:

- La VPNs de capa 3 son fáciles de configurar y proveer. La adición de un nuevo sitio a una VPN de capa 3 existente sólo requiere la configuración de los respectivos *routers* CE y PE. En contraste, en una VPN de capa 2 completamente mallada con n sitios, se deben configurar n – 1 conexiones en cada CE.
- En una VPN de capa 3, un *router* CE tiene un solo vecino, el *router* PE, y solo necesita mantener una sola adyacencia[9] de enrutamiento. En contraste, en una VPN de capa 2 con n sitios, cada *router* CE debe tener n vecinos de enrutamiento.
- En las VPNs de capa 3, el cliente es responsable por el enrutamiento solo dentro de cada sitio. En las VPNs de capa 2, el cliente tiene que construir y operar la red entera, lo que puede ser inapropiado para clientes con poca experiencia en enrutamiento.
- Las VPNs de capa 3 son totalmente independientes de las tecnologías de capa 2.
- Las VPNs de capa 3 pueden ocuparse de la QoS. Puesto que el *router* PE tiene visibilidad de la capa 3, puede realizar la clasificación de QoS y aplicar funciones DiffServ.

Las VPNs basadas en MPLS de capa 2 también tienen algunas ventajas cuando se comparan con las VPNs de capa 3:

- Debido a que las VPNs basadas en MPLS de capa 2 son funcionalmente equivalentes a las VPNs "tradicionales" de capa 2 (por ejemplo basadas en ATM o FR), el proceso de migración puede ser simple.
- Las VPNs de capa 2 garantizan privacidad de enrutamiento al cliente, ya que el proveedor de servicio no participa en el enrutamiento. Los *routers* del proveedor de servicio no necesitan hacer algo especial para guardar rutas del cliente separadas de otros clientes o del Internet.

---

[9] En una red, una adyacencia, está relacionada con dispositivos, nodos o dominios que están vinculados directamente a un enlace de datos o que comparten un control común.

- Las tablas de enrutamiento por VPN no son necesarias en los *routers* PE. La escalabilidad de las VPNs de capa 2 depende del número de sitios de la VPN pero no del número de rutas del cliente. En contraste, en las VPNs de capa 3 cada CE puede tener un número arbitrario de rutas que necesitan ser aprendidas y transportadas por el proveedor de servicio. Para muchos críticos de las VPNs de capa 3, la escalabilidad del enrutamiento será un problema mayor en las grandes redes.
- En las VPNs de capa 2 hay una clara separación entre la responsabilidad del proveedor de servicio (conectividad de capa 2) y la responsabilidad del cliente (conectividad de capa 3, incluso el enrutamiento).
- Las VPNs de capa 2 proporcionan independencia de capa 3. Porque el proveedor de servicio simplemente proporciona conectividad de capa 2, el cliente puede ejecutar cualquier protocolo de capa 3. En contraste, en las VPNs de capa 3, el cliente y el proveedor de servicio deben usar el mismo protocolo o los mismos protocolos de capa 3 y protocolos de enrutamiento.
- En las VPNs de capa 2 los *routers* CE ejecutan enrutamiento *multicast* nativo directamente. El *backbone* del proveedor de servicio simplemente proporciona interconexión de los *routers* CE; si los *routers* CE ejecutan *unicast* IP o *multicast* IP o algún otro protocolo de red es irrelevante a los *routers* del proveedor de servicio.

En la tabla 3.1, se muestra un resumen de las tecnologías anteriormente señaladas.

	VPN BGP/MPLS	Martini L2 VPN	Kompella L2 VPN
Basado en CE/PE	Basado PE	Basado PE	Basado PE
Capa	Capa 3	Capa 2	Capa 2
Modelo *Overlay / Peer*	*Peer*	*Overlay*	*Overlay*
Túnel	MPLS	MPLS	MPLS
Descubrimiento	BGP	LDP	BGP
Establecimiento del túnel	LDP/RSVP	LDP/RSVP	LDP/RSVP
Enrutamiento VPN	BGP	No Aplicable	No Aplicable

Tabla 3.1: Tecnologías usadas en las VPNs MPLS

3.5 CALIDAD DE SERVICIO EN REDES PRIVADAS VIRTUALES [7], [8]

La calidad de servicio generalmente describe la convicción de un retardo suficientemente bajo o pérdida del paquete para ciertos tipos de aplicaciones o tráfico. Las redes corporativas tradicionales pudieron garantizar un nivel mixto de recursos disponibles en todas las condiciones usando los circuitos arrendados dedicados.

Las VPNs de capa 2 han utilizado tecnologías como ATM o FR durante algún tiempo y pueden proporcionar un desempeño comparable a las soluciones de líneas privadas. Igualmente, los proveedores de servicio de IP-VPNs esperan proporcionar el mismo tipo de soporte para la calidad de servicio.

Dos conceptos han sido ideados por el IETF como las arquitecturas de QoS en las redes basadas en IP: Servicios integrados (IntServ, *Integrated Services*) y Servicios Diferenciados (DiffServ, *Differentiated Services*). MPLS con ingeniería de tráfico y CR (*Constraint-based Routing*), también proveen nuevas herramientas para manejar y controlar la calidad de servicio.

3.5.1 SERVICIOS INTEGRADOS (IntServ)

Servicios Integrados (IntServ) es un estándar que propone una reservación de recursos para garantizar el flujo de datos con QoS. El nivel de QoS necesario es programable de acuerdo al requerimiento de las aplicaciones finales. El modelo IntServ especifica diferentes servicios. Un servicio se define como un conjunto coordinado de QoS requeridos, provistos por un solo elemento en la red. Únicamente dos servicios han sido especificados para uso con un protocolo de reservación:

- *Servicio garantizado*: Asegura un nivel dado de ancho de banda punto a punto, se garantiza que los retardos solamente se dan por factores como velocidad de propagación de las ondas o mecanismos de configuración

que no son controlados; el retardo entre paquetes no es controlado, sino minimizado.

- *Carga de servicio controlada:* Provee un flujo de datos para el cliente punto a punto. El retardo y pérdida de paquetes son controlados por el flujo de carga que tiene la red, pero a la larga no se controla el deterioro de la red a medida que el flujo se vuelve mayor.

Para proveer estos mecanismos de señalización de flujo, se usan protocolos como RSVP, debe notarse que éste no es un protocolo de enrutamiento, sino de reservación de recursos.

3.5.2 SERVICIOS DIFERENCIADOS (DiffServ) [7]

La arquitectura DiffServ, propone una arquitectura de servicios diferenciados basada en la discriminación del tráfico de una red en diferentes clases, dichas clases son tratadas de formas diferentes en los nodos de la red. La utilización de servicios diferenciados exige el establecimiento de un Acuerdo a nivel de servicio (SLA, *Service Level Agreement*). El SLA se establece entre el proveedor de servicios y el cliente antes de la utilización de los servicios diferenciados.

Un concepto clave en DiffServ, es el Comportamiento para cada salto (PHB, *Per Hop Behavior*). El PHB se usa para identificar el "tratamiento" que se dará al paquete dentro del nodo. Este "tratamiento" incluye la selección de la cola y fija la disciplina a aplicarse en la interfaz de salida y congestión en los umbrales. Un PHB puede ser especificado en términos de sus recursos: *Buffer*, ancho de banda; o de las características de tráfico: Retardo, variación del retardo (*jitter*).

El grupo de trabajo del IETF define el Campo DS (*Differentiated Services*) para IPv4 e IPv6 (RFC 2474). El *byte* DS reemplaza el *byte* ToS (*Type of Service*) en la cabecera IP. Los paquetes se marcan para identificar el tratamiento que los paquetes necesitan usando el byte DS. Dentro del byte DS, existe un campo denominado DSCP (*DiffServ CodePoint*). El *byte* DS contiene 6 bits para el DSCP, más 2 bits que no se usan actualmente y son reservados para el futuro. El

valor en este campo identifica el PHB a aplicar al paquete dentro de ese nodo en la red. Así un PHB es el medio por el cual el nodo asigna recursos a una colección de paquetes con un mismo DSCP. Esto permite 64 puntos de código (*codepoints*) independientes. Éstos se asignan en el nodo para determinar el "tratamiento" a aplicarse. Los PHBs definidos son:

- Envío acelerado (EF, *Expedited Forwarding*): El EF PHB proporciona una baja pérdida, bajo *jitter*, un bajo retardo dentro del nodo y ancho de banda asegurado. El EF PHB se asemeja a un enlace virtual arrendado. Tiene un solo valor de DiffServ (DSCP = 101110). EF PHB es descrito como un servicio *Premium*. El tráfico que excede esta política, es desechado.
- Envío asegurado (AF, *Assured Forwarding*): Los paquetes se agrupan en n grupos. Cada clase AF se puede asignar m niveles de precedencia de descarte (DP, *Drop Precedence*). Un paquete que pertenece a la clase i y tiene un DP j, debe ser marcado por un DSCP: AFij donde: $1 \leq i \leq n$; $1 \leq j \leq m$. Actualmente solo se han definido 4 clases AF PHB (n = 4) y 3 niveles DP (m = 3). Los valores asignados al DSCP para AF PHB son los indicados en la tabla 3.2:

Porcentaje de descarte	Clase 1	Clase 2	Clase 3	Clase 4
DP bajo	AF_{11}-001 010	AF_{21}-010 010	AF_{31}-011 010	AF_{41}-100 010
DP medio	AF_{12}-001 100	AF_{22}-010 100	AF_{32}-011 100	AF_{42}-100 100
DP alto	AF_{13}-001 110	AF_{23}-010 110	AF_{33}-011 110	AF_{43}-100 110

Tabla 3.2: Valores asignados al DSCP para AF PHB [10]

Para el grupo AF PHB se ha definido el servicio "olímpico":

Oro → AF3j Plata → AF2j Bronce → AF1j

- *Default Behavior* (DE): El DE PHB identifica la existencia de tráfico de mejor esfuerzo, "*best effort*" (DSCP = 000000). El comportamiento define que el nodo entregará tantos paquetes como sea posible, en cuanto sea posible.

Un dominio DiffServ es un conjunto de nodos (*routers*) dentro de una red que comparten una política común de PHB. En un dominio Diffserv existen dos tipos de nodos, los vecinos que conectan sus dominios a otros dominios y los nodos del interior. Los nodos vecinos tienen la tarea de clasificar el tráfico que llega en los diferentes flujos, los tipos de clasificaciones son: Agregación de comportamiento (BA, *Behavior Aggregate*) y Multicampo (MF, *Multifield*). Las BAs clasifican los paquetes basados en el análisis del campo DS. Los MF clasifican los paquetes basados en el análisis de varios campos de la cabecera IP, tales como dirección IP fuente y destino o puertos. Las reglas usadas para esta clasificación son especificadas por un acuerdo denominado Acuerdo de Acondicionamiento de Tráfico (TCA, *Traffic Conditioning Agreement*). Después de clasificar el tráfico se condiciona a las reglas dadas por el TCA.

3.5.3 SOPORTE DE MPLS A LOS SERVICIOS DIFERENCIADOS

Las arquitecturas IntServ y DiffServ pueden usarse para servicios de QoS en una red IP, pero necesitan algunas modificaciones para trabajar en una arquitectura MPLS debido al uso de etiquetas.

Las arquitecturas DiffServ y MPLS tienen algunas cosas en común. Ambos enfoques colocan la complejidad al borde de la red. MPLS y DiffServ etiquetan los paquetes después de clasificarlos. Éstos se llaman etiquetas MPLS en las redes MPLS y DSCPs en las redes DiffServ. El DSCP de un paquete determina la conducta de los nodos con respecto a los mecanismos de planificación y el manejo de la cola. Ellos típicamente definen la prioridad y la precedencia de descarte de los paquetes. La etiqueta MPLS de un paquete determina el camino que el paquete debe tomar. El paquete se envía basado en su etiqueta.

Por lo cual, es deseable combinar las características de MPLS y DiffServ [8] para lograr una buena QoS en la red. Combinando ambos mecanismos, es posible especificar los caminos que los paquetes toman y su comportamiento en las colas de diferentes *routers*. Para esto es necesario introducir conceptos relacionados con estas dos arquitecturas, los mismos que se detallan a continuación:

BA (*Behavior Aggregate*): El conjunto de todos los paquetes que tienen el mismo valor DSCP (y así ellos recibirán el mismo PHB).

OA (*Ordered Aggregate*): El conjunto de BAs que comparten un ordenamiento obligado, es decir el orden del conjunto de BAs debe mantenerse durante la transmisión. Esto significa que paquetes que pertenecen al mismo OA no deben ser reordenados.

PSC (PHB *Scheduling Class*): El conjunto de uno o varios PHBs que son aplicados a los BAs que pertenecen a un OA dado (conjunto de PHBs que usa la misma cola). Por ejemplo, AF1j es una PSC que comprende los PHBs: AF11, AF12 y AF13. EF es un ejemplo de PSC que comprende un solo PHB, el EF PHB. Un LSP puede asociarse con propiedades de calidad de servicio que necesitan ser implementadas por los mecanismos de QoS en los LSRs mediante otro medio no MPLS. El principal requerimiento para usar DiffServ en redes MPLS es asegurar que los paquetes consigan el tratamiento apropiado de QoS por cada LSR en la red. Sin embargo, puesto que el LSR por definición no inspecciona la cabecera IP, es necesario proporcionar la información DSCP a través de la cabecera de la etiqueta. Esto puede lograrse de dos maneras (ver figura 3.15):

a) **E-LSP (*EXP-Inferred-PSC LSP*):** Estos LSPs transportan múltiples OAs, para que el campo EXP de la etiqueta MPLS lleve al LSR, el PHB a ser aplicado al paquete (cubriendo información sobre PSC y su precedencia de descarte). La asignación del campo EXP al PHB para un E-LSP es explícitamente señalada en el establecimiento de la etiqueta o una asignación pre-configurada.

b) **L-LSP (*Label-Only-Inferred-PSC LSP*):** Estos LSPs solo transportan una única OA; con tales LSPs, el PSC está explícitamente señalado en el momento del establecimiento de la etiqueta, para que después del establecimiento de la etiqueta, el LSR pueda inferir exclusivamente del valor de la etiqueta el PSC a ser aplicado a un paquete etiquetado mientras que la precedencia de descarte del paquete se lleva en el campo EXP del paquete MPLS.

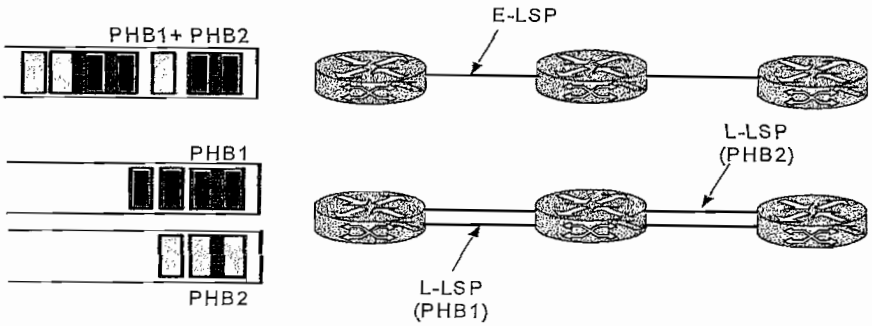


Figura 3.15: E-LSP y L-LSP [10]

El L-LSP supera el problema de tener un campo pequeño para codificar el DSCP; sin embargo impone requerimientos más altos en el sistema. En una red con tres diferentes PHBs el número de etiquetas necesarias se multiplica por tres. Habrá tres etiquetas diferentes que indican el mismo LSP pero con niveles de prioridad diferentes para el tráfico, manteniendo esa cantidad de etiquetas pueden volverse pronto un problema si el número de PHBs en el sistema se incrementa. Esto puede llevar a un problema severo de escalabilidad.

El E-LSP es simple, tales LSPs pueden transportar a ocho BAs de un FEC dado. Cuando más tráfico necesita ser acomodado, es necesario compartir la carga. Usando este esquema, los paquetes de cierto flujo de tráfico pueden pasar por diferentes caminos experimentando diferentes retrasos, esto causa el problema de reordenar el paquete. Por otro lado, L-LSP usa etiquetas separadas para el soporte de cada PSC (PHB *Scheduling Class*), por tanto introduce más operaciones de señalización y complejidad en el manejo de la etiqueta.

E-LSP y L-LSP pueden establecerse con o sin reservación de ancho de banda. Establecer un E-LSP o un L-LSP con reservación de ancho de banda quiere decir que los requerimientos de ancho de banda para el LSP son señalados en el momento del establecimiento del LSP. Tales requerimientos de ancho de banda señalados pueden usarse al momento del establecimiento por los LSRs para realizar el control de admisión que depende de los recursos DiffServ suministrados.

Existen varios protocolos disponibles para emprender la tarea de distribuir las etiquetas en un ambiente DiffServ-MPLS. Protocolos que ya están en uso en la red pueden ser empleados con información extra para realizar esta tarea, tales como: CR-LDP o RSVP-TE pueden usarse para establecer LSPs con recursos reservados. Otra solución es implementar un protocolo con la tarea específica de distribuir las etiquetas, como LDP.

3.5.4 DS-TE (*DIFFSERV-AWARE TRAFFIC ENGINEERING*)

La ingeniería de tráfico permite diseñar redes que utilizan total y eficazmente los enlaces de la red y los recursos de los elementos de la red para transportar el tráfico del cliente y prevenir puntos de congestión en el enrutamiento evitando que el desempeño de la red sea imprevisible.

Los mecanismos de DiffServ pueden trabajar paralelamente con mecanismos de ingeniería de tráfico de MPLS existentes en algunas redes, donde se requiera alguna optimización de los recursos de transmisión. Esta combinación da un nuevo aspecto al panorama de la QoS, como se presenta en la figura 3.16.

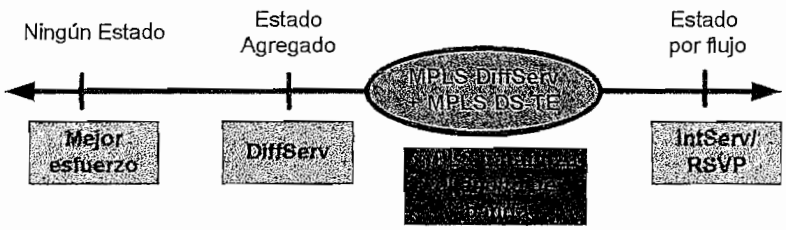


Figura 3.16: Panorama de la Calidad de Servicio [10]

DiffServ y MPLS TE proporcionan sus respectivos beneficios, es decir DiffServ realiza la diferenciación de servicio en cada salto y la ingeniería de tráfico logra una buena distribución de la carga de tráfico agregado por el conjunto de recursos de la red.

La ingeniería de tráfico MPLS (MPLS TE) permite un enrutamiento basado en restricciones (CR, *Constraint-based Routing*) del tráfico IP. Una de las

restricciones satisfechas por CR es la disponibilidad de ancho de banda requerida sobre un camino seleccionado.

Esta sección describe brevemente el trabajo que en la actualidad está "en progreso" en el grupo de trabajo de ingeniería de tráfico del IETF. El modelo DS-TE (*DiffServ-aware Traffic Engineering*)[9], a pesar de su estado pre-estándar, es un componente esencial en las redes MPLS, para poder brindar las capacidades de QoS.

La meta esencial de DS-TE es garantizar el ancho de banda separadamente para cada tipo de tráfico para mejorar y optimizar su complacencia con los requisitos de QoS. El modelo DS-TE, combina *DiffServ* e Ingeniería de tráfico en un esfuerzo por proporcionar garantías de servicio extremo a extremo dentro de una red MPLS.

DS-TE extiende MPLS TE para permitir la realización de un enrutamiento basado en restricciones del tráfico "garantizado". El ancho de banda más restrictivo es llamado: *sub-pool*, mientras el ancho de banda regular de un túnel TE es llamado: *global pool* (Un *sub-pool* es una porción del *global pool*). Esta habilidad de satisfacer un ancho de banda más restrictivo se traduce en la capacidad de lograr una calidad de servicio (QoS) más alta (en términos de retardo, *jitter* o pérdidas) para el tráfico garantizado.

DS-TE no solo permite la configuración de un *global pool* para la estimación del ancho de banda, también proporciona una configuración de un *sub-pool* restrictivo que puede usarse para el tráfico de alta prioridad de la red tal como voz u otras aplicaciones. El ancho de banda disponible en el *global pool* y en el *sub-pool* se anuncia por un IGP, asegurando que cada *router* guarde la pista del ancho de banda disponible al admitir nuevos LSPs para voz o tráfico de alta prioridad. DS-TE utiliza E-LSPs.

3.5.5 CALIDAD DE SERVICIO EN LAS VPNs MPLS [10]

Las VPNs tradicionales basadas en tecnologías de capa 2 o líneas arrendadas ofrecen una mínima garantía de nivel de calidad de servicio (QoS), expresados por parámetros tales como: CIR (*Commited Information Rate*), en el caso de FR; CBR (*Constant Bit Rate*) y SCR (*Sustained Cell Rate*), en el caso de ATM; o ancho de banda del circuito, en el caso de líneas arrendadas. De ahí que, en el caso de los clientes de las VPNs MPLS, deben esperar garantías de QoS similares.

Existen dos modelos básicos en el control de la calidad de servicio (QoS) en las VPNs MPLS: el modelo *pipe* y el modelo *hose*.

El modelo *hose* está basado en dos parámetros definidos por cada interfaz CE/PE, el ICR (*Ingress Committed Rate*) y ECR (*Egress Committed Rate*). Estos dos parámetros especifican el tráfico que cada *router* CE es capaz de transmitir/recibir a/desde otros sitios de la VPN.

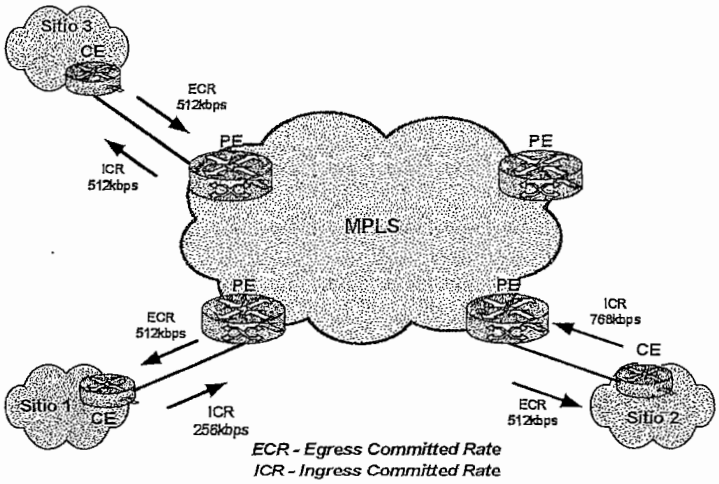


Figura 3.17: Modelo Hose [10]

En la figura 3.17, se muestra un ejemplo del "modelo *hose*". En este caso, el *router* CE conectado al sitio 1 es capaz de recibir información a 512 kbps de otros sitios de la misma VPN, y transmite a 256 kbps. Debe notarse que estos valores no son dependientes en la distribución de tráfico entre los sitios remotos, por

ejemplo, al sitio 1 se le permite enviar a 256 kbps al sitio 2 en un intervalo de tiempo específico, con tal de que no envíe tráfico al sitio 3 en el mismo intervalo.

El control de la calidad de servicio en el núcleo de la red MPLS puede realizarse por medio de DiffServ, ver la sección 3.5.3. En este caso, el modelo *hose* puede aplicarse separadamente para cada clase de servicio. Desde el punto de vista del cliente, una ventaja del modelo *hose* es que no requiere un conocimiento detallado de la distribución de tráfico entre los sitios de la VPN, lo cual hace que la implementación sea simple. Este modelo también se denomina modelo punto a nube.

La alternativa al modelo *hose* es el modelo *pipe*. Consiste en proporcionar garantías de QoS, por ejemplo un mínimo ancho de banda, entre cada par de *routers* CE. Se pueden usar LSPs con ancho de banda garantizado entre PEs para soportar el modelo *pipe*. Un LSP con ancho de banda garantizado puede ser establecido para cada par de CEs pero, por razones de escalabilidad, un solo LSP debería ser usado para soportar múltiples conductos CE-CE.

El modelo *pipe* hereda el enfoque básico de QoS usado en VPNs tradicionales basadas en ATM o FR (aparte del hecho de que el modelo *pipe* es unidireccional, considerando que en ATM o FR la conexión normalmente se define como bidireccional).

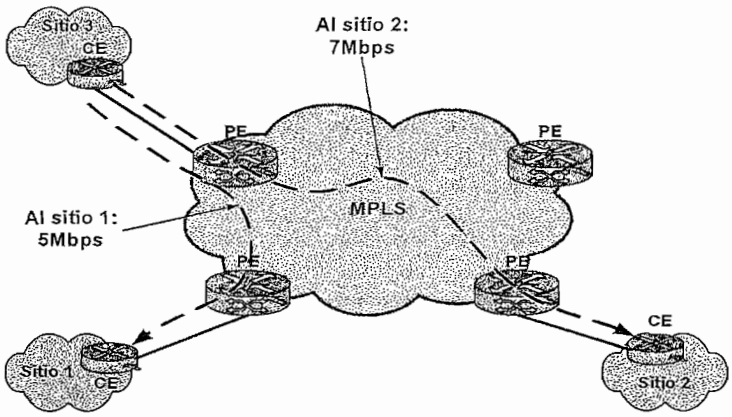


Figura 3.18: Modelo Pipe [10]

En el ejemplo mostrado en la figura 3.18, las dos conexiones sitio 3 - sitio 1 y sitio 3 - sitio 2 proporcionan 5 Mbps y 7 Mbps, respectivamente. De nuevo, el modelo *pipe* puede aplicarse a varias clases de servicio, posiblemente usando mecanismos de DS-TE, ver la sección 3.5.4.

Para la migración de una VPN MPLS de un cliente desde una VPN basada en ATM o FR, el modelo *pipe* es probablemente el enfoque más fácil ya que éste emula el mismo tipo de control de QoS. Una desventaja de este modelo es la necesidad de especificar un ancho de banda específico para cada par de sitios de la VPN, lo cual requiere de un conocimiento detallado del tráfico de la VPN matriz. Este modelo también se denomina modelo punto a punto.

Por supuesto, no hay una sola solución que encaje en todos los requerimientos. En la práctica, implementaciones combinadas de ambos modelos pueden ser la solución más apropiada.

BIBLIOGRAFÍA – CAPÍTULO 3

[1] CALLON R. y Otros, "*A Framework for Layer 3 Provider Provisioned Virtual Private Networks*", IETF draft, draft-ietf-ppvpn-framework-07.txt, Enero 2003 (trabajo en progreso).

[2] FERGUSON P., HUSTON G., "*What is a VPN?*", http://www.cisco.com.

[3] ROSEN E. y Otros, "BGP/MPLS VPNs", IETF draft, draft-ietf-ppvpn-rfc2547bis-03.txt, Octubre 2002 (trabajo en progreso).

[4] MARTINI L. y Otros, "*Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*", IETF draft, draft-martini-l2circuit-encap-mpls-05.txt, Abril 2003 (trabajo en progreso).

[5] MARTINI L. y Otros, "*Transport of Layer 2 Frames Over MPLS*", IETF draft, draft-martini-l2circuit-trans-mpls-11.txt, Abril 2003 (trabajo en progreso).

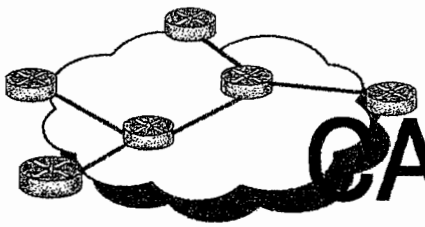
[6] KOMPELLA K. y Otros, "*Layer 2 VPNs Over Tunnels*", IETF draft, draft-kompella-ppvpn-l2vpn-02.txt, Noviembre 2001 (trabajo en progreso).

[7] BLAKE S. y Otros, "*An Architecture for Differentiated Services*", RFC 2475, Diciembre 1998.

[8] LE FAUCHEUR F. y Otros, "*MPLS Support for Differentiated Services*", RFC 3270, Mayo 2002.

[9] LE FAUCHEUR F. y Otros, "*Requirements for support of DiffServ-aware MPLS Traffic Engineering*", IETF draft, draft-ietf-tewg-diff-te-reqts-06.txt, Septiembre 2002 (trabajo en progreso).

[10] OJA Jari y Otros, "*IP Virtual Private*", http://www.eurescom.de.



CAPÍTULO 4

DISEÑO DE REDES PRIVADAS VIRTUALES CLÁSICAS

4.1 INTRODUCCIÓN

Las redes privadas virtuales VPNs (*Virtual Private Networks*) ofrecen una buena alternativa de interconexión ya que permiten que usuarios remotos accedan a redes corporativas para realizar diferentes tareas, tal como si se encontraran conectados directamente a la red LAN de la compañía, mediante el uso de una red pública, como medio de transporte de datos.

El propósito de este capítulo es el diseño de VPNs clásicas, para lo cual el modelo a desarrollarse responde al de las VPNs basadas en dispositivos CE (*Customer Edge*), cuyo modelo de referencia se presenta en la figura 4.1, para mayores detalles de dicho modelo, ver la sección 3.2; en la cual se utilizará la tecnología de *tunneling* IPSec. A este tipo de VPNs en el presente trabajo se las denomina como: "*VPNs clásicas*".

En la figura 4.1, el dispositivo CE proporciona la conectividad IP a los sitios de una determinada empresa. Para el presente proyecto, el dispositivo CE es un *router* y actuará como un *Gateway* de seguridad. El dispositivo CE está localizado en el borde de un sitio de una red empresarial.

La red de acceso proporciona las conexiones de acceso entre los dispositivos CE y un *router* PE (*Provider Edge*). Puede ser una red de capa 2 (por ejemplo: Frame Relay, ATM y Ethernet) o una red IP. En el contexto de las VPNs basadas en dispositivos CE, el dispositivo CE y el dispositivo PE tienen una conectividad de capa 3 sobre la conexión de acceso.

En el contexto de las VPNs basadas en dispositivos CE, el túnel VPN es un túnel IP (en este proyecto se usará el protocolo IPSec) entre dos dispositivos CE sobre la red pública.

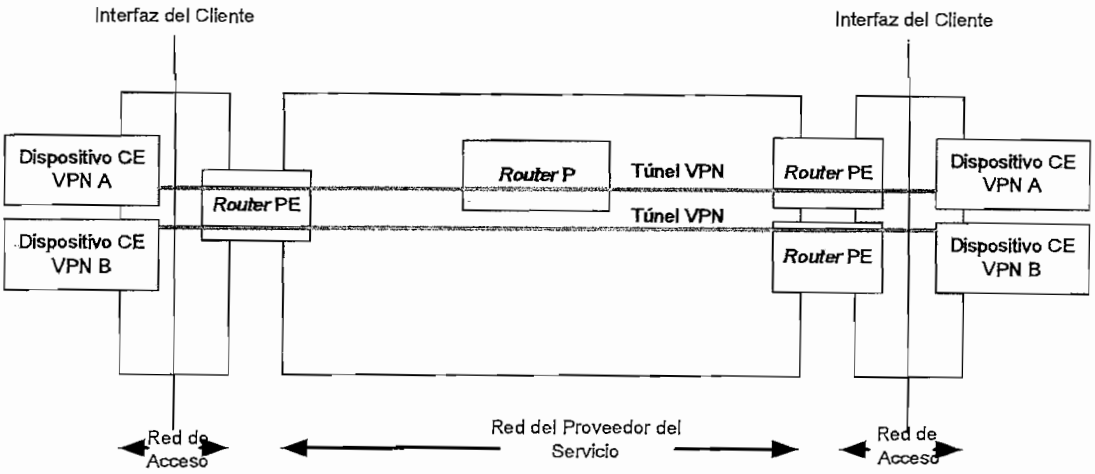


Figura 4.1: Modelo de referencia para las VPNs basadas en dispositivos CE [1]

4.2 DISEÑO DE LA VPN CLÁSICA

Previo al diseño de una VPN clásica, se debe considerar la infraestructura existente en el lado de la empresa tomada como referencia.

4.2.1 DESCRIPCIÓN ACTUAL DEL ESCENARIO

Por lo general, una red empresarial consta de una oficina central o matriz y las agencias o sucursales distribuidas en lugares geográficamente distantes. Para el presente proyecto, la empresa en referencia es una distribuidora de equipos de soldadura, la cual dispone de tres oficinas, la primera ubicada en el sector Norte de la ciudad de Quito (matriz), la segunda en el sector Sur de la Ciudad de Quito (primera sucursal), y la tercera ubicada en la ciudad de Guayaquil (segunda sucursal).

Es preciso indicar que actualmente, ni la matriz ni las sucursales se encuentran interconectadas entre sí, pero cada oficina cuenta con una conexión hacia Internet (ver la figura 4.2) principalmente para la búsqueda de información, y no para la transmisión de datos. Los dos enlaces en la ciudad de Quito son realizados por cable de cobre, por ser lo más económico, y el enlace de Guayaquil es realizado vía microonda. El enlace ofrecido por el ISP es un enlace *Frame Relay* (FR), ya que es una conexión eficaz y económica disponible en nuestro medio.

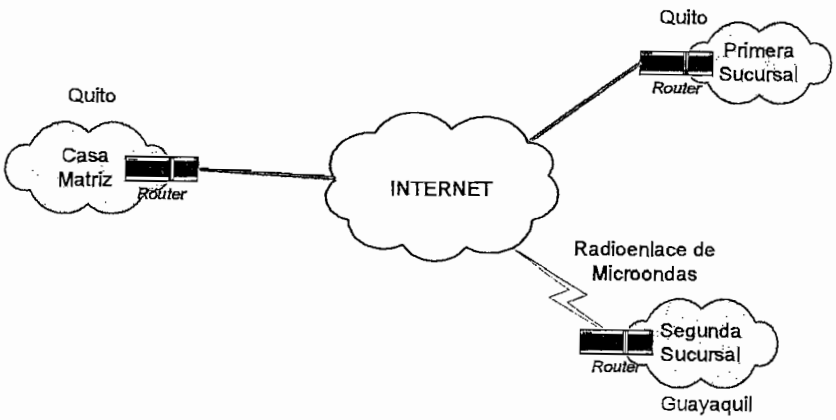


Figura 4.2: Esquema general de la red empresarial

Las aplicaciones que sirven a la empresa actualmente son:

- Correo Electrónico: Este servicio es dado a través de Internet y es de gran ayuda para la empresa porque permite mantener al tanto a todos los empleados de cambios durante el día o informar sobre las características de los equipos nuevos que llegan.
- Base de Datos: Este es un servicio propio de la empresa, la cual requiere mantener un control sobre todo lo que compra o vende. Con este sistema cada fin de mes, se tiene que reunir la información correspondiente de todas las sucursales y la matriz a fin de procesarla y realizar un balance total.
- Internet: Para la empresa es importante el acceso a Internet ya que le permite estar al tanto de nuevos cambios y ofrecer sus productos.
- El servicio de voz es provisto por centrales telefónicas PBX conectadas a líneas *dial-up* provistas por Andinatel y Pacifictel, respectivamente.

4.2.1.1 Matriz

La oficina matriz cuenta con:

- 25 empleados cada uno de ellos posee un computador, conectado a una red LAN de 100 Mbps.
- Un *router* 1750 de la marca Cisco.

- Un *switch* 3Com de 48 puertos
- Un servidor de correo.
- Un servidor de base de datos.
- Central Ericsson de 16 troncales con una capacidad de 48 extensiones de las cuales solo están usadas 24 extensiones.

Los servicios implementados para todos los empleados de la oficina matriz, son:

- Correo electrónico.
- Internet.
- El servicio de base de datos que tiene información relacionada con los equipos en *stock* y su precio, la maneja un número determinado de usuarios del área de contabilidad y bodega[1].

El enlace a Internet es suministrado por un ISP, a través de un enlace de cobre, desde un nodo de conmutación hasta el cliente. Actualmente el enlace de datos contratado al ISP es de 128 kbps, dicho canal es empleado para: correo electrónico e Internet.

El servicio de voz es proporcionado por la empresa telefónica Andinatel, a través de líneas convencionales hacia la central telefónica en el cliente.

4.2.1.2 Primera Sucursal

La Primera Sucursal de esta empresa, cuenta con:

- *15 usuarios* conectados a una red LAN de 100 Mbps.
- Un *router* 1601 de la marca Cisco.
- Un *switch* 3Com de 24 puertos.
- Un servidor de correo.
- Un servidor de base de datos.

[1] Actualmente la base de datos maneja el stock de equipos solo de este sitio, y al final de cada mes se actualiza con la información de las dos sucursales.

- Central Siemens de 15 troncales con una capacidad de 30 extensiones de las cuales solo están usadas 12 extensiones.

Los servicios implementados para todos los empleados de la sucursal, son:

- Correo electrónico.
- Internet.
- El servicio de base de datos es para un número determinado de usuarios de contabilidad y bodega.

El enlace a Internet es suministrado por un ISP, a través de un enlace de cobre, desde un nodo de conmutación hasta el cliente. Actualmente el enlace de datos contratado al ISP es de 64 kbps, dicho canal es empleado para: correo electrónico e Internet.

El servicio de voz es proporcionado por la empresa telefónica Andinatel, a través de líneas convencionales hacia la central telefónica en el cliente.

4.2.1.3 Segunda Sucursal

La Segunda sucursal es más pequeña y cuenta con:

- 10 usuarios conectados a una red de 100 Mbps
- Un *router* 1601 de la marca Cisco.
- Un *switch* de 12 puertos (fabricante desconocido);
- Un servidor de correo.
- Un servidor de base de datos.
- Central de 15 troncales con una capacidad de 30 extensiones de las cuales solo están usadas 9 extensiones.

Los servicios con los que cuenta la sucursal son:

- Correo electrónico.

- Internet.
- El servicio de base de datos está definido para un número limitado de usuarios.

El enlace que tiene el cliente hacia el ISP es de 64 kbps y es realizado mediante microonda a través de radios DMC de 23 GHz.

El servicio de voz es proporcionado por la empresa telefónica Pacifictel, a través de líneas convencionales hacia la central telefónica en el cliente.

4.2.2 CARACTERÍSTICAS DE DISEÑO PARA LA VPN CLÁSICA

Los requerimientos de la empresa son conectar, a través de Internet, la matriz con sus sucursales, lo que permitiría disponer de una base de datos actualizada del equipo en stock para todas las oficinas, sin necesidad de un enlace de datos adicional.

La base de datos distribuida (base de datos residente en cada servidor de cada oficina), es un programa que funciona en ambiente Windows, denominado SAP (*Systems, Applications, Products in Data Processing)* versión 3.1H.

Para esto se requiere realizar una *Intranet* corporativa, con este propósito se implementará una VPN.

Así las características del nuevo escenario son:

- El tráfico entre las oficinas sucursales de Quito y Guayaquil (a las que se denominará sitio 2 y sitio 3 respectivamente) y la oficina central (sitio 1), debe protegerse[2]. En la tabla 4.1, se muestra la definición de los sitios de la VPN de diseño.

[2] El tráfico debe protegerse ya que viajará sobre una red pública, en este caso Internet.

Nombre del sitio de la VPN	Definición del sitio de la VPN
Sitio 1	Sitio de la Matriz.
Sitio 2	Sitio de la Primera Sucursal (Quito).
Sitio 3	Sitio de la Segunda Sucursal (Guayaquil).

Tabla 4.1: Definición de los sitios de la VPN de diseño

- El soporte de IPSec sólo se requerirá en los límites de la intranet, es decir en los *gateways* (*routers* CE) de la VPN. Y no habrá ningún protocolo de seguridad en cualquiera de los *switches* que están localizados en el interior de la Intranet o en el *backbone* de la red pública.
- Los *routers* CE situados en el perímetro de cada sucursal de la Intranet implementan las funciones básicas de un *firewall* (filtración de paquetes) y también el soporte de los protocolos de IPSec para construir túneles seguros y autentificados entre todos los *routers* que comprenden la VPN.
- Las direcciones IP son asignadas para el uso en la Intranet, de un espacio de direcciones privado. Solo las interfaces de los *gateways* que se unen al *backbone* de la red pública requerirán de direcciones IP públicas.

4.2.3 DETERMINACIÓN DE LA CAPACIDAD DEL CANAL

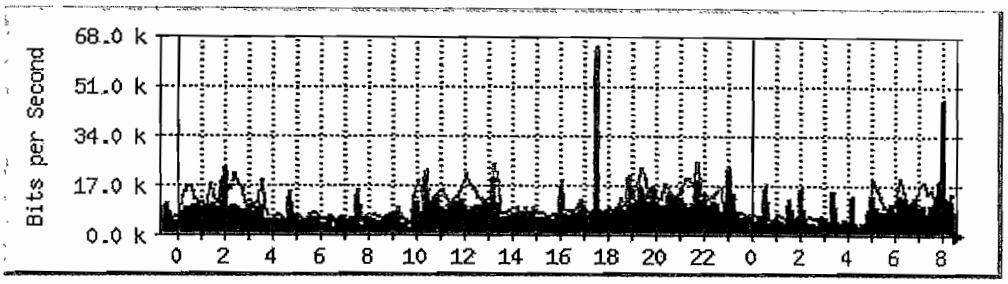
4.2.3.1 Análisis del tráfico de datos actual de la empresa

Para la determinación de la capacidad del canal se ha empleado la información actual del tráfico de datos, entregada por el programa MRTG (*Multi Router Traffic Grapher*). Esta información ha sido recopilada durante una semana laboral (5 días), para cada sucursal y la matriz.

a) Tráfico de datos actual de la Matriz

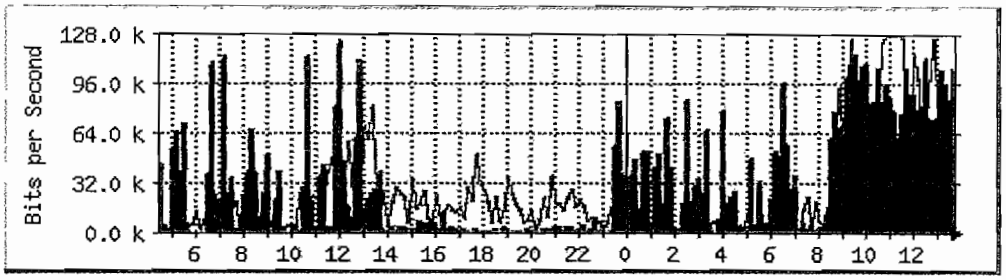
Para la determinación del tráfico en la matriz se han tomado muestras durante cinco días y en cada día durante la respectiva jornada laboral (8:00 am – 18:00 pm), esto es debido a que en esas horas se espera tener un intercambio de datos a través de la VPN. Aunque se puede observar que en horas no laborables existe

también tráfico, generalmente debido a que algunos usuarios bajan archivos o música en dichas horas. Los resultados correspondientes se presentan en las figuras 4.3 hasta la 4.7.



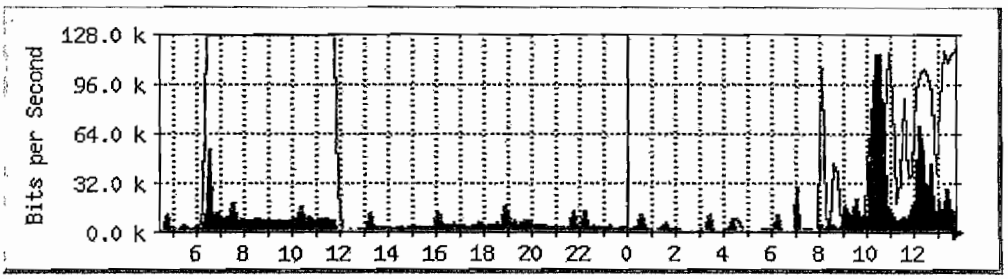
Máx Ent:64.8 kb/s (50.6%) Promedio Ent:9336.0 b/s (7.3%) Actual Ent:8512.0 b/s (6.7%)
Máx Sal:24.7 kb/s (19.3%) Promedio Sal: 10.7 kb/s (8.3%) Actual Sal:14.2 kb/s (11.1%)

Figura 4.3: Tráfico para el Lunes 17 de Mayo del 2004



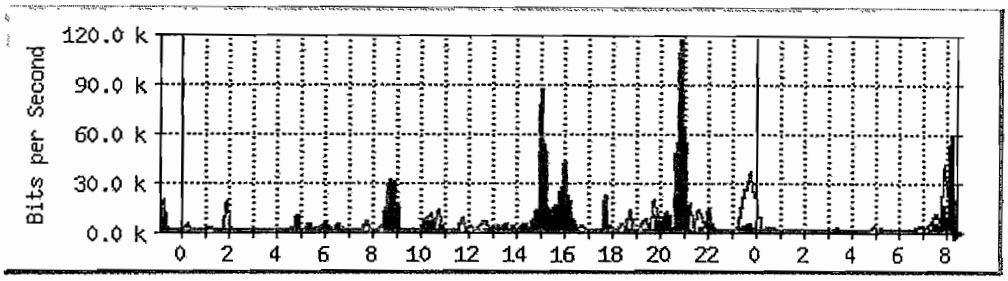
Máx Ent:123.2 kb/s (96.2%) Promedio Ent:32.5 kb/s (25.4%) Actual Ent:107.1 kb/s (83.7%)
Máx Sal:127.4 kb/s (99.5%) Promedio Sal:24.1 kb/s (18.9%) Actual Sal: 56.1 kb/s (43.9%)

Figura 4.4: Tráfico para el Martes 18 de Mayo del 2004



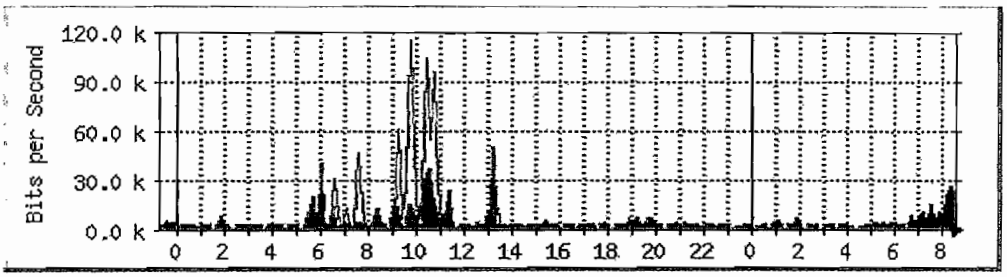
Máx Ent:116.4 kb/s (91.0%) Promedio Ent:8744.0 b/s (6.8%) Actual Ent: 14.2 kb/s (11.1%)
Máx Sal:127.9 kb/s (99.9%) Promedio Sal:33.2 kb/s (25.9%) Actual Sal:119.5 kb/s (93.4%)

Figura 4.5: Tráfico para el Miércoles 19 de Mayo del 2004



Máx Ent:118.5 kb/s (46.3%) Promedio Ent:5808.0 b/s (2.3%) Actual Ent:14.6 kb/s (5.7%)
Máx Sal: 41.0 kb/s (16.0%) Promedio Sal:4592.0 b/s (1.8%) Actual Sal:17.0 kb/s (6.7%)

Figura 4.6: Tráfico para el Jueves 20 de Mayo del 2004



Máx Ent: 51.2 kb/s (40.0%) Promedio Ent:5520.0 b/s (4.3%) Actual Ent:21.7 kb/s (16.9%)
Máx Sal:115.1 kb/s (89.9%) Promedio Sal:4832.0 b/s (3.8%) Actual Sal:9376.0 b/s (7.3%)

Figura 4.7: Tráfico para el Viernes 21 de Mayo del 2004

Para el cálculo de la capacidad del canal se tomará el tráfico de entrada y de salida durante la jornada laboral para luego calcular el tráfico promedio del día respectivo (ver la tabla 4.2 hasta la tabla 4.6).

Horas	Tráfico Entrante (kbps)	Tráfico Saliente (kbps)
8	6	8
9	8	9
10	10	18
11	9	15
12	10	19
13	9	10
14	7	7
15	9	9
16	17	18
17	9	9
18	10	10
Promedio	9.45	12

Tabla 4.2: Tráfico para el Lunes 17 de Mayo del 2004

Horas	Tráfico Entrante (kbps)	Tráfico Saliente (kbps)
8	22	9
9	48	13
10	3	6
11	6	22
12	125	34
13	16	22
14	3	6
15	3	6
16	10	19
17	6	16
18	3	29
Promedio	22.27	16.54

Tabla 4.3: Tráfico para el Martes 18 de Mayo del 2004

Horas	Tráfico Entrante (kbps)	Tráfico Saliente (kbps)
8	10	128
9	10	128
10	13	128
11	10	128
12	3	3
13	6	6
14	9	9
15	9	9
16	13	16
17	9	9
18	9	9
Promedio	9.18	52.10

Tabla 4.4: Tráfico para el Miércoles 19 de Mayo del 2004

Horas	Tráfico Entrante (kbps)	Tráfico Saliente (kbps)
8	3	6
9	18	6
10	3	6
11	6	6
12	3	9
13	6	6
14	6	6
15	87	16
16	46	31
17	6	6
18	3	6
Promedio	17	9.45

Tabla 4.5: Tráfico para el Jueves 20 de Mayo del 2004

Horas	Tráfico Entrante (kbps)	Tráfico Saliente (kbps)
8	6	3
9	15	6
10	12	3
11	6	3
12	6	3
13	12	6
14	15	3
15	6	3
16	4	3
17	8	3
18	6	3
Promedio	8.73	3.54

Tabla 4.6: Tráfico para el Viernes 21 de Mayo del 2004

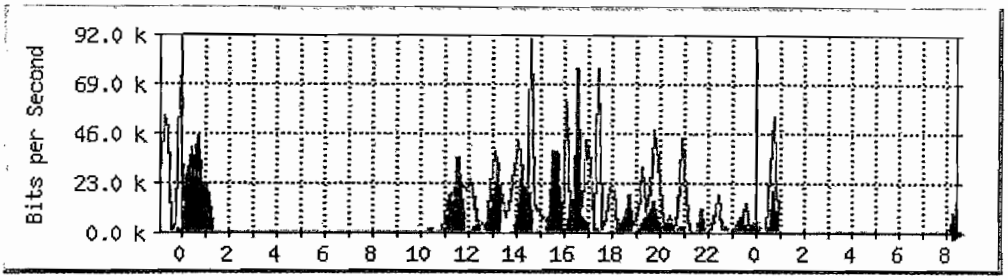
Día	Tráfico Entrante (kbps)	Tráfico Saliente (kbps)
17 de Mayo	9.45	12
18 de Mayo	22.27	16.54
19 de Mayo	9.18	52.10
20 de Mayo	17	9.45
21 de Mayo	8.73	3.54
Promedio	13.326	18.726

Tabla 4.7: Tráfico de datos promedio de la Matriz

Una vez que se tiene el promedio del tráfico entrante y saliente por separado, ver la tabla 4.7, se procede a sumar dichos valores para obtener el tráfico total (entrante + saliente) de datos actual para la matriz, el resultados es: 13.326 kbps + 18.726 kbps = 32.052 kbps.

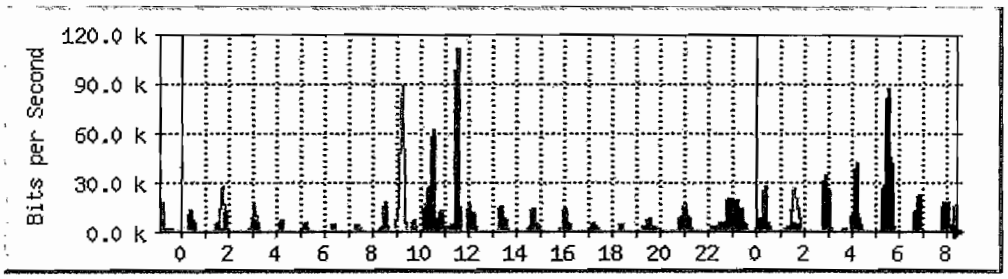
b) Tráfico de datos actual de la Primera Sucursal

Las estadísticas del tráfico de datos actual para la primera sucursal, para los días señalados, se presentan en las figuras 4.8 hasta la 4.12.



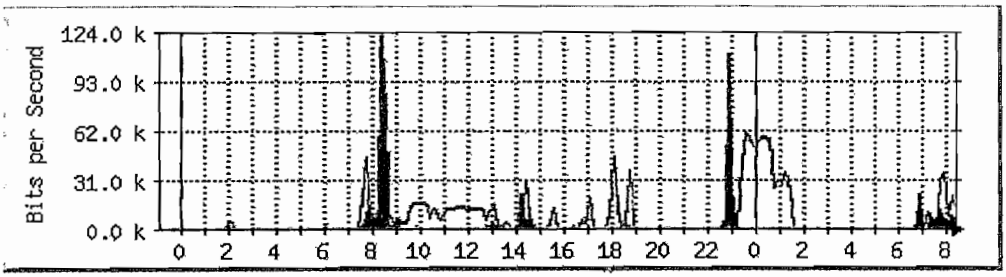
Máx Ent:76.7 kb/s (59.9%) Promedio Ent:4160.0 b/s (3.2%) Actual Ent:9768.0 b/s (7.6%)
Máx Sal:91.0 kb/s (71.1%) Promedio Sal:7672.0 b/s (6.0%) Actual Sal:9248.0 b/s (7.2%)

Figura 4.8: Tráfico para el Lunes 17 de Mayo del 2004 de la Primera Sucursal



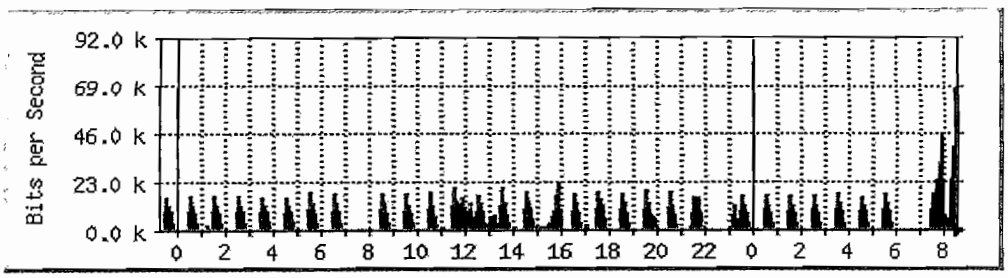
Máx Ent:112.3 kb/s (87.7%) Promedio Ent:5768.0 b/s (4.5%) Actual Ent:17.6 kb/s (13.7%)
Máx Sal: 88.7 kb/s (69.3%) Promedio Sal:2096.0 b/s (1.6%) Actual Sal:13.8 kb/s (10.8%)

Figura 4.9: Tráfico para el Martes 18 de Mayo del 2004 de la Primera Sucursal



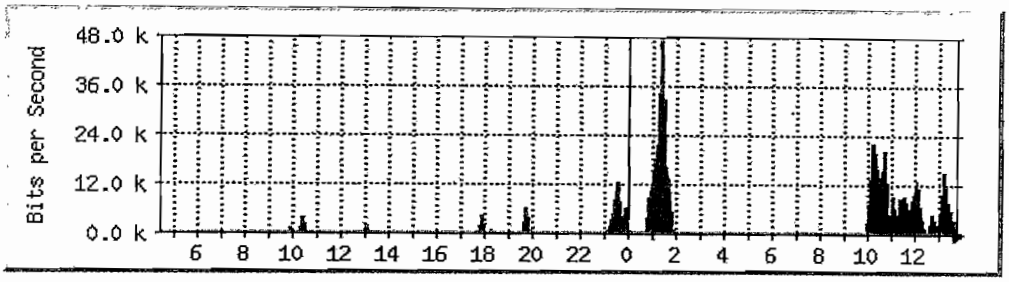
Máx Ent:123.9 kb/s (96.8%) Promedio Ent:3408.0 b/s (2.7%) Actual Ent:6680.0 b/s (5.2%)
Máx Sal: 60.1 kb/s (46.9%) Promedio Sal:6936.0 b/s (5.4%) Actual Sal: 12.5 kb/s (9.8%)

Figura 4.10: Tráfico para el Miércoles 19 de Mayo del 2004 de la Primera Sucursal



Máx Ent:91.4 kb/s (71.4%) Promedio Ent:5712.0 b/s (4.5%) Actual Ent:91.4 kb/s (71.4%)
Máx Sal:28.9 kb/s (22.6%) Promedio Sal:1216.0 b/s (1.0%) Actual Sal: 10.0 kb/s (7.8%)

Figura 4.11: Tráfico para el Jueves 20 de Mayo del 2004 de la Primera Sucursal



Máx Ent:47.8 kb/s (37.3%) Promedio Ent:1912.0 b/s (1.5%) Actual Ent:3712.0 b/s (2.9%)
Máx Sal:12.9 kb/s (10.1%) Promedio Sal: 608.0 b/s (0.5%) Actual Sal:2496.0 b/s (2.0%)

Figura 4.12: Tráfico para el Viernes 21 de Mayo del 2004 de la Primera Sucursal

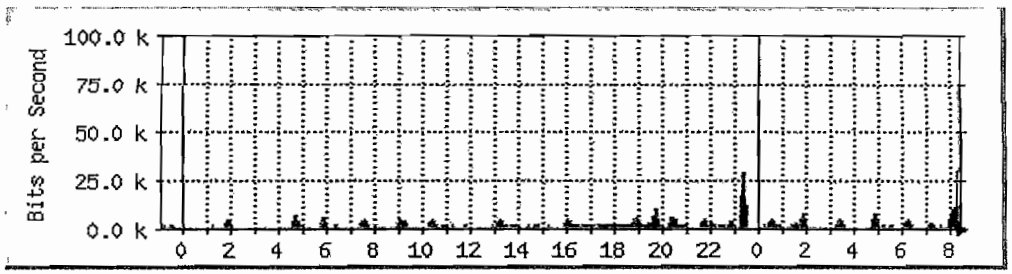
Una vez que se tiene el promedio del tráfico total entrante y saliente por separado, ver la tabla 4.8, se procede a sumar dichos valores para obtener el tráfico total de datos actual para la primera sucursal, el resultados es: 5.252 kbps + 7.312 kbps = 12.564 kbps.

Día	Tráfico Entrante (kbps)	Tráfico Saliente (kbps)
17 de Mayo	6.27	13.82
18 de Mayo	6	5.27
19 de Mayo	5.36	12.27
20 de Mayo	6.27	3.10
21 de Mayo	2.36	2.10
Promedio	5.252	7.312

Tabla 4.8: Tráfico de datos promedio de la Primera Sucursal

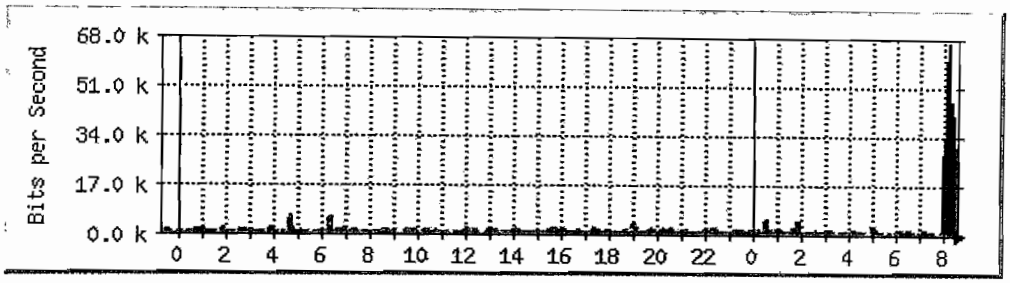
c) Tráfico de datos actual de la Segunda Sucursal

La información relacionada con el tráfico de datos que actualmente maneja la segunda sucursal, para los días especificados, se presentan en las figuras 4.13 hasta la 4.17.



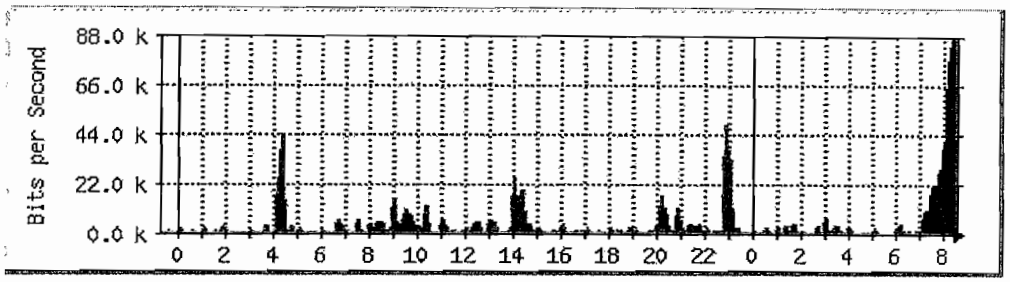
Máx Ent:29.1 kb/s (22.8%) Promedio Ent:1888.0 b/s (1.5%) Actual Ent: 12.0 kb/s (9.4%)
Máx Sal:96.7 kb/s (75.6%) Promedio Sal:1384.0 b/s (1.1%) Actual Sal:96.7 kb/s (75.6%)

Figura 4.13: Tráfico para el Lunes 17 de Mayo del 2004 de la Segunda Sucursal



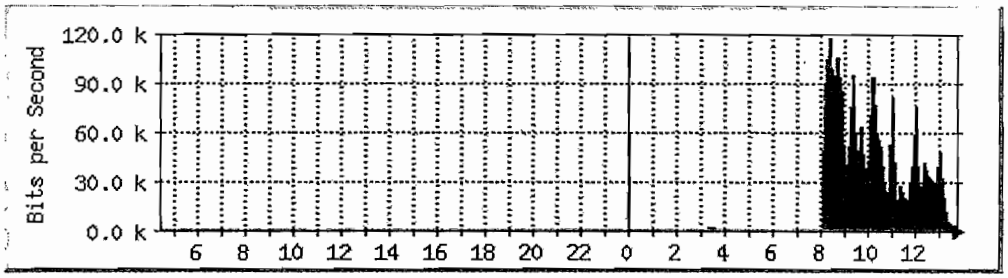
Máx Ent:67.2 kb/s (52.5%) Promedio Ent:2424.0 b/s (1.9%) Actual Ent:28.8 kb/s (22.5%)
Máx Sal:17.0 kb/s (13.3%) Promedio Sal:1376.0 b/s (1.1%) Actual Sal:13.2 kb/s (10.3%)

Figura 4.14: Tráfico para el Martes 18 de Mayo del 2004 de la Segunda Sucursal



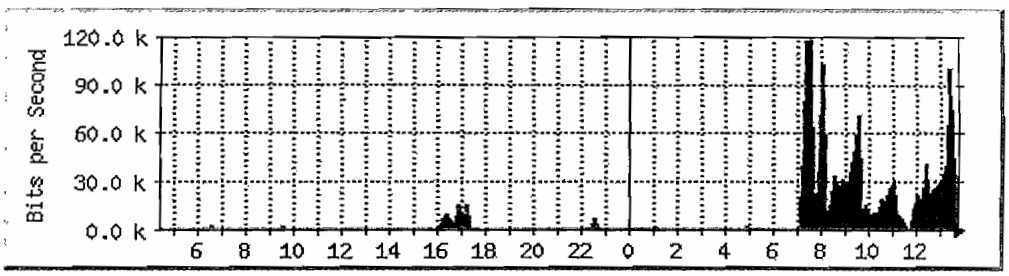
Máx Ent:87.8 kb/s (68.6%) Promedio Ent:4952.0 b/s (3.9%) Actual Ent:87.8 kb/s (68.6%)
Máx Sal:66.4 kb/s (51.9%) Promedio Sal:1784.0 b/s (1.4%) Actual Sal:26.7 kb/s (20.9%)

Figura 4.15: Tráfico para el Miércoles 19 de Mayo del 2004 de la Segunda Sucursal



Máx Ent:117.9 kb/s (92.1%) Promedio Ent:8256.0 b/s (6.5%) Actual Ent:3864.0 b/s (3.0%)
Máx Sal: 19.2 kb/s (15.0%) Promedio Sal:1488.0 b/s (1.2%) Actual Sal:3928.0 b/s (3.1%)

Figura 4.16: Tráfico para el Jueves 20 de Mayo del 2004 de la Segunda Sucursal



Máx Ent:119.0 kb/s (46.5%) Promedio Ent:7224.0 b/s (2.8%) Actual Ent: 25.4 kb/s (9.9%)
Máx Sal: 15.6 kb/s (6.1%) Promedio Sal:1072.0 b/s (0.4%) Actual Sal:4504.0 b/s (1.8%)

Figura 4.17: Tráfico para el Viernes 21 de Mayo del 2004 de la Segunda Sucursal

Una vez que se tiene el promedio del tráfico total entrante y saliente, ver la tabla 4.9, se procede a sumar dichos valores para obtener el tráfico total de datos actual para la segunda sucursal, el resultados es: 3.91 kbps + 3.018 kbps = 6.928 kbps.

Día	Tráfico Entrante (kbps)	Tráfico Saliente (kbps)
17 de Mayo	3.45	3.45
18 de Mayo	2.73	2.91
19 de Mayo	7.10	3.73
20 de Mayo	4	3
21 de Mayo	2.27	2
Promedio	3.91	3.018

Tabla 4.9: Tráfico de datos promedio de la Segunda Sucursal

4.2.3.2 Determinación de la capacidad requerida para la VPN

Ya que la VPN se utilizará para realizar operaciones comerciales, a través de la base de datos (SAP), el tamaño de los archivos SAP generado típicamente por la base de datos es de 64 kbytes, como se puede observar en la figura 4.18.

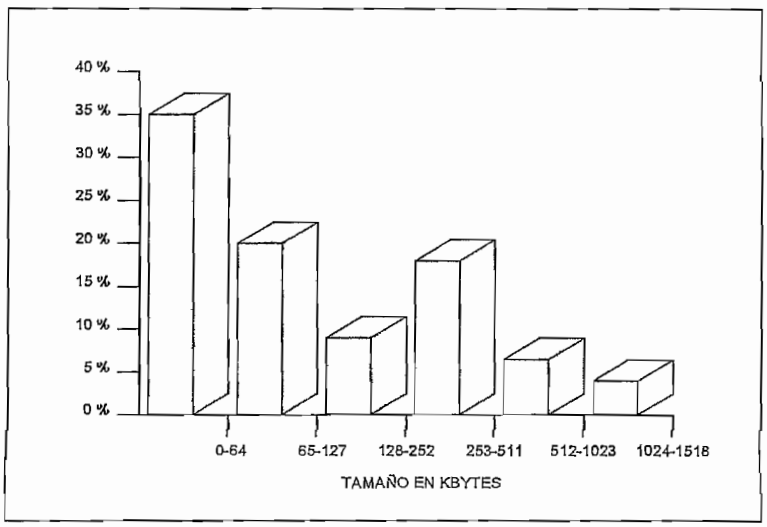


Figura 4.18: Distribución del tamaño de los paquetes de SAP[3]

[3] Esta distribución del tamaño típico de los paquetes de SAP ha sido recopilada de la página web de SAP, http://www.sap.com.

Así, la base de datos utilizará la VPN para realizar transacciones comerciales tales como: facturación y determinación del equipo disponible en *stock* en la empresa, de una manera confiable y segura. La base de datos distribuida (base de datos residente en el servidor de cada oficina) deberá ser actualizada cuando se realice una compra o venta (de acuerdo a los requerimientos actuales de la empresa), no solo en la matriz sino también en sus sucursales.

La tabla 4.10, muestra la distribución del número total de usuarios de la red empresarial y el número de usuarios que necesitan seguridad en los datos, es decir usuarios de la VPN.

Lugar	Número de usuarios	Número de usuarios de la VPN
Matriz Quito	25	5
Primera Sucursal	15	3
Segunda Sucursal	10	3

Tabla 4.10: Número de usuarios de la VPN

Debe notarse que el número de usuarios de la VPN es igual al número de usuarios autorizados a tener acceso a la base de datos en su respectiva oficina, ya que esta información se considera confidencial.

a) Capacidad requerida para la Primera Sucursal

La empresa necesitará que los 3 usuarios de la primera sucursal que manejan la base de datos estén simultáneamente conectados con la matriz.

Como ya se mencionó anteriormente, la aplicación de la base de datos es de 64 kbytes y se tiene 3 usuarios conectados simultáneamente, por lo que la aplicación de la base de datos generará un flujo de información de:

64 kbytes/usuario * 8 bits/byte= 512 kbits/usuario

512 kbits/usuario * 3 usuarios = 1536 kbits

$$1536 \text{ kbits} / 50^{4} \text{ s} = 30.72 \text{ kbps} \approx 31 \text{ kbps}.$$

Se considera 50 segundos, ya que la información deberá ir y volver ante alguna respuesta del lado de la matriz.

Es necesario para complementar la capacidad total del canal, añadirle al tráfico de la base de datos, aquel que generan los usuarios en Internet, por lo tanto se tiene: 13 kbps + 31 kbps = 44 kbps.

b) Capacidad requerida para la Segunda Sucursal

Igualmente, la empresa necesitará que los 3 usuarios de la segunda sucursal que manejan la base de datos de esta sucursal, estén simultáneamente conectados con la matriz.

Como ya se mencionó anteriormente la aplicación de la base de datos es de 64 kbytes y se tiene 3 usuarios conectados simultáneamente, por lo que la aplicación de la base de datos generará un flujo de información de:

$$64 \text{ kbytes/usuario} * 8 \text{ bits/byte} = 512 \text{ kbits/usuario}$$
$$512 \text{ kbits/usuario} * 3 \text{ usuarios} = 1536 \text{ kbits}$$
$$1536 \text{ kbits} / 50 \text{ s} = 30.72 \text{ kbps} \approx 31 \text{ kbps}.$$

Es necesario para complementar la capacidad total del canal para la segunda sucursal, añadirle al tráfico debido a la base de datos, aquel que generan los usuarios en Internet, por lo tanto se tiene: 7 kbps + 31 kbps = 38 kbps.

A las capacidades de los canales de las tres oficinas se considerará un incremento del tráfico del 15 %, por los siguientes factores:

---

[4] En la página web de SAP, mencionada anteriormente, se indica que el tiempo de respuesta para esta aplicación sería de aproximadamente 25 segundos.

- Crecimiento: según el dato proporcionado por la empresa, ésta ha experimentado un crecimiento del 30 % en cinco años, lo cual significa un crecimiento promedio anual del 6 %, dicho porcentaje se reflejará principalmente en la capacidad del canal de transmisión; y
- *Overhead*: Se considerará que en FR, con un campo típico de datos de 128 *bytes*, el rendimiento es del 92.75% ((128/138)*100). Con lo cual el porcentaje estimado por *overhead* está alrededor del 7.25 %.

En la tabla 4.11, se muestran las capacidades totales de transmisión de la primera y segunda sucursal.

Sitio	*Capacidad* requerida (kbps)	*Incremento (15%)* (kbps)	*Capacidad total* (kbps)	*Capacidad ofrecida* (kbps)
Primera Sucursal	44	6.6	50.6	64
Segunda Sucursal	38	5.7	43.7	64

Tabla 4.11: Capacidad total de los canales de las sucursales

Esto sugiere que con la actual capacidad contratada de 64 kbps, por parte de las dos sucursales, es suficiente para soportar la nueva aplicación de la base de datos, por lo que no es necesario un incremento adicional.

c) Capacidad requerida para la Matriz

En la matriz se debe tomar en cuenta que va a concurrir la información de las dos sucursales, por lo tanto para dimensionar la capacidad de la matriz se procederá de la siguiente manera:

- Según el tráfico de datos que actualmente maneja la matriz (ver sección 4.2.3.1, literal a), éste es de 32 kbps. Nótese que este tráfico no considera los requerimientos de la base de datos.

- Por otro lado, el tráfico requerido por la base de datos, de acuerdo a las nuevas necesidades de la empresa (ver sección 4.2.3.2, literales a y b), es: 31 kbps para la primera sucursal y 31 kbps para la segunda sucursal.

De manera que la capacidad requerida por la matriz incluida la nueva aplicación de la base de datos, es: 32 kbps + 31 kbps + 31 kbps = 94 kbps.

Además considerando el factor de crecimiento del 15% ya explicado anteriormente, se tiene que para la matriz se requiere una capacidad total de 108 kbps, por lo que la capacidad contratada al ISP deberá ser de 128 kbps (ver tabla 4.12).

Sitio	*Capacidad* requerida (kbps)	*Incremento (15%)* (kbps)	*Capacidad total* (kbps)	*Capacidad ofrecida* (kbps)
Matriz	94	14.1	108.1	128

Tabla 4.12: Capacidad total para la Matriz

Esto sugiere que con la actual capacidad contratada de 128 kbps, es suficiente para soportar la nueva aplicación de la base de datos, por lo que no es necesario ningún incremento adicional.

4.2.4 CONEXIÓN A INTERNET

El servicio contratado al SP consta de los siguientes componentes:

- Un *router* para transmitir las tramas al medio de comunicación contratado.
- Una unidad terminal de datos digitales DTU[5].
- Un enlace proporcionado por el proveedor de comunicaciones.

[5] Un dispositivo en el extremo del usuario, habitualmente un módem u otro dispositivo de comunicaciones, que actúa como punto de acceso al medio de transmisión.

Al configurar una conexión permanente a Internet, se trabaja con el ISP, el cual se encarga de dimensionar e instalar los equipos terminales necesarios (*router* y DTU) y de proporcionar el enlace requerido. La red local deberá conectarse a la interfaz correspondiente del *router*. El ISP se encarga de todos los aspectos relacionados con la conexión de la interfaz WAN a Internet.

Puesto que el enlace ofrecido por el ISP es un enlace *Frame Relay*, se sugiere mantener dicho enlace FR, como tecnología de acceso al ISP, por lo que no es necesario cambio alguno.

4.2.5 TOPOLOGÍA DE LA VPN

La topología de la red de diseño es del tipo *hub and spoke* o radial (ver la sección 3.4.1.2), implementada en un modelo VPN *overlay* (ver la sección 3.3.1), ya que las oficinas remotas (sitio 2 y sitio 3) se conectan a la oficina central (sitio1), como se muestra en la figura 4.19. Esta topología es apropiada para entornos, en los que la mayor parte del trabajo de las oficinas remotas es intercambiar datos con el sitio central y no entre ellas, ya que los datos intercambiados entre las oficinas remotas se transportan a través del sitio central.

La capacidad total para los enlaces, es la señalada en la figura 4.19 y corresponde a la calculada en las tablas 4.11 y 4.12. Además se sugiere mantener los dos enlaces en la ciudad de Quito mediante cable de cobre, por su economía, y el enlace de Guayaquil vía microonda.

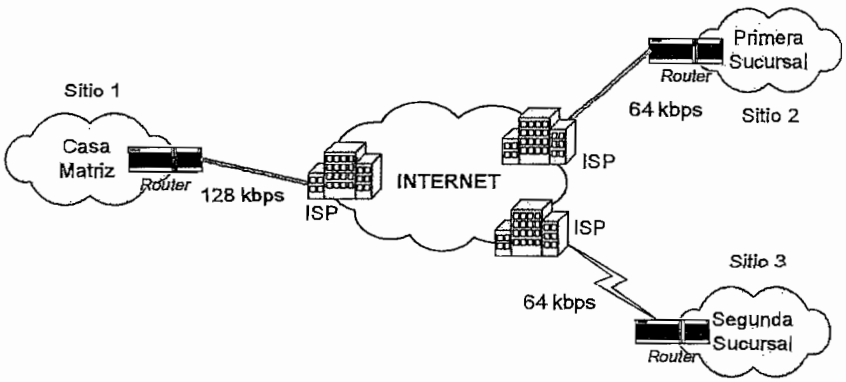


Figura 4.19: Topología de la VPN de diseño

4.2.6 EQUIPOS PARA LA VPN CLÁSICA [2]

En general la VPN estará conformada por los siguientes equipos:

- Servidores de base de datos y de correo electrónico.
- Estaciones de trabajo.
- *Switches.*
- *Routers* para el acceso a la red pública y/o a la red privada de datos.
- Una DTU para la conexión física hacia el ISP.

Existen varios fabricantes, que presentan equipos que reúnen todas las funcionalidades para construir VPNs, particularmente la autentificación así como también el cifrado y túnel.

Como se indicó al principio de este capítulo, el modelo a desarrollarse responde al de las VPNs basadas en dispositivos CE, para lo cual se utilizará la tecnología de *tunneling* IPSec, instalada en el *router* CE para dar la adecuada conectividad entre los diferentes sitios de la VPN.

Para el caso particular de la empresa tomada como referencia, los equipos con los que cuenta actualmente dicha empresa se describen a continuación:

a) Matriz

En la red LAN de la matriz se cuenta con un *switch* de 100 Mbps de 48 puertos, dado que la empresa tiene 25 usuarios, con este equipo se dispondría de un excedente, lo cual permitiría ampliar la red a futuro.

Para la conexión de la LAN de la matriz y la WAN se utiliza un *router.* El *router* tiene un puerto Fast Ethernet, para conectar la LAN; y, un puerto serial (V.35) para conectar el equipo al enlace WAN. En la tabla 4.13, se muestra el modelo actual del *router* de la empresa con su respectivo *hardware* y el costo referencial[6].

[6] Estos precios no incluyen IVA y además son precios referenciales.

El costo del *router* es presentado en caso de que la empresa necesite un equipo de similares características, ya sea por: respaldo, reposición o implementación de una nueva sucursal.

Equipo	Descripción	Cantidad	Costo unitario (USD)	Costo Total (USD)
Cisco 1750	*Router* + 1 puerto Ethernet 10/100	1	1850	1850
	WIC-1T con 1 puerto Serial WAN	1		
	CAB-SS-V35MTV.35 Cable, DTE	1	100	100
			Total	**1950**

Tabla 4.13: Router de la oficina Matriz

b) Primera sucursal

En la red LAN de la primera sucursal se tiene un *switch* de 100 Mbps de 24 puertos lo que permite tener un crecimiento y además puertos disponibles en caso de daños de alguno de ellos.

Para la conexión de la LAN de la primera sucursal y la WAN se utiliza un *router*. El *router* tiene un puerto Fast Ethernet, y un puerto serial el cual permita conectar el equipo al DTU (enlace WAN). En la tabla 4.14, se muestra el modelo actual del *router* de la empresa con su respectivo *hardware* y el costo referencial correspondiente.

Equipo	Descripción	Cantidad	Costo unitario (USD)	Costo Total (USD)
Cisco 1601	*Router* + 1 puerto Ethernet 10/100	1	1400	1400
	WIC-1T con 1 puerto Serial WAN	1		
	CAB-SS-V35MTV.35 Cable, DTE	1	100	100
			Total	**1500**

Tabla 4.14: Router de la Primera Sucursal y Segunda Sucursal

c) Segunda Sucursal

Al igual que en la sucursal anterior, la red LAN tiene un *switch* de 100 Mbps de 12 puertos, lo que permite tener un crecimiento y además puertos disponibles en caso de daño de alguno de ellos.

Para la conexión de la LAN y la WAN se utiliza un *router*. El *router* debe tener un puerto Fast Ethernet, y un puerto serial que permita conectar el equipo al DTU (enlace WAN). Puesto que la segunda sucursal cuenta con un *router* 1601 de la marca Cisco (ver la sección 4.2.1.3), las características de dicho *router* se muestran en la tabla 4.14.

Como se aclaró anteriormente la empresa posee *routers* de la marca Cisco, (ver sección 4.2.1), los cuales presentan adicionalmente las siguientes características:

- Proporciona el *software* Cisco IOS (*Internetworking Operating System*).
- Puertos LAN 10/100 Mbps.
- Para la serie 1600, se tiene 8 MB de memoria DRAM y 4 MB memoria Flash, expandible a 24 MB y 16 MB respectivamente. Para la serie 1700, se tiene de 64 MB de memoria DRAM y 32 MB de memoria Flash, expandible a 128 MB en memoria DRAM.
- Ofrece métodos de *tunneling* basados en estándares tales como: IPSec, L2TP, L2F para crear VPNs.
- La serie 1700 puede establecer 100 túneles.
- La serie 1700 permite un cifrado DES ó 3DES (168 bits).

En el Anexo C, se puede observar mayores detalles de los *routers* mencionados.

Debido a que los *routers* actuales de la empresa reúnen las características adicionales, anteriormente señaladas, dichos *routers* pueden soportar la tecnología VPN y así para el presente proyecto se utilizarán los *routers* de la empresa, los cuales con una configuración extra, además de la actualización del

sistema operativo del *router* CE, pueden brindar el servicio de VPNs, ya que éstos tienen la capacidad de cifrar datos.

Las ventajas de esta solución son: el uso del *hardware* existente, disponibilidad de una sólida seguridad y bajo costo. Pero es necesario aclarar que en el futuro se deberá realizar mediciones de tráfico, para las correcciones adecuadas que podrían implicar una actualización a un *router* de mejores características técnicas (CPU y memoria) y/o un redimensionamiento de las capacidades de los canales.

Así, cuando un usuario quiera conectarse a la oficina central desde la sucursal, el tráfico saldrá cifrado del dispositivo CE de la sucursal; al llegar a la oficina central, será descifrado.

La administración de claves se realiza en el *router* de la oficina central, utilizando para el cifrado de datos, el protocolo IPSec. La autentificación de los dispositivos CE estará basada en claves precompartidas[7].

4.2.7 ASIGNACIÓN DE UN ESPACIO DE DIRECCIONES IP

Por lo general, el ISP contratado se encarga del direccionamiento WAN. Así la dirección de red asignada a la empresa es 195.12.2.0 IP pública clase C. Para el direccionamiento WAN se utilizará la dirección pública con una máscara 255.255.255.224, lo cual posibilita el tener 6 subredes. La asignación de las direcciones IP de subred para la WAN, se muestra en la tabla 4.15.

El direccionamiento de las LANs internas puede ser realizado utilizando el RFC 1918. Para el presente proyecto se usará un espacio de direcciones IP privadas de clase C en cada sitio, el espacio se refiere al número previsto de redes y *hosts* que se deben admitir en la red de toda la empresa. Puesto que la matriz cuenta con 25 *hosts*, es recomendable utilizar el espacio de direcciones del bloque de

[7] Clave introducida en cada par manualmente, usada para autentificar al par. Los pares de IKE se autentifican el uno al otro calculando y enviando una función tipo *hash* con clave de datos que incluye la clave precompartida. Si el par receptor es capaz de crear la misma función tipo *hash* independientemente usando su clave precompartida, sabe que ambos pares deben compartir la misma clave secreta, autentificando así al otro par.

clase C. De este espacio de direcciones IP para las sucursales se tendrá un sobrante de direcciones IP privadas para un crecimiento futuro, ya que es necesario menos direcciones IP. Así, las direcciones internas se configuran en una subred de la red 192.168.10.0/27, en la matriz. En las sucursales se procede de manera similar (ver tabla 4.15).

Red	Lugar	Sitio	Subred
WAN	Quito (Matriz)	1	195.12.2.32/27
	Quito (Primera Sucursal)	2	195.12.2.64/27
	Guayaquil (Segunda Sucursal)	3	195.12.2.96/27
LAN	Red Interna (Matriz)	1	192.168.10.32/27
	Red Interna (Primera Sucursal)	2	192.168.10.64/27
	Red Interna (Segunda Sucursal)	3	192.168.10.96/27

Tabla 4.15: Direcciones IP asignadas a la VPN de diseño

Cuando se utiliza direcciones IP privadas (RFC 1918), no es posible conectarse directamente a Internet, para lo cual es necesaria una dirección pública enrutable. La traducción de direcciones de red (NAT, *Network Address Translation*) posibilita a las redes IP privadas, conectarse a Internet.

NAT traduce una dirección IP en otra de acuerdo con cierta tabla de equivalencias. En la VPN de diseño, la traducción la realizará el *router* (ver figura 4.20) en cada sitio de la red empresarial. Así, NAT tiene una doble función: brindar seguridad y conservar el direccionamiento privado.

La Traducción de direcciones de puerto (PAT) o NAT multiplexada a nivel de puerto, se utiliza para traducir todas las direcciones privadas (locales) internas a una sola dirección IP exterior (global, generalmente registrada). Se utiliza números de puerto únicos en cada conversión para distinguir entre las comunicaciones.

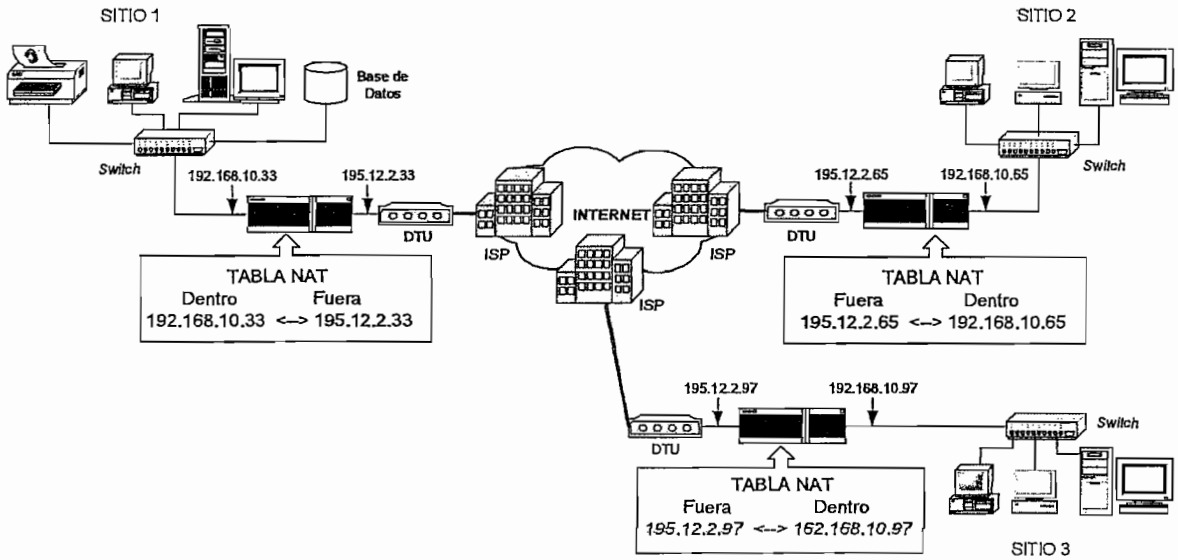


Figura 4.20: Aplicación de NAT en la VPN de diseño

Un aspecto a tener en cuenta es que al utilizar NAT, ésta sucede antes de IPSec en la ruta de salida, e IPSec sucede antes de NAT en la ruta de entrada. Por tanto, IPSec funciona con las direcciones traducidas en términos de identificación de los flujos que debe proteger. Esto también significa que el paquete IPSec no puede ser traducido posteriormente en ningún sitio entre el origen y el destino, porque modificar el paquete protegido mediante IPSec de cualquier forma hará fracasar la autentificación IPSec, invalidando así el paquete.

Adicionalmente se implementará en los *routers* de la red empresarial un *firewall* de filtración de paquetes (ver la sección 1.7). El filtrado de paquetes, se instalará en el *router* de la VPN para controlar el tráfico que ingresa en la red. El filtrado de paquetes es usado como una segunda línea de defensa, después que los paquetes son autentificados por IPSec.

Puesto que el modelo de referencia TCP/IP no tiene un estándar sobre el filtrado de paquetes, los fabricantes de *routers* son libres de elegir las características del filtrado. Algunos permiten configurar distintos filtros, dependiendo de la interfaz sobre la que van a actuar, mientras que otros sólo permiten una única configuración para todas las interfaces del *router*.

Se tiene dos estrategias básicas para decidir qué tipo de información se admite:

- Permitir por defecto la entrada: se le da al *firewall* las condiciones para bloquear el tráfico.
- Denegar por defecto: se dan las condiciones para permitir el tráfico.

El filtrado de paquetes se configura en el *router* mediante listas de control de acceso (ACLs, *Access Control Lists*)[8], que son instrucciones que especifican condiciones que se definen para que el *router* maneje el tráfico definido por la lista de acceso.

Para aprovechar las ventajas de seguridad de las ACLs, se configuran las ACLs en el *router* CE situado en la frontera de la red. Esto proporciona protección básica con respecto a la red externa, u otra parte menos controlada de la red, para un área más privada de la red.

Por ejemplo los *routers* de Cisco soportan dos tipos de listas: las listas estándares, que restringen el flujo de paquetes basándose en la dirección origen del paquete y las extendidas, que además de la dirección origen, también miran la dirección destino, el tipo de protocolo, el número de puerto y otros parámetros, como se muestra en la tabla 4.16.

PROTOCOLO	TIPO	RANGO	FILTRADO POR
IP	Estándar	1-99 y 1300-1999	El origen
IP	Extendidas	100-199 y 2000-2699	El origen, destino, protocolo, puerto...
Ethernet	Código (tipo)	200-299	El tipo de código Ethernet
DECnet	Protocol suite	300-399	El origen
Appletalk	Protocol suite	600-699	El origen
Ethernet	Direcciones	799-799	La dirección MAC

Tabla 4.16: Numeración de las listas de acceso [3]

[8] Las listas de acceso son una serie de declaraciones condicionales, que pueden restringir la entrada de paquetes desde una interconexión a un *router*, de acuerdo con una serie de criterios. Los listados de acceso pueden utilizarse para impedir el flujo de paquetes entre una determinada interfaz del *router* o que salga de la misma. También puede utilizarse para restringir el acceso, a determinados usuarios y dispositivos, a los *routers* de la interconexión.

Las ACLs estándar no especifican direcciones destino, de manera que se debe colocar la ACL estándar lo más cerca posible del destino, las ACLs extendidas deben colocarse lo más cerca posible del origen del tráfico denegado. Dentro de las interfaces se colocan en el sentido de salida, para no procesar demasiados paquetes.

Así, como medida temporal para la matriz se asume que el tráfico proveniente de las sucursales se dejará pasar y el tráfico que no provenga de las sucursales será descartado, ver figura 4.21. De igual manera se procede en cada sucursal.

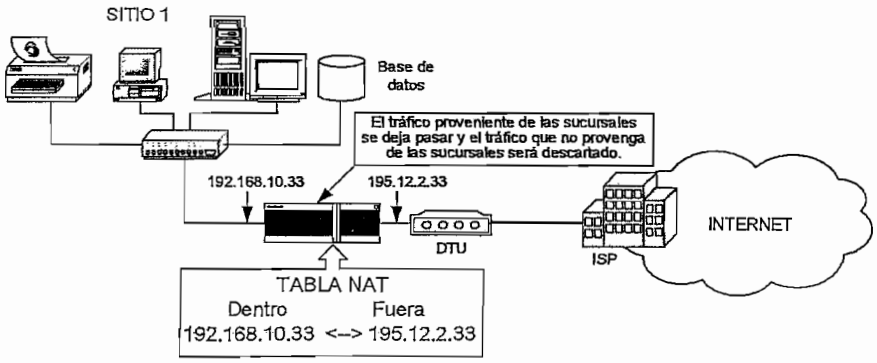


Figura 4.21: Lista de Control de Acceso

Para la VPN de diseño se utiliza tanto ACLs estándares como ACLs extendidas, ya que estas últimas definen qué tráfico IP será cifrado por IPSec y cuál no. Una mejora adicional al nivel de seguridad es la incorporación de un servidor *Proxy*, encaminado al control de acceso a Internet por parte de los usuarios internos y la implementación de funciones de autentificación.

4.2.8 ENRUTAMIENTO

El *router* CE está involucrado en: (i) el enrutamiento intra-sitio, (ii) terminación del túnel de la VPN, y (iii) el enrutamiento inter-sitio de la VPN. Así, el dispositivo CE es un dispositivo integrado que proporciona enrutamiento y terminación del túnel IPSec.

Puesto que solo se tiene un punto de entrada en la red del proveedor, y ya que el tráfico y la topología no varían significativamente, se utilizará enrutamiento estático. Las rutas hacia los destinos son numeradas manualmente en el *router.* La accesibilidad de la red en este caso no depende de la existencia y el estado de la propia red. Tanto si un destino está activo como si no, las rutas estáticas permanecen en la tabla de enrutamiento, y el tráfico es enviado hacia el destino especificado.

En la figura 4.22, se muestra la VPN de diseño. Debe notarse que los túneles VPN que aparecen señalados no son enlaces físicos sino lógicos que atraviesan el Internet.

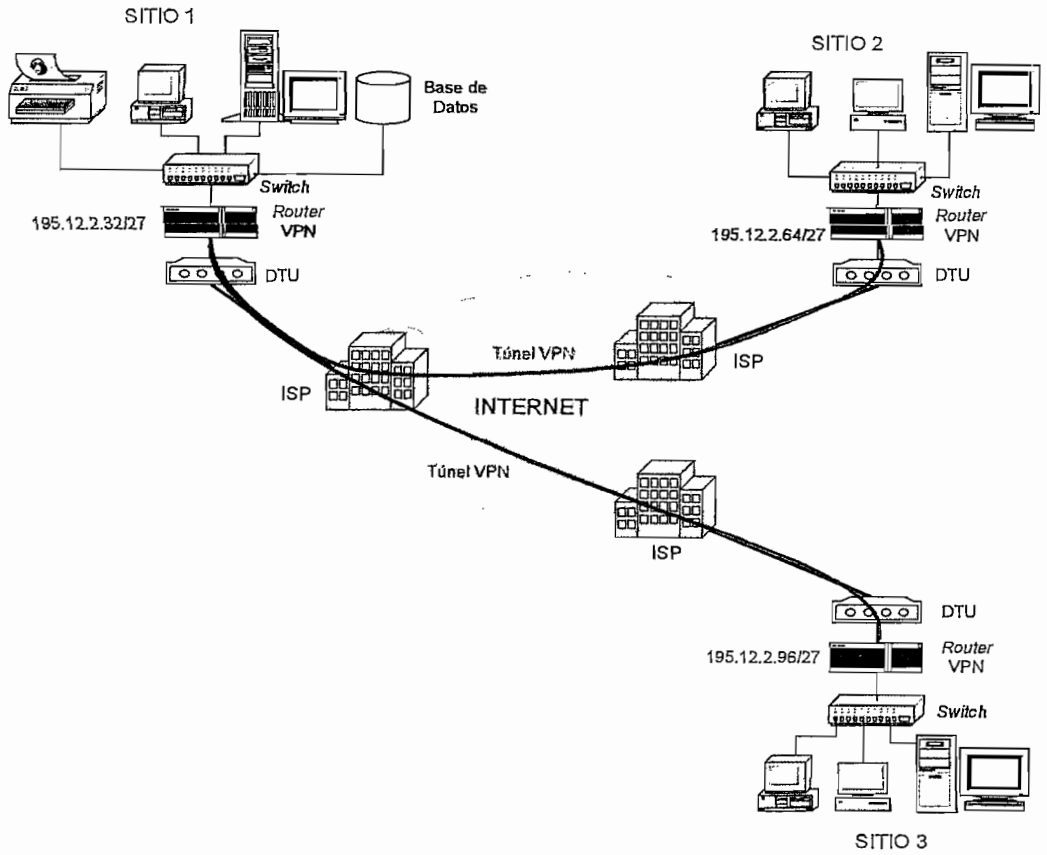


Figura 4.22: Diseño de la VPN clásica

A continuación se presenta la configuración básica de la VPN IPSec entre la matriz y la primera sucursal, dicha configuración tiene lugar en los *routers* CE de los dos sitios respectivos, ver figura 4.23.

Figura 4.23: Túnel IPSec entre la oficina Matriz y la Primera sucursal

Configuración del *Router* 1:

```
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key vpn-tesis address 195.12.2.66
!
!
crypto ipsec transform-set thesis esp-des esp-md5-hmac      ! Define el tipo de
                                                             cifrado (des) y el
                                                             algoritmo hash (md5-
                                                             hmac)
!
!
crypto map Supervpn 10 ipsec-isakmp      ! Define una entrada IPSec
 set peer 195.12.2.66                    ! Define el par asociado a esta entrada
 set transform-set thesis                ! Define el conjunto de transformación
                                         asociada con esta entrada
 match address 101                       ! Define la lista de acceso asociada con
                                         esta entrada
!
interface Serial 0
 ip address 195.12.2.34 255.255.255.224
 no ip directed-broadcast
 no ip mroute-cache
 crypto map Supervpn                     ! Indica a la interfaz que por ella
                                         trabajara una VPN denominada Supervpn
!
access-list 101 permit ip 192.168.10.32 0.0.0.31 192.168.10.64 0.0.0.31

!El comando anterior sirve para permitir o denegar a determinadas direcciones IP
transitar dentro del túnel IPSec
```

Configuración del *Router* 2:

```
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key vpn-tesis address 195.12.2.34
!
!
crypto ipsec transform-set thesis esp-des esp-md5-hmac
!
!
crypto map Supervpn 10 ipsec-isakmp
 set peer 195.12.2.34
 set transform-set thesis
 match address 101
!
interface Serial 0
 ip address 195.12.2.65 255.255.255.224
 no ip directed-broadcast
 no ip mroute-cache
 crypto map Supervpn
```

```
!
access-list 101 permit ip 192.168.10.64 0.0.0.31 192.168.10.32 0.0.0.31
```

4.3 COSTOS [9]

Esta sección detalla el costo que la empresa debería invertir para llevar a cabo la interconexión entre sus sucursales y su casa matriz utilizando la VPN. Cabe destacar que la red empresarial dispone de los enlaces hacia Internet para la matriz y sus sucursales, por lo tanto la empresa ya no paga por costos de instalación sino un costo mensual por el servicio de Internet.

La tabla 4.17, detalla los precios del servicio de Internet que un ISP cobra a sus clientes mensualmente.

Velocidad de transmisión (kbps)	Tipo de enlace	Costo del servicio de Internet (USD)
64	Local	350
128	Local	450

Tabla 4.17: Costos del medio de comunicación

La tabla 4.18, presenta el costo mensual que la empresa debería pagar por el acceso a Internet, para la oficina Matriz (128 kbps) y las sucursales (64 kbps, cada una), como sigue: 450 + 350 + 350 = 1150 USD. En el servicio técnico se incluye la actualización de la versión del sistema operativo y configuración de los *routers* CE para el soporte de la VPN.

Servicio	Costo del servicio (USD)
Internet (matriz + 2 sucursales)	1150
Servicio técnico	200
Total	**1350**

Tabla 4.18: Costo mensual por acceso a Internet

[9] Todos los valores presentados en esta sección fueron proporcionados por la empresa Impsat.

A continuación se presentará un análisis de los beneficios y desventajas que poseen las VPNs clásicas.

4.4 BENEFICIOS Y DESVENTAJAS DE LAS VPNs CLÁSICAS

4.4.1 BENEFICIOS

Seguridad: La VPN basada en IPSec ofrece cifrado. El cifrado añade otra capa de seguridad a la red. Otro nivel de seguridad puede lograrse a través de la implementación de una solución integrada. Las soluciones integradas combinan *firewall* y funcionalidad VPN en un dispositivo versus tener dispositivos separados para cada uno. Esta integración refuerza el nivel global de seguridad de la red y proporciona muchos beneficios a la empresa, como no tener que pasar los datos sin cifrar hacia o desde el *firewall* y una administración más fácil.

Costo: Puesto que se puede utilizar los dispositivos ya disponibles en la red empresarial, como los *routers*, la implementación de VPNs representa una alternativa rentable para conectar todas las redes remotas de una manera segura y económica.

Administración: La administración de la VPN basada en IPSec ha superado las capacidades de administración de otras tecnologías como FR, mediante la incorporación de políticas de administración en las actividades de configuración y actualización.

Complejidad: Tunneling, autentificación, cifrado, *firewall*, y seguridad, son nuevos aspectos que fueron requeridos para asegurar una red IP. Con las mejoras en la administración y facilidad de uso, mucha de la complejidad de las VPNs basadas en IPSec tiende a desaparecer. Con la simplicidad y las eficacias que se disponen por la administración centralizada y políticas de administración, las VPNs basadas en IPSec empiezan a ser menos complejas para instalar y administrar.

4.4.2 DESVENTAJAS

A continuación se comenta sobre algunos problemas que pueden afectar la implementación de la VPN IPSec.

La implementación de IPSec añade una sobrecarga debido a la complejidad de los algoritmos utilizados por IPSec. Existe también una sobrecarga del procesamiento adicional por las cabeceras de los paquetes relacionados con IPSec. El impacto de esta sobrecarga es difícil de cuantificar debido a que depende de la velocidad de procesamiento de los nodos de comunicación y el ancho de banda disponible.

Un inconveniente con IPSec es la degradación del desempeño. Así, la cantidad de latencia experimentada dependerá del dispositivo CE involucrado. Generalmente, un mejor desempeño, implica un costo más alto del dispositivo CE. Además, cada dispositivo CE, que en este caso es un *router*, debe tener la capacidad de soportar *tunneling*. Esta funcionalidad añadida se traduce en un costo adicional para este tipo de equipo.

Las VPNs IPSec son un tipo de red *overlay*. Éstas se colocan en lo alto de otra red IP. Debido a esto, se necesita establecer un túnel entre cada sitio, lo cual puede conducir a problemas de escalabilidad y desempeño.

La provisión es otro problema en las VPNs IPSec, ya que cada túnel IPSec debe establecerse manualmente. Configurar un solo túnel IPSec no es un problema, pero el tiempo requerido para formar una VPN multisitio aumenta cuando el tamaño de la red crece. Sustentar y restaurar este tipo de redes es dificultoso.

La seguridad es otra consideración, ya que cada dispositivo CE es accesible al Internet y confía en los túneles IPSec para transmitir los datos de manera segura entre los sitios. Por tanto, cada dispositivo CE debe tener medidas de seguridad, como un *firewall*, para proteger cada sitio de la red empresarial. El manejo de cada *firewall* se volverá muy difícil cuando la red crezca.

IPSec está solamente diseñado para manejar tráfico IP. Si se ejecuta en una red multiplataforma, puede ser necesario utilizar otros protocolos como PPTP o L2TP.

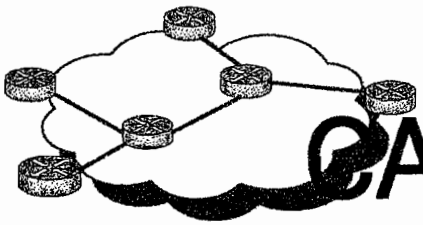
La interoperabilidad entre clientes IPSec de diferentes fabricantes a otros *gateways* de IPSec es débil, principalmente debido a los problemas de configuración.

BIBLIOGRAFÍA – CAPÍTULO 4

[1] CALLON R. y Otros, "*A Framework for Layer 3 Provider Provisioned Virtual Private Networks*", IETF draft, draft-ietf-ppvpn-framework-07.txt, Enero 2003 (trabajo en progreso).

[2] BROWN Steven, "Implementación de Redes Privadas Virtuales", Editorial McGraw-Hill, 2000.

[3] SACKETT C. George, "Manual de *routers* Cisco", Editorial McGraw-Hill, 2002.



CAPÍTULO 5

DISEÑO DE REDES PRIVADAS VIRTUALES CON MPLS

5.1 INTRODUCCIÓN

La reciente tendencia de obtener servicios de conectividad por parte de los Proveedores de Servicios (*Service Providers*) empieza a adquirir un gran apogeo. La demanda ha llevado a los SPs a buscar modos eficientes para dar servicios de valor agregado y ha llevado al advenimiento de un modelo basado en red, donde la inteligencia para dar los servicios reside en el borde de la red del SP. Como resultado, un conjunto completo de servicios de conectividad a empresas, incluyendo Redes Privadas Virtuales (VPNs) basadas en tecnología MPLS, pueden ahora ser proporcionados por los SPs desde dentro de sus redes.

Así, las VPNs MPLS vendrán dadas por un proveedor de servicios, ya que MPLS está desplegada en el núcleo de la red de un SP y es aquí donde la QoS, Ingeniería de tráfico y la utilización del ancho de banda pueden ser controladas, permitiendo a los proveedores habilitar SLAs (*Service Level Agreements*).

El mercado global para las "VPNs MPLS", como fue esbozado por el RFC 2547 [1], ha visto un crecimiento significativo desde el año 2000. La arquitectura MPLS promete dar una infraestructura de red capaz de entregar servicios IP a un gran número de subscriptores. Así, los SPs ven a las VPNs BGP/MPLS como una manera ideal de presentar los nuevos servicios al subscriptor básico e incrementar el retorno de inversión en su infraestructura de IP existente. Adicionalmente, el implementar las VPNs BGP/MPLS es una cuestión de actualizar el *software* del plano de control en los *routers* PE del SP, siempre y cuando los *routers* PE soporten esta tecnología, más adelante se presenta una tabla de los dispositivos que soportan MPLS.

El propósito de este capítulo es el diseño de VPNs basadas en MPLS, para lo cual el modelo a desarrollarse responde al de las VPNs basadas en dispositivos PE (*Provider Edge*) proporcionadas por un proveedor (ver la sección 3.2). Así, se procederá a presentar un modelo de diseño dado por el RFC 2547 o VPNs

BGP/MPLS, que de aquí en adelante se las denominará simplemente VPNs MPLS.

Revisando de forma rápida lo analizado anteriormente, respecto de las VPNs basadas en dispositivos PE (ver figura 5.1), un dispositivo PE (*Provider Edge*) implementa una o más VRFs (*VPN Routing and Forwarding*) para el soporte de una o más VPNs. El dispositivo PE puede ser un *router*, que incluya VRFs y la funcionalidad VPN en el borde del proveedor tales como provisión, manejo, clasificación y separación del tráfico. (Debe notarse que las conexiones de acceso son terminadas por VRFs desde el punto de vista funcional). Un dispositivo PE se conecta mediante una conexión de acceso a uno o más dispositivos CE (*Customer Edge*). Dichas conexiones de acceso pueden ser circuitos físicos dedicados, circuitos lógicos (tales como Frame Relay), o túneles IP. Puesto que la tecnología MPLS está propuesta para ser usada, sin tener en cuenta los medios de comunicación de la capa 1 y protocolos de la capa 2.

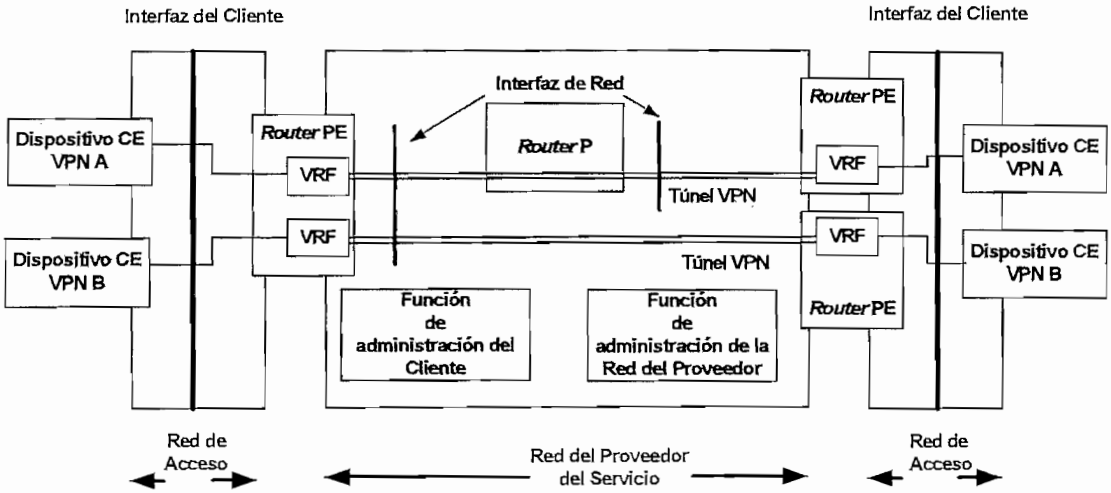


Figura 5.1: Modelo de referencia para las VPNs basadas en dispositivos PE [2]

Una red de acceso proporciona las conexiones de acceso entre los dispositivos CE y PE. Puede ser una red de capa 2 (por ejemplo: Frame Relay, ATM y Ethernet) o una red IP.

El *router* P se usa dentro de la red del proveedor para interconectar los dispositivos PE, pero no tiene funcionalidad específica de VPN y no tiene ninguna conexión directa con los dispositivos CE, como ya se comentó en la sección 3.4.1.1.

La figura 5.2, muestra una asociación IP convencional entre el dispositivo CE y PE, mientras la conexión PE a PE está basada en MP-iBGP para la distribución de la ruta de la VPN y tunelización jerárquica MPLS para el envío de datos.

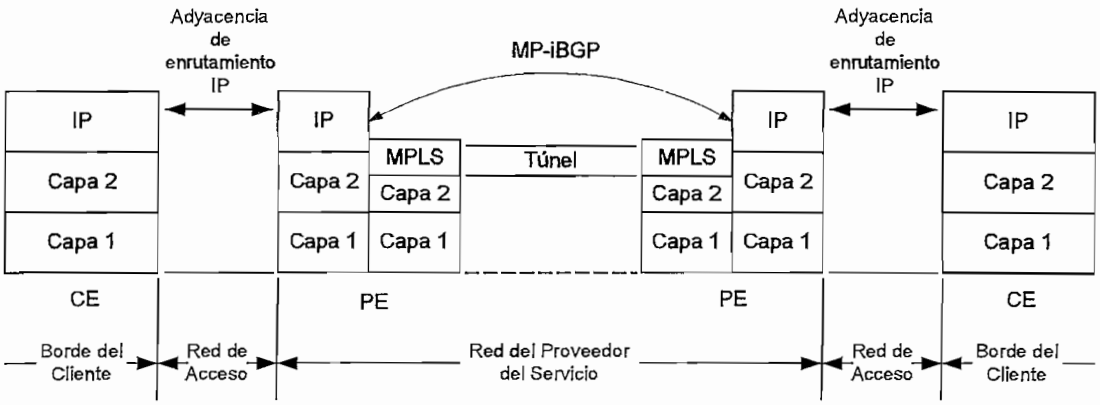


Figura 5.2: Conexión CE a CE con VPNs MPLS basadas en dispositivos PE [6]

5.2 DISEÑO DE LA VPN MPLS

Una vez que se describió en el capítulo anterior los elementos de la red del cliente y puesto que la tecnología MPLS no determina un cambio físico sobre la misma, el cambio radicará en que el proveedor será quien proporcione el servicio de VPN basado en tecnología MPLS.

Así, el *router* CE no será consciente de ninguna funcionalidad de MPLS. El único dispositivo en la red que se configurará específicamente para la VPN MPLS es el *router* PE. La interfaz de ingreso en el *router* PE se configurará para definir la VPN específica a la cual se conectan los sitios de la red empresarial. El *router* PE es responsable de asignar una etiqueta a cada VPN y de redistribuir las rutas entre el sitio y BGP dentro de la red del proveedor.

5.2.1 CARACTERÍSTICAS DE DISEÑO PARA LA VPN MPLS

Conocida la infraestructura existente, ver la sección 4.2.1, la misma idea se mantiene, es decir conectar las oficinas de la empresa tomada como referencia de una manera segura, por lo tanto se requiere realizar una Intranet corporativa, con este propósito se implementará una VPN basada en MPLS.

Así las características del escenario son:

- La VPN MPLS soportará el solapamiento de los espacios de direcciones, permitiendo a la empresa usar un espacio de direcciones IP privado. Solo las interfaces de los *routers* CE que se unen al *backbone* de la red pública requerirán de direcciones IP públicas.
- El *router* CE en cada sitio de la red empresarial no intercambiará directamente la información de enrutamiento con otros *routers* CE. La empresa no tiene que ocuparse de las cuestiones del enrutamiento intersitio, ya que éstas son responsabilidades del SP.
- Los usuarios de la VPN no tienen un *backbone* que administrar. Así, los usuarios no necesitan manejar el acceso a los *routers* PE.
- La escalabilidad está asegurada gracias a la doble indexación de etiquetas, ya que el núcleo de la red no tiene que saber nada de VPNs, y los equipos de borde solo tienen que almacenar la información relevante a las VPNs que cada uno maneje.
- El Internet público puede ser accedido sin requerir que las rutas de Internet sean reproducidas en las VRFs.

Puesto que la tecnología MPLS no puede intercambiarse con otras redes: si un proveedor de servicios no posee su propia red y se ve en la obligación de crear una VPN incorporando ancho de banda de una serie de proveedores mayoristas, no se podrá ofrecer MPLS en toda la red. Mientras que, en la actualidad, el intercambio de tráfico no representa un problema, el intercambio de clases de servicio de conformidad con los contratos de nivel de servicio (SLAs) específicos resulta muy difícil.

El primer paso del diseño, es definir los requerimientos para la solución VPN MPLS y asignar las convenciones de denominación necesarias y las políticas de enrutamiento para cada uno de los sitios que utilizará el servicio de VPN. Estos requerimientos están basados en la conectividad necesaria de los miembros de la VPN.

Así, las sucursales y la matriz de la Empresa, deben ser capaces de comunicarse entre sí. Dado este requerimiento de conectividad, se definen las mismas denominaciones para los sitios de la VPN de diseño, que en el anterior capítulo, ver la tabla 4.1, los cuales proveen la conectividad necesaria entre todos los sitios de la red empresarial.

5.2.2 DETERMINACIÓN DE LA CAPACIDAD DEL CANAL

Puesto que el tipo de información a transmitirse entre los sitios de la VPN es la misma que en el capítulo anterior, entonces se necesita la misma capacidad en los canales a contratarse al SP, ver la tabla 5.1.

Sitio	Capacidad de canal requerida
Matriz	128 kbps
Primera Sucursal	64 kbps
Segunda Sucursal	64 kbps

Tabla 5.1: Resumen de las capacidades de los canales

5.2.3 CONEXIÓN AL PROVEEDOR

Los elementos de red que forman parte de una VPN MPLS serán: el dispositivo CE, el enlace entre el dispositivo CE y el dispositivo PE, y la interfaz o subinterfaz en el dispositivo PE, ver la figura 5.3. El dispositivo PE en sí mismo no es parte de la VPN MPLS; esto implica que las direcciones *loopback*[1] no se proporcionan en el dispositivo PE como parte del servicio VPN MPLS.

[1] Dirección *loopback*: dirección reservada, que está diseñada para utilizarse en pruebas de TCP/IP y para la comunicación de procesos internos en una máquina local. Se puede usar para ejecutar y probar servicios (servidor/cliente) sin necesidad de estar conectado a una red física.

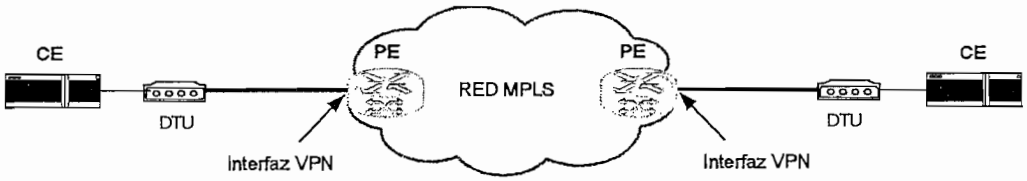


Figura 5.3: Elementos de la VPN MPLS de diseño

5.2.3.1 Puntos de Acceso al Servicio

El punto de acceso al servicio es la interfaz donde el SP proporciona el servicio de la VPN MPLS y garantiza el Nivel del Servicio acordado según el SLA. Además determina el límite de responsabilidad de la calidad de servicio total del SP.

Se definen dos tipos de puntos de acceso al servicio, los cuales se detallan a continuación:

5.2.3.1.1 SAP-CE

El SAP-CE está localizado en el dispositivo CE proporcionado, operado y mantenido por el SP. Es el punto lógico y físico donde el cliente accede a los servicios VPN MPLS y donde las responsabilidades del SP terminan (ver figura 5.4).

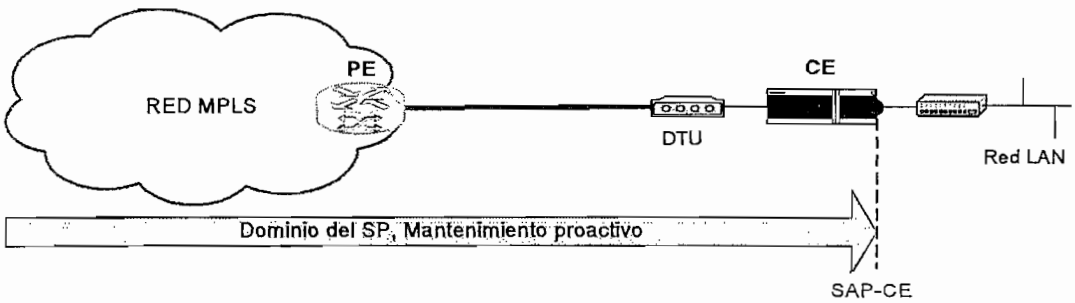


Figura 5.4: Punto de Acceso al Servicio en el dispositivo CE [4]

Debido a que el *router* CE pertenece al dominio del SP, éste monitorea el estado operativo del *router* CE y proporciona un mantenimiento proactivo, según el SLA y el servicio contratado.

El estado operativo del puerto LAN del *router* CE depende del cliente. El SP proporciona un mantenimiento reactivo (es decir que cuando el servicio colapsa, recién entonces se trata de corregir los problemas que lo causaron), después de los reportes de problemas referentes al puerto LAN del cliente del *router* CE.

Los SLAs proactivos son más atractivos ya que el proveedor mantiene una monitorización continua y, si es necesario, procede a una adecuada corrección. Los SLAs reactivos obligan a localizar al proveedor para obtener la indemnización, lo cual puede ser un proceso lento y complicado.

5.2.3.1.2 SAP-PE

El punto de acceso al Servicio es denominado SAP-PE, cuando el cliente proporciona, opera y mantiene el *router* CE (ver figura 5.5). Así, el SAP-PE está localizado en el *router* PE que pertenece a la red MPLS del SP.

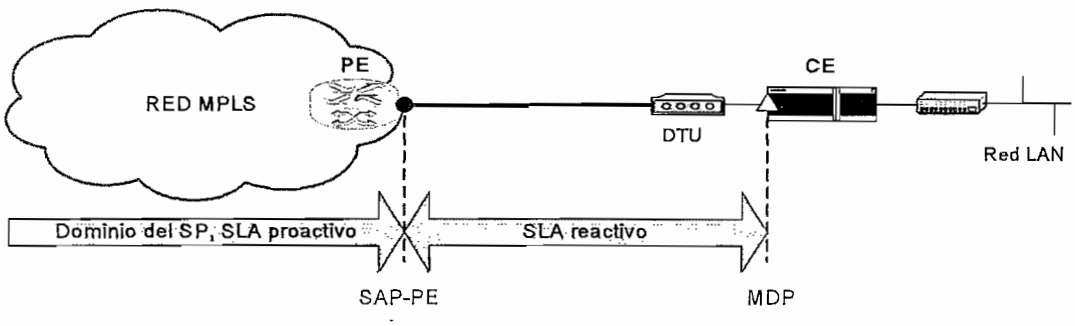


Figura 5.5: Punto de Acceso al Servicio en el dispositivo PE [4]

El SP proporciona la línea de acceso del *router* PE al *router* CE. Ésta puede ser:

1. Una línea arrendada que conecte la red del SP a la red del cliente;
2. Una conexión interna si el cliente despliega el *router* CE en un sitio o centro de alojamiento del SP.

El punto donde la conexión física entre las redes del cliente y del SP es llevada a cabo, también será el Punto de Demarcación de Mantenimiento (MDP,

Maintenance Demarcation Point) donde la responsabilidad de mantenimiento del SP termina.

La responsabilidad por la calidad de servicio extremo a extremo es dividida entre el SP y el cliente, como se muestra a continuación:

1. El SP es responsable de operar, mantener, administrar y proveer el servicio VPN MPLS hasta el SAP-PE, garantizar la disponibilidad del servicio de acuerdo a la Clase de Servicio definida en el SLA y realizar el mantenimiento proactivo.
2. El SP provee el acceso del SAP-PE y el MDP en el sitio del cliente o en centro de alojamiento del SP y proporciona un mantenimiento reactivo al recibir un informe del problema del cliente.

Comparando los dos tipos de puntos de acceso al servicio, es decir SAP-CE y SAP-PE, para la VPN de diseño lo recomendable es tener un servicio SAP-CE. Esto es debido a que el SP se hace responsable de la operación y mantenimiento del dispositivo CE, y la empresa puede enfocarse en sus redes de área local.

5.2.3.2 Red de Acceso

Como se comentó en la parte inicial del capítulo, la arquitectura VPN MPLS permite utilizar una red de acceso basada en tecnologías de acceso tradicionales, como circuitos Frame Relay. De modo que, para conectar los dispositivos CE y PE se lo hará utilizando Frame Relay, ver la figura 5.6.

Con la alternativa FR, no es necesario de más interfaces para la red WAN, lo que se requiere es de subinterfaces las cuales van a estar definidas dentro de la configuración del *router*, pero a través de una sola interfaz física. Lo cual se aprovecha para intercambiar entre la empresa y el proveedor, datos de la VPN e Internet sobre la misma infraestructura física. Es decir una subinterfaz se utilizará para transportar rutas específicas de la VPN y la otra subinterfaz se utilizará para transportar rutas específicas no VPN entre los *routers* CE y PE.

Los enlaces individuales de acceso son dimensionados de acuerdo al requerimiento de la capacidad de comunicación de los respectivos sitios. La tabla 5.1, muestra la capacidad total para los enlaces. Para mayores detalles, ver la sección 4.2.3.

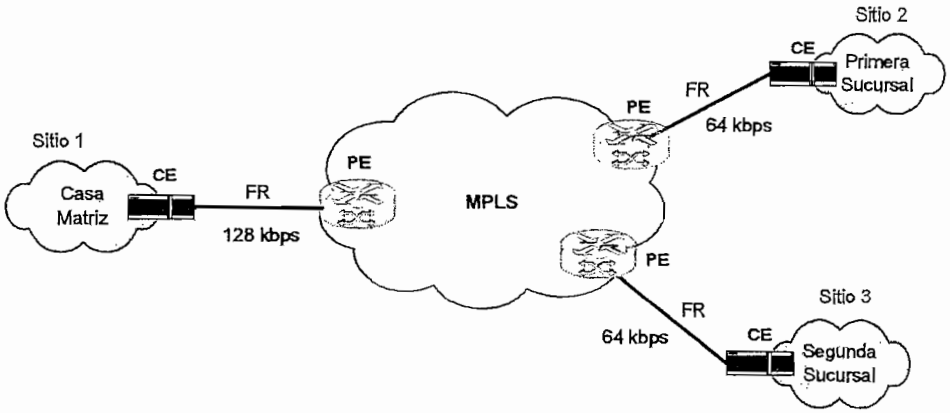


Figura 5.6: Red de Acceso de la VPN MPLS

5.2.4 TOPOLOGÍA DE LA VPN MPLS

La arquitectura VPN MPLS posibilita algunas alternativas en cuanto a topologías, tanto en el modelo VPN *overlay* como en el modelo VPN *peer to peer*. Así, permite topologías como por ejemplo: la topología *hub and spoke*, totalmente mallada (*full mesh*), y parcialmente mallada.

La topología de la red de diseño será del tipo *hub and spoke* o radial, ya que las oficinas remotas (sitio 2 y sitio 3) se conectan a la oficina central (sitio1). Esta topología es apropiada para entornos, en los que la mayor parte del trabajo de las oficinas remotas es intercambiar datos con el sitio central y no entre ellas, ya que los datos intercambiados entre las oficinas remotas se transportan a través del sitio central, esto debido a las políticas de la empresa de mantener en un solo sitio la administración de la empresa.

Si dichas políticas cambiasen, se podría tener una topología completamente mallada (*full mesh*), puesto que esta topología provee una conectividad "cualquiera a cualquiera", lo cual podría aprovecharse para conectar las

sucursales entre sí y tan solo se requeriría cambiar la configuración del *router* PE al cual está conectado el sitio correspondiente.

5.2.5 ACUERDO DEL NIVEL DE SERVICIO [4]

El contrato que especifica los parámetros de QoS acordados entre el proveedor y el cliente se denomina Acuerdo del Nivel de Servicio (SLA, *Service Level Agreement*). Para forjar un acuerdo en el cual los clientes puedan confiar, un proveedor de servicios necesita una red con capacidades de QoS y un sistema de administración de políticas para configurar, controlar, y mantener los niveles de desempeño. Un SLA define las especificaciones del servicio extremo a extremo y consiste de lo siguiente:

- Disponibilidad: Se define la disponibilidad del servicio como la fracción de tiempo en el cual el servicio está disponible entre un punto especifico de ingreso y un punto especifico de salida con los límites definidos en un SLA.
- Servicios ofrecidos: especificación de los niveles de los servicios ofrecidos.
- Garantías de servicio: para cada clase, para el *throughput*, tasa de pérdidas, retardo, variación del retardo.
- Responsabilidades: consecuencias por la ruptura de las reglas del contrato; localización del punto de demarcación; soporte 24 x 7 (es decir las 24 horas del día y los siete días de la semana) y servicio al cliente.
- Auditoría del servicio.
- Precios.

En la tabla 5.2, se muestra algunos valores de las especificaciones anteriormente mencionadas, correspondientes a un SP, Cablecom (empresa que opera una red MPLS-IP en la región Suiza), y éstos representan la disponibilidad de clases de desempeño de un servicio particular de una VPN MPLS según los requerimientos de la aplicación del cliente.

Se aplican las siguientes reglas a la especificación y medida del desempeño del servicio [4].

- Las cifras de retardo, *jitter* y descarte son medidas de PE a PE.
- Los descartes en el dispositivo CE y retardos considerados para los enlaces PE a CE no son incluidos dentro de las cifras dadas.
- El retardo es medido con un tamaño máximo del paquete de 128 *bytes*.
- Las cifras de retardo y *jitter* proporcionadas son definidas como los valores garantizados dentro de 99.9%, por ejemplo esto quiere decir que uno de mil paquetes podría exceder el valor máximo especificado.
- La suma del ancho de banda de los servicios de Tiempo Real, Comercial Expreso y Comercial estándar no excederán el 75% del ancho de banda disponible.

Clase de servicio	Cifras de desempeño			Acción si existe congestión	Aplicación típica
	Retardo [ms]	*Jitter* [ms]	*Drop*		
Tiempo real	8	4	1.00 E-4	Descartar	Tiempo real interactivo
Comercial Expreso	14	7	1.00 E-4	Descartar	Tiempo real *streaming*
Comercial estándar	20	10	1.00 E-4	Reclasificar a mejor esfuerzo	Interactivo
Mejor esfuerzo	No aplicable				Servicios *background*

Tabla 5.2: Clases de servicio dadas por un proveedor [4]

Adicionalmente, los SLAs definidas por *Cisco Powered Networks* son [7]: no más de 0.5 % de pérdidas, no más de 60 ms de latencia en una vía de extremo a extremo, y no más de 30 ms en jitter.

La empresa debe evaluar con cuidado las implicaciones del SLA. Por ejemplo, la calidad de servicio (QoS) debería incluirse en el SLA básico. Dado que la VPN de la empresa compartirá con otras la misma red MPLS del proveedor, las garantías de seguridad, prioridad del tráfico y tasa de disponibilidad resultan importantes.

Se debe prestar especial atención a la pérdida de paquetes, capacidad de recuperación, latencia, disponibilidad, mantenimiento y tiempo de reparación. Si el servicio de VPN incluye distintas clases de servicio, será necesario asegurarse de que el contrato de nivel de servicio las contempla.

Como parte del servicio, el cliente debe recibir una herramienta de monitoreo que le permite tener acceso las 24 horas y los 365 días del año al Sistema de Gestión de Red. A través de una página web, el cliente puede monitorear y generar sus reportes sobre las variables críticas como tráfico y ocupación de una determinada conexión de su red. Posteriormente y después de un periodo de monitorización, el tráfico de la VPN MPLS debe adaptarse gradualmente a las necesidades, hasta un mejor afinamiento.

5.2.5.1 Calidad de Servicio

La Calidad de Servicio representa el conjunto de técnicas necesarias para manejar la capacidad del canal, retardo o latencia, *jitter*, y pérdida del paquete. Desde una perspectiva comercial, ésta es esencial para asegurar que las aplicaciones críticas tengan garantizados los recursos de red que ellas necesitan, a pesar del tráfico variante de la red.

La implementación de MPLS convierte las actuales redes IP en redes de Nueva Generación, es decir, redes funcionales multiservicio con la posibilidad de ofrecer servicios diferenciados acordes a la calidad de servicio (QoS) demandada por las distintas aplicaciones de las redes empresariales. Su principal objetivo es crear redes flexibles y escalables con un incremento en el desempeño y la escalabilidad. Esto incluye QoS con múltiples Clases de Servicio (CoS, *Class of Service*).

MPLS permite diferenciar servicios tales como el WWW, el correo electrónico o la transferencia de archivos (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo.

DiffServ es una de las dos arquitecturas de QoS para redes IP definidas por el IETF (*Internet Engineering Task Force*). En este modelo, los paquetes que ingresan a la red DiffServ se agrupan en un pequeño número de clases. Además, cada clase tiene un color o marca asociada con ellos. Esto hace que la clasificación del paquete sea escalable y asegura un apropiado ancho de banda y

garantías de retardo en el centro de la red. Así, cuando los paquetes entran en la red, los paquetes son marcados basados en políticas de clasificación en los nodos de borde de la red.

Una manera escalable de proporcionar los más altos niveles de calidad de servicio con un mínimo de pérdidas de paquetes, es implementar múltiples clases de servicio. La CoS permite a los proveedores categorizar el tráfico en un número manejable de clases de servicio, donde todas las aplicaciones dentro de la clase son tratadas de la misma manera. El SP factura cada clase de servicio apropiadamente, y los subscriptores pueden comprar los servicios que satisfacen sus necesidades, ver la sección 5.3.

5.2.5.2 Determinación de la Calidad de Servicio [7]

Aunque todavía se esté lejos de disfrutar de una calidad de servicio extremo a extremo en todos los casos, es posible obtenerla en redes controladas por un sólo operador. El modo de poder diferenciar el tráfico de cada una de las calidades que se establecen es el marcado de los paquetes IP en los bordes de la red, para después aplicar sobre dichos paquetes, mecanismos de priorización y descarte en función del marcado realizado.

Puesto que la mayoría de los réditos de la empresa vienen de SAP, por consiguiente la empresa dará a esta aplicación comercial un alto nivel de preferencia asignándola a una clase de servicio denominada Oro (Comercial Expreso), por ser una aplicación comercial crítica que no debería admitir mayores retardos (se garantiza un retardo para esta aplicación de 14 ms, ver la tabla 5.2) y necesita tener cierta capacidad del canal garantizada (para la aplicación comercial de SAP se necesita una capacidad de 32 kbps, ver sección 4.2.3.2).

Las aplicaciones como correo electrónico y consultas Web estarán dentro de la clase de servicio denominada Bronce o mejor esfuerzo, para esta clase se asignará como mínimo el 25% de la capacidad total del canal[2], ver la figura 5.7.

---

[2] Este porcentaje del 25% para la clase mejor esfuerzo, es recomendado por Cisco, en su artículo "*Service Provider Quality of Service*" (*Design Guide*), http://www.cisco.com.

Así para las dos sucursales se asigna 32 kbps para la aplicación de SAP (clase Oro), que representa el 50% de la capacidad del canal de las respectivas sucursales, el restante 32 kbps se asignará a la clase de mejor esfuerzo o bronce, el cual representa el 50%, porcentaje superior al recomendado para esta clase (el cual como se indicó correspondía al 25%).

Cosa similar ocurrirá con la matriz, es decir el 50% se dará a SAP (64 kbps), este tráfico se asignará a la clase Oro, ya que la matriz soportará el tráfico generado por esta aplicación procedente de las dos sucursales y los restantes 64 kbps se asignará a la clase de mejor esfuerzo o bronce (cubriendo así el porcentaje mínimo del 25%).

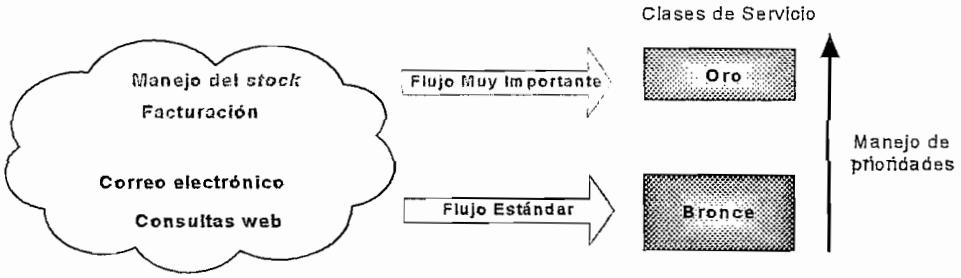


Figura 5.7: Clasificación de los servicios de la VPN de diseño

En la tabla 5.3, se muestran las características de la clase de servicio seleccionada para la oficina matriz y las sucursales.

Clase de Tráfico	Característica	Tipo de tráfico
CoS Oro	Proporciona garantías en retardo y en capacidad de canal.	Aplicación comercial, dada por SAP.
CoS Bronce	Servicio Mejor esfuerzo (*Best effort*).	Navegación por la web, transferencia de archivos, correo electrónico.

Tabla 5.3: Clases de Servicio para la VPN MPLS

Para poder facilitar la calidad buscada a las distintas clases de servicio, se aplican a lo largo de la red una serie de mecanismos, cuyo funcionamiento es necesario

conocer, para luego ser aplicados en la red del proveedor. Dichos mecanismos son:

1. CAR (*Comitted Access Rate*). Este procedimiento, aplicado sobre una interfaz, realiza dos funciones:

   a) Limita la cantidad de tráfico que a través de ella puede ser recibido o enviado.
   b) Incluye en cada paquete entrante la marca indicadora de la calidad de servicio que se le quiere asignar; y, en los paquetes salientes realiza la eliminación de las mismas.

2. CBWFQ (*Class Based Weighted Fair Queue*). Se aplica sobre interfaces de salida de los *routers*, permitiendo dividir todo el ancho de banda disponible entre las clases de servicio existentes. Asignando diferentes pesos a diferentes clases de servicio, un *router* puede manejar el *buffer* y el ancho de banda para cada clase de servicio.

3. WRED (*Weighted Random Early Detection*). Mediante esta técnica se descartan paquetes basados en la precedencia IP o el valor del campo experimental del paquete MPLS de aquellas interfaces próximas al nivel de congestión. Con ello se consigue dos objetivos:

   a) Favorecer las clases de mayor prioridad en situaciones de carga de la red.
   b) No realizar un descarte sistemático de paquetes, que por los mecanismos de retransmisión en TCP/IP llevarían a situaciones de mayor congestión.

La utilización que se realizará de estos mecanismos, sobre los flujos de tráfico existentes, dentro del SP y la red empresarial, es como sigue:

Como se indica en la figura 5.8, se aplica CAR sobre el tráfico entrante al SP, situado en las interfaces de línea de cliente, es decir en los *routers* CE de cada

sitio de la red empresarial, con el objeto de introducir indicadores sobre la calidad de servicio asignada.

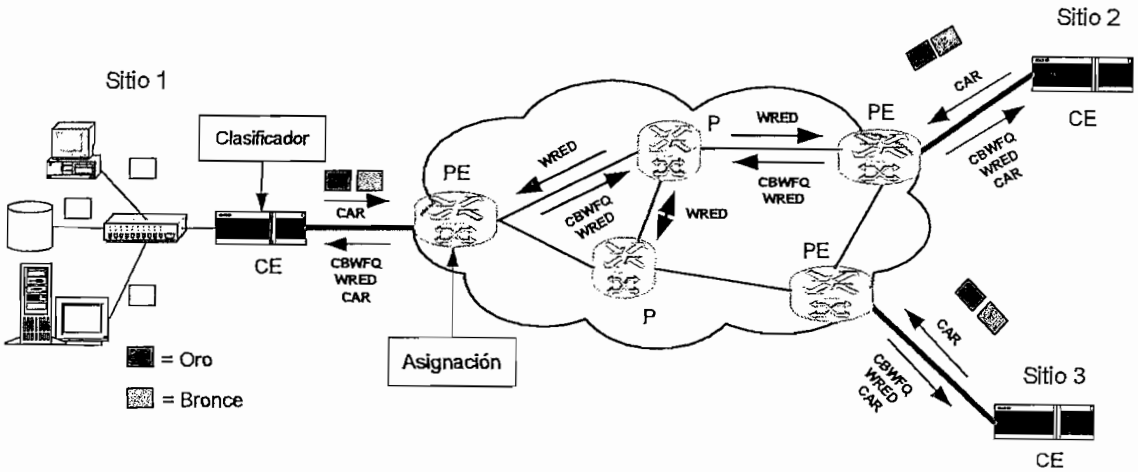


Figura 5.8: Mecanismo de la Calidad de Servicio entre el SP y la red empresarial

En el tráfico saliente del SP es aplicado WRED, conjuntamente con CBWFQ, con el objetivo de facilitar al tráfico de mayor prioridad la llegada a su destino. También es aplicado CAR, en este sentido para eliminar las marcas indicadoras de calidad de servicio utilizadas internamente en la red. En el interior de la red del proveedor, se realiza la aplicación de WRED y CBWFQ conjuntamente. En el sentido contrario del flujo de información, sólo es necesario aplicar WRED, dada la capacidad de conmutación de los *routers* P.

En resumen, cada nodo dentro de la red aplica diferentes puestas en cola y políticas de descarte en cada paquete basado en la marca que transporta el paquete.

Es importante resaltar, que la utilización de estos mecanismos de control de calidad de servicio en el modo indicado, ver la figura 5.8, tiene un carácter provisional. En el futuro, el análisis de su comportamiento en la red cuando esté en pleno funcionamiento, llevarán a modificaciones en la implantación de dichos mecanismos.

Como se vio en la sección 3.5.3, se puede utilizar dos enfoques generales para marcar el tráfico MPLS para manejar la QoS dentro de una red MPLS, en el primer método la información marcada DiffServ se transporta en el campo experimental (EXP) de la cabecera genérica de MPLS. Este campo permite ocho diferentes marcas de QoS. Los LSPs (*Label Switched Paths*) que usan este enfoque son denominados E-LSPs, lo cual significa que la información de QoS se infiere del campo EXP.

Alternativamente, las especificaciones del IETF permiten un segundo método para transportar la información de DiffServ. Aquí, la etiqueta asociada con cada paquete MPLS transporta el marcado de DiffServ que especifica cómo un paquete debe ponerse en cola. La porción de precedencia de descarte del marcado de DiffServ se transporta en el campo EXP, si se usa una cabecera genérica MPLS. Los LSPs dentro de la red MPLS que se usan para este enfoque se denominan L-LSPs, lo cual significa que la información de QoS se infiere, en parte, de la etiqueta MPLS.

En la figura 5.9, se muestra la asignación de prioridades en la configuración del *router* PE, el cual está conectado al *router* CE de la casa matriz.

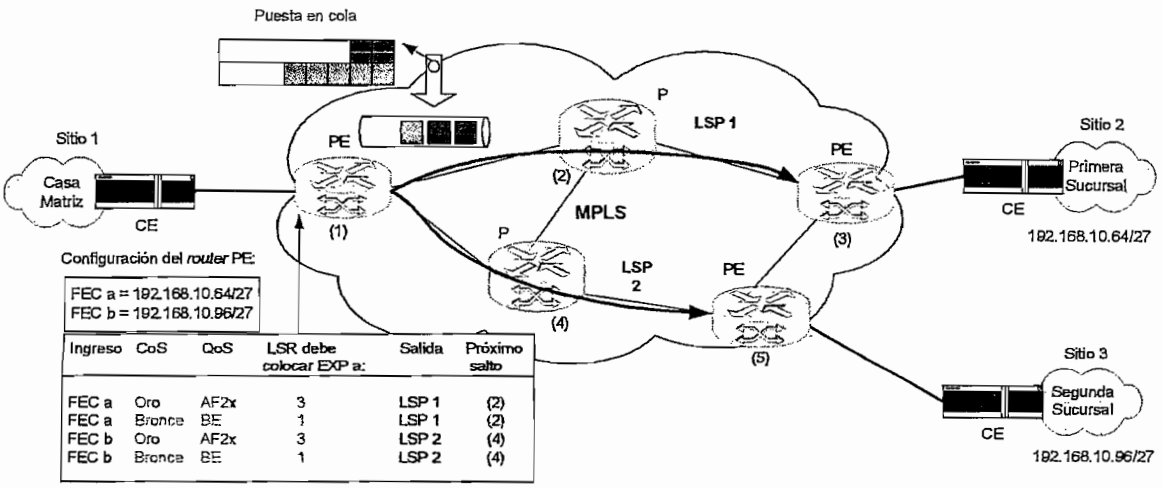


Figura 5.9: Asignación de prioridades en el router PE del proveedor

5.2.6 ASIGNACIÓN DE UN ESPACIO DE DIRECCIONES IP

Puesto que el SP es quien asigna las direcciones IP, es necesario tener en cuenta aspectos del direccionamiento en los dispositivos PE a CE, los cuales son:

1. Las direcciones IP de CE a PE son asignadas por el proveedor contratado.
2. Debido a que se aplica direccionamiento privado, los espacios de direcciones privados usados por el proveedor no serán utilizados dentro de la VPN.

El direccionamiento WAN, es el mismo que se muestra en la tabla 4.15, de igual forma se procede con el direccionamiento LAN.

En la arquitectura VPN MPLS, debido a que la VPN es capaz de usar los mismos prefijos IP que otras VPNs (mientras no se comuniquen), es necesario añadir un distinguidor de ruta (RD, *Route Distinguishers*) a la dirección IPv4 (ver la sección 3.4.1.4). Esto requiere extensiones en el protocolo BGP para que la información de la VPN siga siendo única en el *backbone* VPN MPLS y para que los vecinos BGP puedan identificar las actualizaciones de enrutamiento que no transportan información del prefijo IPv4 estándar. MP-BGP y la información de enrutamiento VPN-IPv4 proporcionan dichas extensiones.

5.2.7 ENRUTAMIENTO

El *router* CE es un dispositivo que proporciona el enrutamiento intrasitio e intersitio en la VPN. Para este último se puede utilizar diferentes protocolos de enrutamiento, como: RIPv2, OSPF y eBGP; y rutas estáticas.

Puesto que solo se tiene un punto de entrada en la red del proveedor, y ya que el tráfico y la topología no varían significativamente, se utilizará enrutamiento estático. Debe configurarse una ruta estática para cada red fuera del *router* CE en la VRF del *router* PE que conecta al sitio de la VPN. Esta información de enrutamiento estático es redistribuida a BGP para ser publicada a través de las sesiones MP-iBGP que conectan los *routers* PE.

5.2.8 EQUIPOS PARA LA VPN MPLS

El equipo en el lado de la empresa es el mismo equipo detallado en el capítulo anterior, ya que la implementación de la VPN MPLS no requiere un *hardware* específico, ni costoso para ser instalado en las oficinas de la empresa.

Este proyecto está basado en las versiones de *software* y de *hardware* que se detallan a continuación.

Debido a que los dispositivos PE y P son parte del proveedor, no se entrará en mayores detalles sobre dicho equipo. Para el diseño se considerará que de parte del proveedor se especifica las siguientes particularidades:

- Cualquier *router* Cisco de la serie 7200 o superior soporta la funcionalidad de un *router* P. Cualquier *router* de la serie 3640 o superior soporta la funcionalidad de un *router* PE, como se aprecia en la tabla 5.4.

Router CE	*Router* PE	*Router* P
Cualquier *router* puede actuar como un dispositivo CE.	Serie 3640	
	Serie 3660	
	Serie 3700	
	Serie 7200	Serie 7200
	Serie 7500	Serie 7500
	Serie 10000	Serie 8540
	Serie 10720	Serie 8800
	Serie 12000	Serie 12000

Tabla 5.4: Tipos de routers Cisco para las VPNs MPLS [5]

- El *software* Cisco IOS® (*Internetworking Operating System*) versión 12.2T que incluye la característica VPN MPLS.
- Para la VPN MPLS de diseño el dispositivo CE será un *router*; se sugiere la marca Cisco, por proporcionar una interoperabilidad del 100% con el SP. Así se puede utilizar los mismos *routers* Cisco 1700 y 1600 que viene utilizando la empresa, ya que pueden intercambiar información de

enrutamiento con el *router* PE e incluso soportan ciertas funciones de QoS requeridas para la realización de la VPN MPLS. Así las características más importantes de dichos *routers* Cisco son:

- Proporciona el *software* Cisco IOS (*Internetworking Operating System*).
- Puertos LAN 10/100 Mbps.
- Asigna ancho de banda a aplicaciones de prioridad, utilizando: CAR, PQ/CBWFQ, RSVP.

En el Anexo C, se puede observar mayores detalles de los *routers* CE.

5.2.9 REQUERIMIENTO PARA EL SERVICIO VPN MPLS

La VPN MPLS es implementada por el SP en su red MPLS. Por lo tanto, para proporcionar el servicio de VPN MPLS, se deben definir, junto con la empresa, aspectos que se indican a continuación.

5.2.9.1 Definición de las VRFs

Para proporcionar el servicio de VPN basado en la arquitectura MPLS se debe definir las tablas VRFs (*VPN Routing and Forwarding*). La relación entre las VPNs, sitios y VRFs puede ser resumida en una regla, la cual se indica a continuación y puede emplearse para cualquier definición de VRF en una red VPN MPLS.

Todos los sitios que comparten la misma información de enrutamiento (esto significa que pertenecen al mismo conjunto de VPNs), que tienen permiso de comunicarse directamente entre sí y que están conectados al mismo router PE pueden ser colocados en una VRF común. [3]

Así, en la arquitectura VPN MPLS, una VPN puede ser vista como una "comunidad de intereses" en la que los miembros de una VPN comparten la

misma información de enrutamiento. Esta información de enrutamiento se coloca en la VRF específica. La misma notación de la tabla 4.1 es utilizada para definir las VRFs correspondientes a cada sitio de la red empresarial, en cada *router* PE de la red MPLS del SP.

5.2.9.2 Definición de los Distinguidores de Ruta

Para la VPN de diseño, cada VRF en la configuración del *router* PE necesita tener un distinguidor de ruta asociado, que esté relacionado al sitio particular de la red empresarial. Así, el distinguidor de ruta es asignado en base a la VRF de la VPN. Esto significa que el valor del distinguidor de ruta será único en cada VRF de la VPN.

Además, es necesario asignar los atributos de *route target* correspondientes, basados en las definiciones de servicio para cada sitio de la red empresarial. Estas *route targets* se utilizarán con las políticas de importación y exportación para cada VRF para proporcionar los requerimientos necesarios de conectividad entre los sitios.

Nombre de la VPN	Distinguidor de ruta	Atributo *Route Target*
Sitio 1	100:25	100:13
Sitio 2	100:26	100:14
Sitio 3	100:27	100:15

Tabla 5.5: Definiciones de los distinguidores de ruta y route targets

Se pueden utilizar los mismos valores para el distinguidor de ruta y la *route target* por VPN. Esto puede ayudar a reducir la complejidad de la configuración, pero puede generar confusión y una mala interpretación del uso de los distinguidores de ruta y las *route targets*. Por lo tanto, se utiliza diferentes valores para los distinguidores de ruta y las *route targets* para cada sitio de la VPN, en la configuración del *backbone* de la VPN MPLS, ver la tabla 5.5. Donde el valor 100 identifica el número del sistema autónomo (asumido).

5.2.9.3 Definición de las políticas de importación y exportación

Se ha visto que cada *router* PE aprende rutas a través del *backbone* VPN MPLS y desde los sitios conectados al cliente. Estas rutas son hechas públicas en tablas de enrutamiento específicas. Cualquier ruta aprendida de los sitios es anunciada a través del *backbone* MPLS usando MP-iBGP; y, cualquier ruta aprendida mediante MP-iBGP se coloca en las VRFs de las partes interesadas. Para lograr esto, cada *router* PE necesita la información que le diga cómo procesar cualquier ruta recibida. La información no solo le dice al *router* PE en qué VRF deben importarse las rutas sino también qué información debería añadir a la ruta cuando sea anunciada a otros *routers* PE.

Cada sucursal de la empresa tiene acceso a la matriz directamente a través del *backbone* del SP. La tabla 5.6, muestra las políticas de importación y exportación utilizadas para la Matriz.

VRF de la oficina Matriz	
Importación y exportación	100:13 (sitio 1)
Importación	100:14 (sitio 2)
Importación	100:15 (sitio 3)

Tabla 5.6: Políticas de importación/exportación de la Matriz

La tabla 5.6, muestra que la VRF de la Matriz exportará sus rutas locales usando el valor de *route target* 100:13, y estas rutas serán importadas por todos los otros sitios de la VPN, es decir en las VRFs de la primera sucursal y segunda sucursal. Las rutas que contiene un valor de *route target* de 100:14 (Sitio 2) ó 100:15 (Sitio 3) serán importadas para permitir la comunicación con los demás sitios.

En cada sitio de la empresa se configurará una ruta estática en la VRF correspondiente apuntando al rango de direcciones IP de los demás sitios de la empresa. Esta ruta estática debe ser redistribuida desde la VRF en MP-BGP para que las direcciones IPv4 puedan ser anunciadas a través de las sesiones MP-iBGP como direcciones VPNv4 para la importación por otros *routers* PE.

La tabla 5.7, muestra las políticas de importación y exportación utilizadas para la Primera sucursal. Esta tabla muestra que la VRF de la Primera Sucursal exportará sus rutas locales usando el valor de *route target* 100:14, y esta ruta será importada en la VRF de la matriz. La ruta que contiene un valor de *route target* de 100:13 (Sitio 1) será importada para permitir la comunicación con la Matriz.

VRF de la Primera sucursal	
Importación y exportación	100:14 (Sitio 2)
Importación	100:13 (Sitio 1)

Tabla 5.7: Políticas de importación/exportación de la Primera Sucursal

La tabla 5.8, muestra las políticas de importación y exportación utilizadas para la Segunda sucursal. Esta tabla muestra que la VRF de la Segunda Sucursal exportará sus rutas locales usando el valor de *route target* 100:15, y esta ruta será importada en la VRF de la matriz. La ruta que contiene un valor de *route target* de 100:13 (Sitio 1) será importada para permitir la comunicación con la Matriz.

VRF de la Segunda sucursal	
Importación y exportación	100:15 (Sitio 3)
Importación	100:13 (Sitio 1)

Tabla 5.8: Políticas de importación/exportación de la Segunda Sucursal

5.2.9.4 Asociación de interfaces a las VRFs

Después de definir todas las VRFs correspondientes en los *routers* PE, es necesario decirle al *router* PE las interfaces que pertenecen a cada VRF, por consiguiente, se debe llenar la VRF con rutas de los sitios conectados.

Cuando la interfaz es asociada con una VRF particular, su dirección IP es removida de la tabla de enrutamiento global y de la interfaz. Esto es debido a que se asume que la dirección no es válida a través de múltiples tablas de

enrutamiento y debería ser reconfigurada después de que la interfaz sea parte de la VRF.

Para los *routers* Cisco, solo las interfaces que ejecutan la conmutación CEF (*Cisco Express Forwarding*) pueden ser asociadas con VRFs, porque el mecanismo de conmutación CEF es un prerrequisito necesario para un envío de datos exitoso al conseguirse una imposición de etiquetas a través del camino de conmutación CEF.

5.2.9.5 MP-iBGP en los *routers* PE

MP-BGP es requerido solo dentro del *backbone* del SP. Así MP-iBGP es requerido dentro de la arquitectura VPN MPLS debido a que la actualización de BGP necesita transportar más información que solo una dirección IPv4. Así en la sección 3.4.1.6.4, se vio que una actualización MP-iBGP contiene una dirección VPN-IPv4, información del etiquetado MPLS, comunidades extendidas BGP y posiblemente comunidades estándares BGP.

Después de llenar la VRF con cualquiera de las rutas de la empresa, estas rutas necesitan ser anunciadas a través del *backbone* VPN MPLS. MP-iBGP realiza este trabajo transportando estas rutas como prefijos VPN-IPv4 a través de sesiones MP-iBGP entre los *routers* PE. Para permitir que esto suceda, el contexto de enrutamiento debe ser configurado en el proceso BGP para decir a BGP qué rutas de la VRF anunciar.

En la figura 5.10, se muestra la VPN MPLS de diseño, como se puede observar la implementación de la VPN MPLS radica en los *routers* PE del SP contratado.

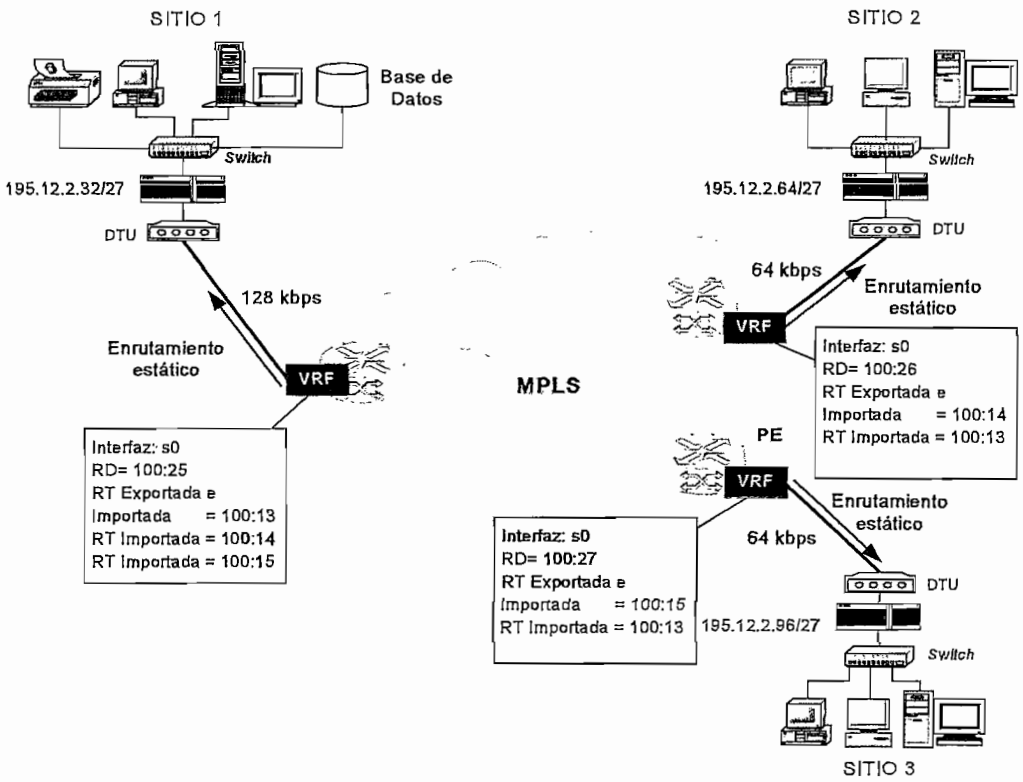


Figura 5.10: VPN basada en MPLS

Adicionalmente se implementa en los *routers* de la red empresarial un *firewall* de filtración de paquetes. El filtrado de paquetes, se instalará en el *router* CE para controlar el tráfico que ingresa en la red, ver la sección 4.2.7.

A continuación se presenta una configuración básica de la VPN MPLS de diseño, dicha configuración tiene lugar en el *router* PE (ver figura 5.11), el cual conecta a la oficina matriz con la red MPLS, así los pasos de configuración son:

- Definir y configurar la VRF respectiva.
- Definir y configurar el distinguidor de ruta.
- Definir y configurar las políticas de importación y exportación.
- Configurar el enlace PE-CE.
- Asociar la interfaz CE a la VRF previamente definida.
- Configurar el Multiprotocolo BGP.

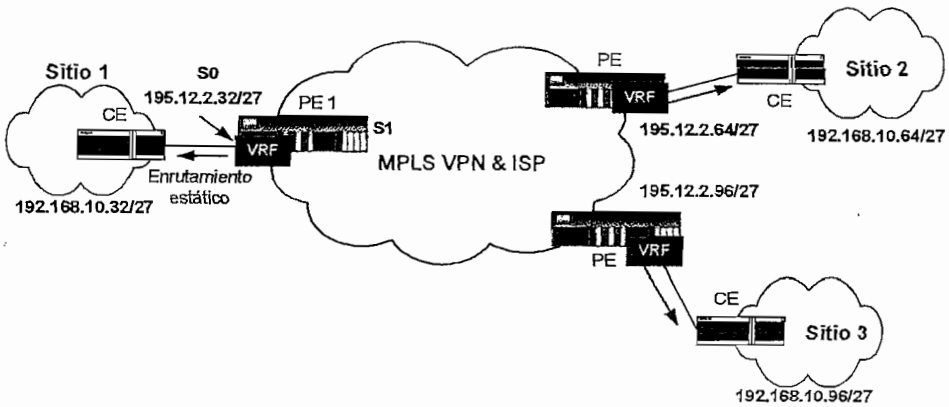


Figura 5.11: Configuración del router PE que conecta a la oficina matriz

```
hostname PE1
!
ip cef
!
ip vrf Sitio 1                          ! Define una VRF
 rd 100:25                              ! Configura el distinguidor de ruta
 route-target both 100:13               ! Configura las route targets para la VRF
 route-target import 100:14
 route-target import 100:15
!
interface loopback0                     ! Se usa como identificador del nodo en MPLS
ip address 194.22.15.2 255.255.255.255
!
interface serial0
 description Matriz
 ip vrf forwarding Sitio 1              ! Asocia la VRF con la interfaz serial
 ip address 195.12.2.33 255.255.255.224
!
interface serial1
 description Backbone
 mpls ip
 ip address 192.168.254.17 255.255.255.224
!
router bgp 100                          ! Configura las sesiones BGP
 no bgp default ipv4-unicast            ! Desactiva los anuncios IPv4 por defecto
 neighbor 194.22.15.3 remote-as 100     ! Define una sesión iBGP con otro router PE
 neighbor 194.22.15.3 update-source loopback0
 neighbor 194.22.15.3 activate
 neighbor 194.22.15.1 remote-as 100
 neighbor 194.22.15.1 update-source loopback0
!
address-family vpnv4
 neighbor 194.22.15.3 activate
! Indica que intercambie rutas en la familia vpn4 con los miembros del backbone
 neighbor 194.22.15.3 send-community extended
 neighbor 194.22.15.1 activate
 neighbor 194.22.15.1 send-community extended
exit-address-family
!
address-family ipv4 vrf Sitio 1
! Se crea la familia de direcciones para la VRF de la Matriz
 redistribute static
! Se redistribuye la ruta estática que define la ruta del cliente
 no auto-summary
exit-address-family
!
ip route vrf Sitio 1 192.168.10.32 255.255.255.224 serial 0
```

!

5.3 COSTOS DE LA VPN MPLS

Esta sección detalla el costo que la empresa debe invertir mensualmente para llevar a cabo la interconexión entre sus sucursales y su oficina matriz utilizando la alternativa de VPNs MPLS, dicho costo abarcará los siguientes elementos: circuitos de acceso, velocidad del puerto y CoS.

Es preciso aclarar que los ISPs utilizan la alternativa Frame Relay o ATM, para que el cliente tenga acceso a los servicios del proveedor. La tecnología de acceso, como se comentó anteriormente, hacia la red MPLS será mediante circuitos virtuales FR.

El cliente requiere el servicio de Internet, para enviar y recibir correo electrónico, bajar archivos, etc, y además el servicio de la VPN MPLS, para el envío de tráfico de la base de datos, por lo que es preciso diferenciar los datos de Internet. Debido a que la VPN MPLS radica en la red del proveedor, el tráfico de Internet deberá ser enviado por un PVC con un DLCI diferente al del tráfico de la VPN MPLS.

Para determinar el costo de un enlace hacia una red MPLS se debe considerar éste como un enlace hacia un servicio del proveedor, por lo que el proveedor cobrará por los enlaces Frame Relay, el servicio de Internet y el servicio de la VPN MPLS[3].

Velocidad de Transmisión (kbps)	Tipo de enlace	Canal de Comunicación Frame Relay (USD)	Costo del servicio de Internet (USD)
32	Local	140	150
64	Local	290	350
128	Local	350	450

Tabla 5.9: Costos de la conexión de acceso e Internet

[3] Es preciso aclarar que este esquema de cobro del servicio VPN MPLS, aquí presentado, podría variar dependiendo del proveedor del servicio.

La tabla 5.9, detalla los precios del medio de comunicación y el servicio de Internet que un ISP cobra a sus clientes mensualmente, como ya se indicó estos precios son por el acceso al servicio.

En la tabla 5.10, se muestra el costo mensual que la empresa debería pagar por concepto de la clase de servicio que recibe por parte del SP, ahora el proveedor ya puede diferenciar la clase de servicio que va a dar a las aplicaciones de la empresa, así se tiene:

	Clase de Servicio (USD)		
Velocidad de transmisión (kbps)	Oro	Plata	Bronce
16	27.85	18.21	7.50
32	49.27	26.78	9.64
64	81.40	38.56	12.85
96	95.32	44.98	14.99
128	127.45	53.55	17.14

Tabla 5.10: Costos mensuales de la Clase de Servicio[4]

La información de la VPN (relacionada con la información de la base de datos) se enviará por un DLCI, hasta alcanzar la red MPLS, esta información será tratada como clase ORO.

La información dirigida al Internet pasará por la red MPLS y se enviará a la nube de Internet, por tal motivo usará otro DLCI y dicha información será tratada como clase Bronce o "*best effort*".

Una vez determinado las clases, ya se pueden cobrar por el servicio prestado por parte del proveedor, ver la tabla 5.11.

[4] Precios referenciales tomados de la empresa Telefónica del Perú, http://www.telefonica-data.com/pe.

Contrato a 3 años			
Sitios	Clase de Servicio	Velocidad de transmisión (kbps)	Costo mensual (USD)
Sitio 1	Oro	64	81.40
	Bronce	64	12.85
Sitio 2	Bronce	32	9.64
Sitio 3	Bronce	32	9.64
TOTAL			113.53

Tabla 5.11: Costo mensual de la Clase de Servicio de la VPN MPLS

El proveedor de la red MPLS/VPN cobrará de la siguiente manera:

Para la matriz, el enlace de 128 kbps será dividido en uno de 64 kbps para datos (VPN MPLS) y otro de 64 kbps para el servicio de Internet. Así, por concepto del enlace local FR (64 kbps) se pagará 290 USD, por acceso a Internet (64 kbps) el costo será 350 USD y adicionalmente se debe pagar por concepto de la CoS (ver tabla 5.11).

Para la primera sucursal, el enlace de 64 kbps, se fraccionará en uno de 32 kbps para datos (VPN MPLS) y otro de 32 kbps para el servicio de Internet. Así, por concepto del enlace local FR (32 kbps) se pagará 140 USD, por acceso a Internet (32 kbps) el costo será 150 USD y adicionalmente se debe pagar por concepto de la CoS. Puesto que la segunda sucursal posee similares características, el costo a pagar será el mismo que el de la primera sucursal.

Resumiendo, por concepto de enlaces locales FR en cada sitio, se tiene: 290 + 140 + 140 = 570 USD. Por concepto de acceso a Internet, se tiene: 350 + 150 + 150 = 650 USD. Por concepto de la CoS, se tiene: 81.40 + 12.85 + 9.64 + 9.64 = 113.53 USD.

En la tabla 5.12, se muestra el costo mensual del enlace, del servicio de Internet para la red empresarial y de la Clase de Servicio.

Servicio	Costo del servicio
Enlaces FR por cada sitio	570
Servicio de Internet por sitio	650
Clase de Servicio	113.53
Total	1333.53

Tabla 5.12: Costo mensual del servicio VPN MPLS para la empresa

El costo a facturar mensualmente es de aproximadamente 1334 dólares. Comparando las soluciones dadas en el capítulo 4 y 5 (ver tabla 5.13), se concluye que el costo mensual por el servicio de la VPN MPLS es comparable que el servicio de la VPN clásica, pero se debe notar que en el caso del servicio VPN MPLS se tiene más opciones para los servicios entregados al cliente, diferenciación del tráfico, y herramientas de control en el lado del SP.

	VPN MPLS	VPN IPSec
Costo mensual (aproximado)	1334 USD	1350 USD

Tabla 5.13 Comparación entre las dos soluciones de VPNs

Así, el precio no siempre es el factor más importante de evaluación y últimamente el aspecto de la seguridad toma mayor prioridad al momento de elegir un tipo de solución para las VPNs.

Una VPN clásica significa implementar varios elementos de seguridad, como adquirir dispositivos especializados (como *firewalls*) y definir políticas de seguridad claras y respetadas.

Mientras que la VPN MPLS es una solución de conectividad IP orientada a la interconexión de redes LAN de la empresa. Este estándar, al igual que la VPN clásica ofrece seguridad, por lo que no necesariamente requiere cifrado. Además, MPLS garantiza la calidad de servicio (QoS) y priorización de ciertos tipos de tráfico.

5.4 COMPARACIÓN ENTRE VPNs BASADAS EN IPSec Y BASADAS EN MPLS

IPSec y MPLS son indudablemente las dos tecnologías principales para construir IP-VPNs. Estas dos tecnologías han sido desarrolladas independientemente una de la otra. Mientras IPSec es particularmente orientado a ocuparse de la seguridad, MPLS está principalmente orientado a cubrir con requisitos tales como: escalabilidad, ingeniería de tráfico y control de la QoS.

De hecho, ambas tecnologías deben tener su campo de acción en las redes del proveedor de servicios. El criterio más claro, aunque no completamente exacto, para definir el campo de aplicación de cada solución es el factor tamaño, IPSec es la opción para ambientes de red pequeños, mientras MPLS se usa cuando la escalabilidad es una preocupación (ambos en términos del tamaño promedio de la red del cliente y el número de clientes). IPSec tiene varios puntos fuertes:

- IPSec es la única tecnología de VPN que soporta cifrado de datos, que es un requisito crucial en los casos donde una VPN atraviesa segmentos de red inseguros (A diferencia de MPLS, que proporciona un nivel de seguridad equivalente al dado por Frame Relay y ATM);
- IPSec no impone ningún requisito especial en el soporte del *backbone* de IP; en principio una VPN basada en IPSec podría desplegarse sobre cualquier red basada en IP (a diferencia de una VPN MPLS, que requiere una infraestructura de *backbone* habilitada para MPLS);
- IPSec proporciona una implementación fácil de una VPN y un tiempo corto para comercializarla (A diferencia de MPLS, que necesita una funcionalidad completa del *backbone* MPLS y requiere un tiempo considerable para implementarla).
- Un VPN basada en túneles de IPSec puede ser, en principio, extendida a cualquier lugar conectado al Internet y está limitada por el alcance de la red del proveedor de servicios.

A pesar de los méritos indicados, las VPNs basadas en IPSec están localizadas en un mercado restringido, éstas típicamente no pueden venderse a empresas grandes u otros portadores. De hecho, MPLS es la única solución factible para soportar implementaciones de IP-VPNs a gran escala (realmente, ésta ha sido probablemente la principal razón para la implementación de esta tecnología debido a un incremento en el número de proveedores de servicios de IP y operadores de red).

En términos de seguridad, las VPNs MPLS no proporcionan cifrado o algún mecanismo de seguridad específico. En todo caso, asumiendo que el proveedor de servicio sea confiable, la seguridad de la VPN está garantizada por el aislamiento de tráfico y dirección, y separación del enrutamiento, aspectos que la mayoría de las implementaciones de VPNs MPLS pueden proporcionar.

En ciertos escenarios de las VPNs, puede usarse IPSec y MPLS como tecnologías complementarias. IPSec debe usarse en casos donde se requiere una fuerte autentificación y confidencialidad (típicamente, acceso remoto a VPNs a través del Internet público o algunas redes no confiables); mientras que MPLS proporciona funciones flexibles de control de la VPN y permite ingeniería de tráfico y diferenciación del tráfico requerido para las implementaciones de grandes VPNs.

La tabla 5.14, muestra un resumen de las características, beneficios y las diferencias entre las VPNs MPLS y las VPNs basadas en IPSec.

	VPN BASADA EN IPSec	VPN BASADA EN MPLS
Modelos de Servicios	Servicios de Internet de alta velocidad, servicio de IP-VPN de calidad para negocios, comercio electrónico y servicios de aplicación.	Servicios de Internet de alta velocidad, servicio de IP-VPN de calidad para negocios, comercio electrónico y servicios de aplicación.
Calidad de Servicio	Depende de la Internet pública para el transporte; solamente puede ofrecer el "caudal disponible" (*best effort*).	Ofrece priorización del tráfico a través de clases de servicio.
Costo	Bajo, dado que utiliza el Internet público para el transporte de datos.	Inferior al del Frame Relay o ATM, aunque superior al de otras IP-VPNs.
Seguridad	Una VPN basada en IPSec proporciona privacidad de datos a través de un conjunto de mecanismos de cifrado y *tunneling* en la capa red de IP.	La arquitectura MPLS separa el tráfico entre clientes ofreciendo seguridad de una manera similar a un ambiente de red confiable como FR o ATM.
Cobertura	Muy extenso, dado que se basa en el acceso a Internet.	Depende de la red MPLS del proveedor de servicios.
Adecuación a aplicaciones	Acceso remoto y móvil seguro. Aplicaciones centradas en IP, como el correo electrónico o Internet. No adecuado para tráfico en tiempo real o de alta prioridad.	Todas las aplicaciones, incluido el *software* empresarial de misión crítica que requiere alta calidad y baja latencia, así como las de tiempo real, como el vídeo y la voz sobre IP (VoIP).
Escalabilidad	El despliegue a gran escala exige planificación y coordinación para dirigir los problemas en la distribución de la clave, administración de claves y configuración con los pares (*peering*).	Alta escalabilidad ya que no se requiere *peering* sitio a sitio. Un despliegue típico de VPN basada en MPLS es capaz de soportar miles de grupos de la VPN sobre la misma red.
Provisión	En general, ninguna provisión de nivel de red es requerida para el ofrecimiento del servicio basado en dispositivos CE.	La activación del servicio requiere simplemente que se proporcione los dispositivos de borde del cliente (CE) y los dispositivos de borde del proveedor (PE) para permitir que el sitio se vuelva un miembro de un grupo de una VPN MPLS.
Transparencia	Una VPN basada en IPSec reside en la capa de red, es transparente a las aplicaciones.	Una VPN basada en MPLS opera en un ambiente IP; es completamente transparente a las aplicaciones.
Participación del cliente	Requiere *software* o *hardware* del cliente	No requiere ninguna. Una VPN basada en MPLS es un servicio de VPN basada en dispositivos PE o de Red.

Tabla 5.14: Diferencias entre las VPNs basadas en IPSec y basadas en MPLS [5]

	VPN BASADA EN IPSec	VPN BASADA EN MPLS
Implementación del servicio	Tiempo rápido para comercializarse; puede implementarse a través de una red IP existente.	Requiere la participación de los elementos de red en el centro y borde para habilitar MPLS.
Sesión de Autentificación	Cada sesión de IPSec debe autentificarse mediante un certificado digital o clave precompartida; los paquetes que no están de acuerdo con la política de seguridad se descartan.	El número de miembros de la VPN es determinado por el SP, basado en un puerto lógico y un único distinguidor de ruta; el acceso no autorizado a un grupo de la VPN es negado por la configuración del dispositivo.
Localización en la Red *	En el lazo local, el borde y fuera de la red del SP (*off-net*), donde existe un alto grado de exposición de la privacidad de los datos y donde los mecanismos de seguridad de IPSec tales como *tunneling* y cifrado pueden aplicarse mejor.	En el núcleo de la red del SP, donde la QoS, la ingeniería de tráfico y la utilización del ancho de banda pueden controlarse, sobre todo si un SLA es ofrecido como parte del servicio de VPN.

* Ver la figura 5.12. IPSec es aplicado en el lazo local, el borde y fuera de la red del SP, mientras MPLS es aplicado en el núcleo de la red del SP.

Tabla 5.14: Diferencias entre las VPNs basadas en IPSec y basadas en MPLS (continuación)

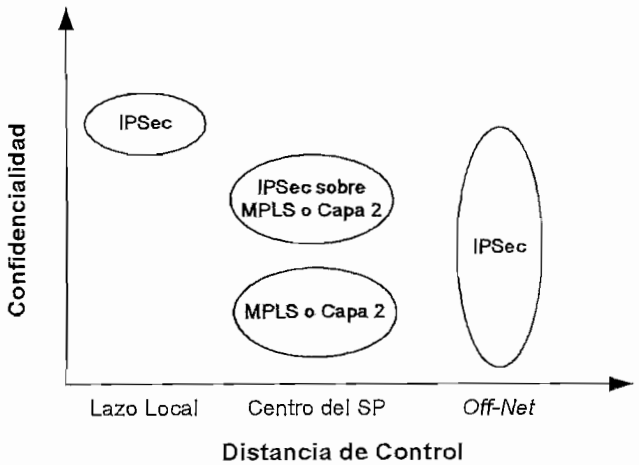


Figura 5.12: Localización en la red para VPNs basadas en MPLS e IPSec [5]

BIBLIOGRAFÍA – CAPÍTULO 5

[1] ROSEN E. y Otros, "BGP/MPLS VPNs", IETF draft, draft-ietf-ppvpn-rfc2547bis-03.txt, Octubre 2002 (trabajo en progreso).

[2] CARUGI M. y Otros, "*Service requirements for Layer 3 Provider Provisioned Virtual Private Networks*", IETF draft, draft-ietf-ppvpn-requirements-05.txt, Octubre 2002 (trabajo en progreso).

[3] GUICHARD Jim y PEPELNJAK Ivan, "*MPLS and VPN Architectures: A practical guide to understanding, designing and deploying MPLS and MPLS-enabled VPNs*", Cisco Press, 2001.

[4] CABLECOM, "*Service Level Agreement MPLS-IP VPN Services*", http://www.cablecom.net.

[5] CISCO SYSTEMS, "*A Comparison Between IPSec and Multiprotocol Label Switching Virtual Private Networks*", http://www.cisco.com.

[6] REPIQUET Joël, "*Keep it Simple with BGP/MPLS Virtual Private Networks*", http://www.lambdanet.net.

[7] CISCO SYSTEMS, "*Service Provider Quality of Service*", http://www.cisco.com.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

Una red privada virtual (VPN, *Virtual Private Network*) es una red privada de datos que hace uso de una infraestructura pública de telecomunicaciones, manteniendo la privacidad a través del uso de un protocolo de *tunneling* y procedimientos de seguridad.

Una red privada virtual puede compararse con un sistema de líneas arrendadas que solo pueden ser utilizados por una compañía. El principal propósito de una VPN es dar a una empresa las mismas capacidades que las líneas arrendadas privadas, pero a un bajo costo, usando una infraestructura pública compartida.

Los servicios de VPN pueden abarcar una variedad de tecnologías y topologías. Las VPNs pueden clasificarse de diversas formas, así: el problema comercial que una VPN va a solucionar, la capa OSI en la cual el SP intercambia la información de topología con el cliente, la tecnología de capa 2 o capa 3 empleada para implementar el servicio VPN dentro de la red del SP y la topología de la red.

Las VPNs clásicas confían en una encapsulación (*tunneling*) y un modelo de cifrado para un transporte seguro de los datos entre dos o más localidades. Este tipo de VPNs es un conjunto de túneles punto a punto sobre una red IP existente. Así, existen diferentes protocolos para este tipo de VPNs como: PPTP, L2TP e IPSec. Todos ellos confían en el concepto de *tunneling* de alguna forma y normalmente emplean cifrado.

IPSec es un protocolo de capa 3 resultando totalmente transparente a las aplicaciones. Así, es posible el uso de redes IP para aplicaciones críticas, como las transacciones comerciales entre empresas. Al mismo tiempo, es la solución ideal para aquellos escenarios en que se requiera seguridad, independientemente

de la aplicación, de modo que es una pieza esencial en la seguridad de las redes IP.

Para la VPN clásica de diseño, se contempla una solución sitio a sitio basada en *hardware* en este caso utilizando *routers*. El dimensionamiento de la capacidad del canal a contratar o la conservación del canal que ya se tiene, se ve influenciado por apreciaciones estadísticas sobre el uso simultáneo del túnel por parte de los usuarios. Por ejemplo es posible que se necesite el mismo ancho de banda para interconectar oficinas que tienen 3 usuarios cada una pero que acceden continuamente a la base de datos o intercambian archivos constantemente, que el necesario para unir oficinas con 30 usuarios cada una pero que rara vez acceden a los recursos remotos o que tienen aplicaciones en modo texto.

En general una VPN clásica proporciona mecanismos de autentificación, administración de direcciones, cifrado de datos (confidencialidad), y administración de claves. Así, para el diseño de la VPN clásica, la autentificación viene dada por el protocolo IPSec. Además se considera como una segunda línea de defensa utilizando el filtrado de paquetes, después que los paquetes son autentificados por IPSec. La administración de direcciones es necesaria para asignar una dirección al cliente en la red privada. La confidencialidad viene dada por el protocolo ESP, ayudado por el algoritmo DES (56 bits). La administración de claves vendrá dada por IKE, para identificar al par se usa claves precompartidas.

Los principales factores de crecimiento que impulsan a las VPNs clásicas, han sido la cobertura que ha alcanzado Internet y la disminución en los precios de acceso, propiciado por la demanda del mercado.

MPLS es el último paso en la evolución de la tecnología de conmutación multinivel para el núcleo de Internet. Éste es un enfoque basado en estándares del IETF, construido a partir de las lecciones aprendidas de varias soluciones de conmutación multinivel de varios propietarios. MPLS combina el uso de la

sustitución de etiquetas en el plano de datos con el enrutamiento IP y señalización estándar basada en IP y protocolos de distribución de etiquetas en el plano de control. Además, MPLS fue específicamente diseñado para ejecutarse sobre cualquier tecnología de capa 2, facilitando la migración a la próxima generación de Internet.

MPLS aparece como una solución para proporcionar Ingeniería de tráfico, Calidad de Servicio y Redes Privadas Virtuales. MPLS es una solución con grandes posibilidades de éxito debido al hecho de poder migrar una red actual (FR, ATM,...) a MPLS, siendo el primer paso la coexistencia entre ellas mediante *software* añadido a los equipos actuales.

MPLS se integra adecuadamente con BGP, el cual distribuye la información de accesibilidad entre los pares BGP, permitiendo a cada sitio BGP aprender de los pares que pertenecen a la misma VPN. Ya que los pares BGP intercambian etiquetas para cada uno de los sitios de la VPN, cada sitio BGP puede establecer automáticamente túneles MPLS (LSPs) conteniendo LSPs específicos de la VPN a sus pares que pertenecen a la misma VPN. Consecuentemente, MPLS proporciona un mallado completo de conectividad VPN a través de una red IP compartida.

MPLS y DiffServ son soluciones complementarias para el problema de proporcionar diferentes niveles de servicio en una sola red. DiffServ define diferentes comportamientos en los nodos mientras MPLS versa sobre los caminos entre los diferentes nodos.

Con la *introducción* de nuevas tecnologías en las redes de los SPs y los nuevos requerimientos de los clientes, el concepto de VPN se vuelve cada vez más complejo. Así, las VPNs están haciendo que los proveedores de transporte de datos migren sus redes a un híbrido entre IP y las tecnologías tradicionales de conmutación de paquetes. Los ISPs están mejor ubicados para explotar este mercado, pues tienen experiencia con IP desde hace un tiempo atrás y tienen la

infraestructura adecuada para que con un mínimo de inversión, puedan proporcionar este servicio sin mayores inconvenientes.

El servicio de la VPN MPLS de diseño es establecido a través del uso de VRFs en las cuales se coloca la información de enrutamiento específica del cliente a través de mecanismos de importación que utilizan la comunidad extendida BGP de *Route Target*. Esta información de enrutamiento se identifica únicamente a través del uso de un distinguidor de ruta (RD) y es distribuida entre los *routers* PE, mediante el uso de extensiones multiprotocolo BGP.

La VPN MPLS de diseño no solo permite seguir usando los espacios de direcciones IP privados, y la empresa no tiene que ocuparse de las cuestiones del enrutamiento intersitio ya que éstas son responsabilidades del SP y pese a que el SP maneja la VPN, las políticas que determinan si un sitio específico es un miembro de la VPN de la empresa siguen siendo políticas de la misma. Así la VPN MPLS permite que las políticas de la empresa sean implementadas por el SP trabajando junto con la empresa.

La VPN MPLS de diseño permite conectar distintas oficinas con seguridad ofreciendo calidad de servicio (QoS) de nivel empresarial. A medida que la empresa despliegue este tipo de red en un número cada vez mayor de sitios, las IP-VPNs se vuelven necesarias para interconectar las redes de forma transparente. Además, la entrada esperada de la videoconferencia podría venir impulsada por el crecimiento de las redes IP de área extensa, que faciliten la utilización y configuración de este tipo de transmisiones como si se trataran de una llamada de voz.

La empresa, no considera tener su propia red MPLS, ya que la naturaleza de la empresa no es brindar servicios de transmisión de datos, además eso implicaría costos adicionales por concepto de arrendar enlaces a terceros, adquisición de equipos, etc.

Principalmente al momento de decidir entre las dos soluciones presentadas en este proyecto, el precio no necesariamente debe influir para tomar cualquiera de las dos opciones, hay que tener en cuenta otros parámetros, principalmente la seguridad, ya que en las VPNs clásicas es recomendable un fuerte cifrado y una autentificación adecuada, y además es muy difícil mantener una calidad de servicio extremo a extremo.

Aunque las VPNs MPLS compiten directamente con las tecnologías de red tradicionales existentes como Frame Relay o ATM, también se puede recurrir a utilizarlas en modo solapado. Así, la empresa utiliza una red MPLS basada en una tecnología de acceso tradicional, circuitos Frame Relay, en todos sus emplazamientos. De este modo, la empresa conserva las inversiones realizadas en tecnologías tradicionales.

Existen pocas dudas acerca del hecho de que MPLS en el extremo de la red vaya a seguir adentrándose en el mercado de Frame Relay y ATM. Mientras tanto, MPLS va en camino de convertirse en el estándar de facto para el núcleo. Las VPNs IPSec coexistirán con MPLS en las empresas que no requieran mayor calidad de servicio, pero que sí se vean en la obligación de permitir a sus usuarios conectarse de forma segura a la red empresarial.

Puesto que en el Ecuador aún no se tienen los servicios prestados por VPNs sobre MPLS, este proyecto presenta costos referenciales de países en donde se tiene dicha tecnología y se han tomado como base estas referencias para realizar los costos de dichos servicios.

No se realizaron la revisión de configuraciones en otras plataformas, principalmente debido a que la plataforma Cisco ofrece herramientas de configuración flexibles y opciones de configuración para el desarrollo del proyecto. Pero el empleo de equipos Cisco, no necesariamente es obligatorio en el lado del cliente, ya que MPLS reside en el *backbone* de la red del SP, el cliente no requiere necesariamente actualizaciones en el *software* del equipo, ni tampoco

necesita de un cambio de equipos; el cliente físicamente no experimenta cambios en su red, la empresa ve los cambios en los servicios prestados.

RECOMENDACIONES:

Cuando se tenga la red en pleno funcionamiento es recomendable realizar una medición del tráfico generado por cada sitio de la VPN, esto es para realizar las correcciones necesarias tales como: en la capacidad del canal contratado, actualización del *hardware* o *software* del equipo usado en la VPN, principalmente el *router* CE. Podría recomendarse que los enlaces sean sobredimensionados principalmente para garantizar el cumplimiento de una SLA, pero esto implica incurrir en costos adicionales.

Un aspecto importante de las IP-VPNs consiste en el hecho de que la separación tradicional entre voz y datos está desapareciendo gracias a las empresas que desean utilizar la misma red para ambos tipos de tráfico, por lo cual, es recomendable realizar un diseño, en el cual se incorpore tecnologías como voz sobre IP y videoconferencia, aplicadas sobre las redes empresariales y se le de la adecuada calidad de servicio.

Se recomienda realizar un estudio en la Escuela Politécnica Nacional para implementar una VPN que permita el acceso remoto al personal administrativo, docente y estudiantil a la red privada de la EPN. Este estudio podría incluir la implementación de una solución de voz sobre IP y videoconferencia privada.

Se recomienda hacer de la Escuela Politécnica Nacional, si se tuviera el apoyo económico, un *backbone* VPN MPLS, así como de un ISP tal como se tiene en otras universidades del país, de esta manera explotar los servicios de la tecnología MPLS.

También se recomienda realizar estudios sobre las nuevas aplicaciones sobre MPLS en redes ópticas, redes inalámbricas, voz sobre MPLS (VoMPLS), además de otras soluciones presentadas por otros fabricantes muy parecidas a MPLS.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS:

- BROWN Steven, "Implementación de Redes Privadas Virtuales", Editorial McGraw-Hill, 2000.
- GUICHARD Jim y PEPELNJAK Ivan, "*MPLS and VPN Architectures: A practical guide to understanding, designing and deploying MPLS and MPLS-enabled VPNs*", Cisco Press, 2001.
- KARANJIT Siyan, "Microsoft Windows 2000 TCP/IP", Editorial Prentice Hall PTR, Madrid.
- KOSIUR Dave, "*Building and Managing Virtual Private Networks*", 1era edición, Editorial Wyley, 1998.
- MURHAMMER Martin W, "*A guide to Virtual Private Networks*", Editorial Prentice Hall PTR, 1998.
- STALLINGS William, "Comunicaciones y Redes de computadoras", 5ta edición, Editorial Prentice Hall PTR.
- SACKETT C. George, "Manual de *routers* Cisco", Editorial McGraw-Hill, 2002.
- TANENBAUM Andrew, "Redes y Ordenadores", Editorial Prentice Hall, 1996.

ARTÍCULO:

- VISWANATHAN, A., FELDMAN N., WANG Z., CALLON R., "*Evolution of Multiprotocol Label Switching*", *IEEE Communications Magazine,* Vol. 36, No. 5, Mayo 1998.

DOCUMENTOS EN FORMATO ELECTRÓNICO:

- CISCO SYSTEMS, "*MPLS Virtual Private Networks*", http://www.cisco.com.
- CISCO SYSTEMS, *"A Comparison Between IPSec and Multiprotocol Label Switching Virtual Private Networks",* http://www.cisco.com.

- CISCO SYSTEMS, "*Service Provider Quality of Service*", http://www.cisco.com.
- FERGUSON P., HUSTON G., "*What is a VPN?*", http://www.cisco.com.
- FIM LSIIS, "MPLS. INGENIERÍA DE TRÁFICO Y RPV DE PROVEEDOR", 2002.
- OJA Jari y Otros, "*IP Virtual Private*", http://www.eurescom.de.
- REPIQUET Joël, "*Keep it Simple with BGP/MPLS Virtual Private Networks*", http://www.lambdanet.net.
- MICROSOFT CORPORATION, "*Understanding Point-to-Point Tunneling Protocol (PPTP)*", http://www.microsoft.com.
- PULLEY R. y CHRISTENSEN P., "*A Comparison Of MPLS Traffic Engineering Initiatives*", NETPLANE Systems, http://www.netplane.com.

RFC (*Request For Comments*):

- ANDERSSON L. y Otros, "*LDP Specification*", RFC 3036, Enero 2001.
- AWDUCHE D. y Otros, "RSVP-TE: *Extensions to RSVP for LSP Tunnels*", RFC 3209, Diciembre 2001.
- BATES T., REKHTER Y., CHANDRA R., y KATZ D., "*Multiprotocol Extensions for BGP-4*", RFC 2858, Junio 2000.
- BLAKE S. y Otros, "*An Architecture for Differentiated Services*", RFC 2475, Diciembre 1998.
- BRADEN R. y Otros, "*Resource ReSerVation Protocol* (RSVP)--*Version 1 Functional Specification*", RFC 2205, Septiembre 1997.
- HAMZEH K. y Otros, "*Point-to-Point Tunneling Protocol* (PPTP)", RFC 2637, Julio 1999.
- HARKINS D., CARREL D., "*The Internet Key Exchange* (IKE)", RFC 2409, Noviembre1998.
- JAMOUSSI B., y Otros, "*Constraint-based LSP Setup Using LDP*", RFC 3212, Enero 2002.
- KALISKI B., "*The MD2 Message - Digest Algorithm*", RFC 1319, Abril 1992.

- KENT S., ATKINSON R., "*Security Architecture for the Internet Protocol*", RFC 2401, Noviembre 1998.
- KENT S., ATKINSON R., "*IP Authentication Header*", RFC 2402, Noviembre 1998.
- KENT S., ATKINSON R., "*IP Encapsulating Security Payload* (ESP)", RFC 2406, Noviembre 1998.
- LE FAUCHEUR F. y Otros, "*MPLS Support for Differentiated Services*", RFC 3270, Mayo 2002.
- MAUGHAN D. y Otros, "*Internet Security Association and Key Management Protocol* (ISAKMP)", RFC 2408, Noviembre 1998.
- ORMAN H., "*The OAKLEY Key Determination Protocol*", RFC 2412, Noviembre 1998.
- REKHTER Y., Li T., "*A Border Gateway Protocol 4* (BGP-4)", RFC 1771, Marzo 1995.
- RIVEST R., "*The MD5 Message - Digest Algorithm* ", RFC 1321, Abril 1992.
- ROSEN E., VISWANATHAN A. y CALLON R., "*Multiprotocol Label Switching Architecture*", RFC 3031, Enero 2001
- TOWNSLEY W. y VALENCIA A., "*Layer Two Tunneling Protocol* L2TP", RFC 2661, Agosto 1999.
- VALENCIA A., LITTLEWOOD M., KOLAR T., *Cisco Layer Two Forwarding (Protocol)* "L2F", RFC 2341, Mayo 1998.

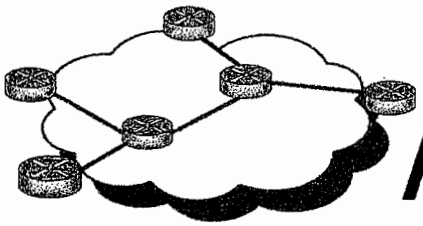
INTERNET-*DRAFTS*:

- CALLON R. y Otros, "*A Framework for Layer 3 Provider Provisioned Virtual Private Networks*", IETF draft, draft-ietf-ppvpn-framework-07.txt, Enero 2003 (trabajo en progreso).
- KOMPELLA K. y Otros, "*Layer 2 VPNs Over Tunnels*", IETF draft, draft-kompella-ppvpn-l2vpn-02.txt, Noviembre 2001 (trabajo en progreso).
- LE FAUCHEUR F. y Otros, "*Requirements for support of DiffServ-aware MPLS Traffic Engineering*", IETF draft, draft-ietf-tewg-diff-te-reqts-06.txt, Septiembre 2002 (trabajo en progreso).

- MARTINI L. y Otros, "*Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*", IETF draft, draft-martini-l2circuit-encap-mpls-05.txt, Abril 2003 (trabajo en progreso).
- MARTINI L. y Otros, "*Transport of Layer 2 Frames Over MPLS*", IETF draft, draft-martini-l2circuit-trans-mpls-11.txt, Abril 2003 (trabajo en progreso).
- ROSEN E. y Otros, "BGP/MPLS VPNs", IETF draft, draft-ietf-ppvpn-rfc2547bis-03.txt, Octubre 2002 (trabajo en progreso).

PÁGINAS WEBS:

- www.ietf.org/html.charters/mpls-charter.html
- www.ietf.org/internet-drafts/
- www.mplrsc.com
- www.mplsforum.org
- www.cisco.com
- www.juniper.net
- www.nortelnetworks.com
- www.riverstone.com
- www.spirent.com
- www.agilent.com
- www.cosinecom.com
- www.dataconnection.com
- www.lambdanet.net
- www.netplane.com



ANEXOS

ANEXO A

A.1 PROTOCOLOS DE ENRUTAMIENTO

En un conjunto de redes, los dispositivos de enrutamiento son responsables de recibir y reenviar los paquetes a través del conjunto de redes interconectadas. Cada dispositivo de enrutamiento realiza la decisión del enrutamiento basándose en el conocimiento que se tiene sobre la topología y las condiciones del conjunto de redes. Una red con un número mínimo de *routers* puede ser configurada con enrutamiento estático. Una tabla de enrutamiento estático es construida manualmente, es decir, por el administrador de la red. Las tablas de enrutamiento estático no se ajustan a los cambios de la red, ellos trabajan mejor cuando las rutas no cambian y el destino final debe ser conocido.

Antes de seguir adelante se debe establecer la diferencia entre enrutamiento y protocolos de enrutamiento. Enrutamiento es el acto de reenviar paquetes basados en la información de las tablas de enrutamiento. Los protocolos de enrutamiento se encargan de intercambiar la información usada para construir las tablas de enrutamiento.

Una red con más de una posible ruta al mismo destino podría utilizar enrutamiento dinámico. Una ruta dinámica es construida usando la información intercambiada por los protocolos de enrutamiento. Los protocolos son diseñados para distribuir información que dinámicamente ajustan las rutas reflejadas en las condiciones de la red. Los protocolos de enrutamiento no solo están diseñados para cambiar a una ruta de respaldo cuando la ruta primaria se vuelve inoperante sino que ellos también evalúan y deciden cual es la mejor ruta para un destino.

Para proceder a discutir los protocolos de enrutamiento, es necesario introducir el concepto de sistema autónomo (AS, *Autonomous System*). Un sistema autónomo es un conjunto de redes conectado por dispositivos de enrutamiento homogéneos; normalmente estos dispositivos de enrutamiento están bajo el control administrativo de una única entidad.

Los protocolos de enrutamiento se pueden dividir en dos grupos generales: protocolos de enrutamiento interior y exterior.

A.1.1 IGPs (*INTERIOR GATEWAY PROTOCOLS*)

Son usados para intercambiar información de enrutamiento entre *routers* dentro de un sistema autónomo. Entre ellos se encuentran: **RIP**, **IGRP** y **OSPF**. Todos los **IGP** cumplen la misma función, determinar la ruta óptima de destino, para ello utilizan diferentes algoritmos los cuales se pueden definir en dos:

- Protocolos de enrutamiento por Vector Distancia, y
- Protocolos de enrutamiento del Estado de Enlace.

Protocolos de enrutamiento por Vector Distancia: En este protocolo cada *router* conoce las rutas a las diferentes subredes y la métrica asociada a esa ruta. Cada *router* envía a sus vecinos información de toda la red. Este protocolo considera que la mejor ruta es aquella que tiene menor métrica. La métrica puede representar el número de saltos o *routers* intermedios. Periódicamente cada *router* envía su tabla de rutas a todos sus vecinos. Ellos calculan sus propias tablas con esta información y con los datos locales. Uno de estos protocolos es **RIP** (*Route Information Protocol*). Éste acepta un máximo de 15 saltos; si existe una ruta con más de esta distancia dicho protocolo la considera como inalcanzable. Esto significa, que en un sistema autónomo que tenga una ruta con más de 15 *routers* no puede usarse RIP.

Protocolos de enrutamiento del Estado de Enlace: Cada *router* mantiene un mapa interno de toda la topología de la red y envía información a toda la red acerca de cuales son sus vecinos. Periódicamente intercambia mensajes con sus vecinos para asegurarse que sus conexiones están bien. Si falla una conexión, envía un mensaje con el nuevo estado a los vecinos alcanzables quienes lo propagan a los demás. Todos redefinen sus tablas de enrutamiento en base a la nueva información. Como ejemplo de estos protocolos se puede mencionar al protocolo **OSPF** (*Open Shortest Path First*), el cual escoge como el mejor camino

el de costo mínimo, donde el costo se puede definir como tiempo de transmisión, número de saltos, etc. En este protocolo cada *router* mantiene una base de datos que describe la topología completa del sistema autónomo.

A.1.2 EGPs (*EXTERIOR GATEWAY PROTOCOLS*)

Son utilizados para intercambiar información de enrutamiento entre diferentes sistemas autónomos en donde cada *router* es responsable de la información de su propio sistema. Como ejemplo de este protocolo podemos citar a **BGP** (*Border Gateway Protocol*) y **EGP** (*Exterior Gateway Protocol*). BGP es el reemplazo para el antiguo EGP (no confundirlo con los protocolos de *gateway* exteriores en general) que se empleaba en ARPANET.

A.2 PROTOCOLO RIP (*ROUTING INFORMATION PROTOCOL*)

Uno de los IGPs más ampliamente utilizados es el RIP. El protocolo RIP es consecuencia directa de la implantación del ruteo de vector distancia para redes locales. En principio, divide las máquinas participantes en activas o pasivas (silenciosas). Los *routers* activos anuncian sus rutas a los otros; las máquinas pasivas listan y actualizan sus rutas con base a estos anuncios. Solo un *router* puede correr RIP en modo activo de modo que un anfitrión deberá correr RIP en modo pasivo.

Un *router* con RIP en activo difunde un mensaje cada 30 segundos, éste mensaje contiene información tomada de la base de datos de ruteo actualizada. Cada mensaje consiste en pares, donde cada par contiene una dirección IP y un entero que representa la distancia hacia esta red.

RIP por tanto hace uso de un vector de distancias, con una métrica por número de saltos donde se considera que 16 saltos o más es infinito. De esta manera, el número de saltos (*hops number*) o el contador de saltos (*hop count*) a lo largo de una trayectoria desde una fuente dada hacia un destino dado hace referencia al número de *routers* que un datagrama encontrará a lo largo de su trayectoria. Por

tanto lo que se hace es utilizar el conteo de saltos para calcular la trayectoria óptima.

Para prevenir que dos *routers* oscilen entre dos o más trayectorias de costos iguales, RIP específica que se deben conservar las rutas existentes hasta que aparezca una ruta nueva con un costo estrictamente menor.

Si falla el primer *router* que anuncia la ruta RIP específica que todas las escuchas deben asociar un tiempo límite a las rutas que aprenden por medio de RIP. Cuando un *router* instala una ruta en su tabla, inicia un temporizador para tal ruta. Este tiempo debe iniciarse cada vez que el *router* recibe otro mensaje RIP anunciando la ruta. La ruta queda invalidada si transcurren 180 segundos sin que el *router* haya recibido un anuncio nuevamente.

RIP debe manejar tres tipos de errores ocasionados por los algoritmos subyacentes. En primer lugar, dado que el algoritmo no especifica detección de ciclos de ruteo, RIP debe asumir que los participantes son confiables o deberá tomar precauciones para prevenir los ciclos. En segundo lugar, para prevenir inestabilidades, RIP debe utilizar un valor bajo para la distancia máxima posible (RIP utiliza 16 saltos como medida máxima). Esto implica que para una red como Internet, los administradores deben dividirla en secciones o utilizar un protocolo alternativo. En tercer lugar, el algoritmo vector distancia empleado por RIP crea un problema de convergencia lenta o conteo al infinito, problema en el cual aparecerán inconsistencias, debido a que los mensajes de actualización de ruteo se difunden lentamente a través de la red. Seleccionando un infinito pequeño (16) se ayuda a limitar la convergencia lenta, pero no se elimina.

La inconsistencia en la tabla de ruteo no es exclusiva de RIP, éste es un problema fundamental que se presenta en todo protocolo con algoritmos vector distancia, en el que los mensajes de actualización transportan únicamente pares de redes de destino y distancias hacia estas redes.

Es posible resolver el problema de la convergencia lenta mediante una técnica conocida como actualización de horizonte separado (*split horizon update*). Cuando se utilizan horizontes separados, un *router* registra la interfaz por la que ha recibido una ruta particular y no difunde la información acerca de la ruta de regreso sobre la misma interfaz. Con esto se evita que la información "negativa" no sea difundida con rapidez.

Una de las técnicas finales para resolver el problema de la convergencia lenta se conoce como *Poison Reverse*. Una vez que una conexión desaparece, el *router* anuncia la conexión conservando la entrada de información por varios periodos de actualización e incluye un costo infinito en la difusión. Para hacer el *Poison Reverse* más efectivo, se debe combinar con las *Triggered Updates* (actualizaciones activadas) que obligan al *router* a que envíe una difusión inmediatamente al recibir "malas noticias", en lugar de esperar el próximo periodo de difusión. Al enviar una actualización inmediatamente, un *router* minimiza el tiempo en que es vulnerable por recibir "buenas noticias".

A.3 OSPF (*OPEN SHORTEST PATH FIRST*)

OSPF (*Open Shortest Path First*, Abrir Primero el Camino más corto), es una alternativa más reciente a RIP entre los protocolos de enrutamiento internos y que corrige todas las limitaciones que tenía éste. OSPF es un protocolo de estado de enlace y de dominio público, definido en el RFC 2328. OSPF provee una rápida convergencia y soporta máscaras de subred de longitud variable. Desde un punto de vista práctico, la diferencia más importante es que un protocolo del estado de enlace converge con mayor rapidez que un protocolo por vector de distancia. Por convergencia se entiende que la estabilización después de cambios en la red, como caídas de *router* o de enlaces.

OSPF comparte información acerca de sus vecinos a una red entera, es decir solo en su sistema autónomo. El trabajo de OSPF no es informar a todos los sistemas autónomos de Internet, su trabajo es construir las rutas dentro de un sistema

autónomo. OSPF perfecciona esta tarea definiendo una jerarquía de áreas de enrutamiento dentro de un sistema autónomo y éstas son:

Áreas: Una área es una colección arbitraria de interconexión de redes, máquinas y *routers*. El intercambio de información de rutas entre áreas se realiza a través del *router* de borde de área (ABR, *Area Border Router*). A cada área se le asigna un número.

Área 0 (*Backbone*): Es una área esencial que interconecta todas las áreas dentro de un sistema autónomo. Todas las áreas deben estar conectadas al *backbone* porque éste es el responsable de distribuir la información de rutas a todas las demás.

Área *Stub*: Una área *stub* (aislada) posee solo un *router* de borde de área, lo cual significa que solo existe una ruta para salir del área.

Cuando un sistema autónomo se divide en áreas, los *routers* pueden clasificarse, de acuerdo a la función que cumplen (ver figura A.1):

- *Routers* internos, dentro de un área.
- *Routers* de borde de área, conectan dos o más áreas.
- *Routers* de *backbone*.
- *Routers* de borde de AS, se comunican con otros *routers* de otros sistemas autónomos.

Estos tipos pueden solaparse: Por ejemplo, los borde de área son automáticamente de *backbone*. Uno del *backbone* sin conexiones externas, es interno.

Los sistemas autónomos grandes deben ser divididos en áreas. Esto es debido a la gran cantidad de datos que deben ser almacenados en una *base de datos del estado de enlace* y el tiempo que puede tomar el calcular las rutas de esta base de datos.

Los sistemas autónomos grandes deben ser divididos en áreas. Esto es debido a la gran cantidad de datos que deben ser almacenados en una *base de datos del estado de enlace* y el tiempo que puede tomar el calcular las rutas de esta base de datos.

Los *routers* OSPF construyen un gráfico directo de la red utilizando el algoritmo **Dijkstra** *Shortest Path First* (SPF). Un gráfico directo es un mapa de la red con perspectiva del *router*, que es la raíz del gráfico. El gráfico es construido a partir de la base de datos del estado de enlace, la cual incluye información acerca de todos los *routers* de la red y de todos los vecinos de estos *routers*.

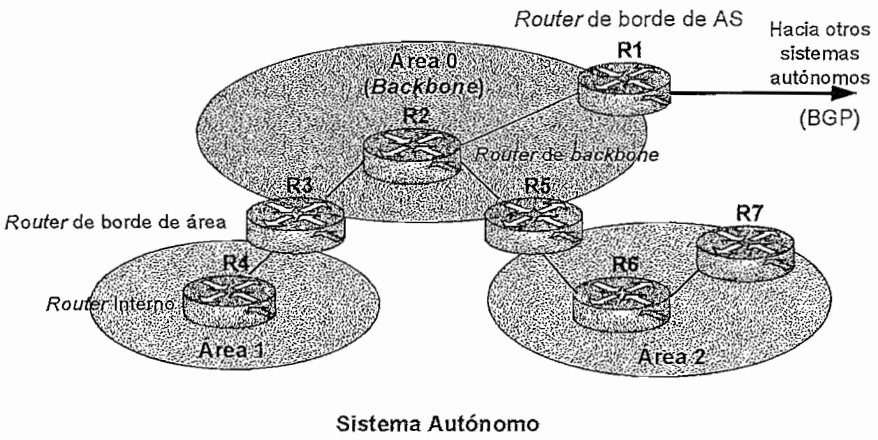


Figura A.1: Relación entre las áreas y los routers en OSPF

En el protocolo OSPF existen cinco tipos de mensajes:

Hello (Hola)*:* Se usa para identificar a los vecinos, es decir, *routers* adyacentes en un área para elegir un *router* designado para una red multienvío, para encontrar un *router* designado existente y para enviar señales de "*Estoy aquí*".

Database Description (Descripción de la base de datos)*:* Durante la inicialización, se usa para intercambiar información de manera que un *router* puede descubrir los datos que le faltan en la base de datos.

Link State Update (Actualización del estado de enlace)*:* Se usa como respuesta a los mensajes de Petición del estado del enlace y también para informar dinámicamente de los cambios en la topología de la red.

Link State Advertisement (Acuse de Recibo del estado de enlace)**:** Se usa para confirmar la recepción de una Actualización del estado del enlace. El emisor retransmitirá hasta que se confirme.

La información de las bases de datos del estado de enlace es conocida y distribuida a través del envío de paquetes OSPF *Hello* a los *routers* vecinos; al llegar este tipo de paquete al *router* vecino, éste coloca al *router* que envió el paquete OSPF *Hello* como vecino.

Los *routers* OSPF reconocen a sus vecinos gracias al flujo de *Link State Advertisement* (LSA) el cual contiene la información de costo de cada uno de sus vecinos. Los LSAs son enviados periódicamente a los *routers* vecinos. Al llegar a ellos, éstos comparan y descartan las entradas duplicadas y guardan el LSA recibido.

Los *routers* OSPF observan a sus vecinos mediante el envío de paquetes *Hello*, cuando un *router* no recibe paquetes de un vecino asume que está caído. Sus vecinos actualizan sus LSAs y los envían a través de la red. El nuevo LSA se incluye en la base de datos de estado de enlace y recalcula el mapa. En redes grandes este cálculo hace ineficiente el protocolo de enrutamiento. Es por esta razón que se divide el sistema autónomo en áreas. Cada área es autónoma; el conocimiento de la topología de un área se mantiene oculto para las otras áreas.

Así, varios grupos dentro de una localidad dada pueden cooperar en el uso de OSPF para enrutar, lo que permite, que cada grupo conserve la capacidad de cambiar su topología de red interna de manera independiente.

Otra característica de eficiencia de OSPF es el permitir un *router designado* el cual está dentro de la red unido a todos los otros *routers* con sus vecinos. Debe

tomarse en cuenta que los otros *routers* solo tiene de vecino al *router* designado. Esto ayuda a reducir el tamaño de la base de datos de enlace de estado y a reducir el proceso de recalculación del mapa.

OSPF puede mantener más de un camino a un destino único; esta característica es usada por medio de balance de carga a través de múltiples enlaces de red. Además, OSPF provee autentificación para asegurar que la actualización de la base de datos se realice por un *router* válido y no sean modificadas inescrupulosamente.

A.4 PROTOCOLO BGP (*BORDER GATEWAY PROTOCOL*)

Los Protocolos EGPs *(Exterior Gateway Protocols)* se usan para intercambiar información de enrutamiento entre distintos sistemas autónomos.

Los EGPs más usados son:

- EGP (*Exterior Gateway Protocol*).
- BGP (*Border Gateway Protocol*).

BGP es el protocolo usado entre ASs para intercambiar información de enrutamiento. BGP mantiene la infraestructura global de *ruteo* en Internet. La última versión en desarrollo es la versión 4. A continuación se dará una breve descripción del protocolo BGP.

BGP es un protocolo vector distancia, a diferencia de los protocolos vector distancia tradicionales tales como RIP (*Routing Information Protocol*), en los que existe solo una métrica (emplea como unidad de medida, saltos), BGP enumera las rutas a cada destino (la secuencia de ASs al destino), es decir BGP determina un orden de preferencia al aplicar una función que asigna cada ruta a un valor de prioridad y selecciona la ruta que tenga el mayor valor. Esta función genera la implementación de BGP según la información de configuración. Para tomar decisiones de enrutamiento, BGP puede tener en cuenta, por ejemplo, cuestiones

existe solo una métrica (emplea como unidad de medida, saltos), BGP enumera las rutas a cada destino (la secuencia de ASs al destino), es decir BGP determina un orden de preferencia al aplicar una función que asigna cada ruta a un valor de prioridad y selecciona la ruta que tenga el mayor valor. Esta función genera la implementación de BGP según la información de configuración. Para tomar decisiones de enrutamiento, BGP puede tener en cuenta, por ejemplo, cuestiones políticas, económicas, de confiabilidad o de seguridad. Este tipo de consideraciones se configura manualmente en los *routers*.

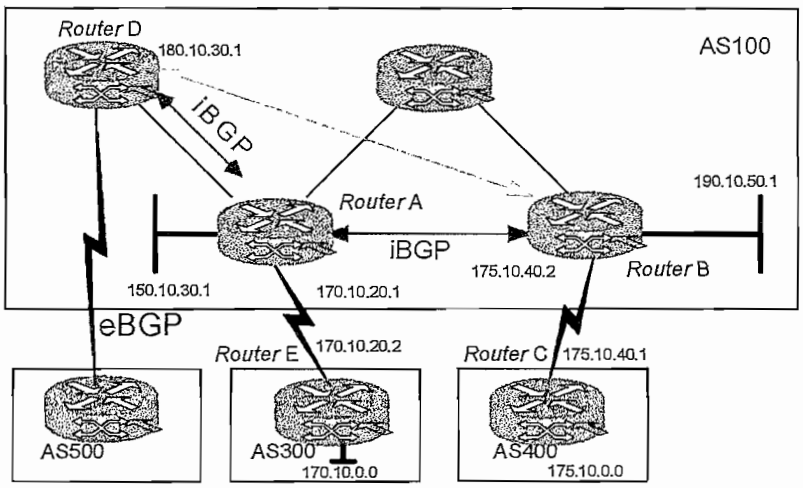


Figura A.2: iBGP y eBGP

El protocolo BGP opera en términos de mensajes, que se envían utilizando conexiones TCP como protocolo de transporte. La comunicación BGP que tiene lugar dentro de un sistema autónomo, es conocida como BGP Interno (iBGP). La comunicación BGP entre diferentes sistemas autónomos, es conocida como BGP Externo (eBGP). Cada AS es identificado por un número de sistema autónomo (ASN), que se requiere cuando BGP se está ejecutando. La figura A.2, ilustra lo indicado anteriormente.

A.4.1 MODO DE OPERACIÓN DE BGP

a otro un mensaje *Open*. Si el dispositivo destino acepta la solicitud, devuelve un mensaje *KeepAlive* como respuesta.

Detección de vecino alcanzable: Una vez establecida la relación de vecino, para mantener la relación se realiza la detección de vecino alcanzable enviándose periódicamente mensajes *KeepAlive*.

Detección de red alcanzable: Para la detección de red alcanzable es necesario que cada dispositivo de enrutamiento tenga una base de datos con todas las redes que puede alcanzar y la mejor ruta para alcanzarla. Cuando se realiza un cambio en la base de datos es necesario enviar un mensaje *Update* por difusión a todos los dispositivos de enrutamiento que implementan BGP para que puedan acumular y mantener la información necesaria, es decir los mensajes *Update* contienen anuncios de redes accesibles y la ruta correspondiente (trayectorias de ASs), así como retiros de redes que ya no son accesibles.

Anunciar una ruta implica que el AS correspondiente puede y acepta transportar información hacia un destino. Cada *router* BGP recibe de sus vecinos las rutas que emplean para llegar a cada posible destino y escoge la mejor. El criterio de selección no forma parte del protocolo.

Periódicamente se envían mensajes de *KeepAlive* para saber el estado de la conexión. Mensajes de notificación son enviados en respuesta a un error o a una condición especial. Si la conexión encuentra una condición de error, un mensaje de notificación (*Notification*) es enviado y se cierra la conexión.

A.4.2 FORMATO DEL MENSAJE DE BGP

Todos los mensajes BGP tienen en común un formato básico. Varían en longitud de 19 a 4096 *bytes*, se transmiten sobre TCP y se procesan en su totalidad (no se procesan hasta que se han recibido por completo). Cada mensaje tiene una cabecera como se muestra en la figura A.3.

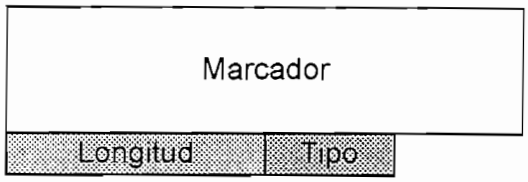


Figura A.3: Cabecera BGP

Marcador: 16 *Bytes*. Sirve de autentificación, es decir, para que el receptor pueda verificar la identidad del emisor.
Longitud: 2 *Bytes*. Indica el tamaño del mensaje en *bytes*.
Tipo: 1 *Byte*. Especifica el tipo de paquete enviado: *Open*, *Update*, *Notification* y *KeepAlive*.

Para adquirir un vecino, un *router* abre primero una conexión TCP al *router* vecino de interés. Entonces envía un mensaje *Open*. Este mensaje identifica al AS al que pertenece el emisor y suministra la dirección IP del *router*. También incluye un parámetro temporizador de mantenimiento, que propone el emisor. Si el destino está preparado para abrir una relación de vecindad, calcula un valor para el temporizador de mantenimiento, que es el valor mínimo de su tiempo de mantenimiento y que introduce en su mensaje *Open*. El valor calculado representa el máximo número de segundos que puede transcurrir entre la recepción de mensajes *Keepalive* sucesivos y/o mensajes *Update* del emisor.

Un mensaje *Keepalive* consta solamente de la cabecera. Cada *router* emite estos mensajes bastante a menudo a cada una de sus parejas para prevenir que expire el temporizador de mantenimiento.

Un mensaje *Update* facilita dos tipos de información: sobre una ruta particular a través del conjunto de redes o una lista de rutas previamente anunciadas por este dispositivo de enrutamiento a ser eliminadas. La información sobre una ruta particular a través de la red implica tres campos, campo de información sobre la capacidad de alcanzar la capa de red (NLRI, *Network Layer Reachability Information*), campo de longitud total de los atributos del camino y el campo de atributos de camino, los atributos BGP son un conjunto de parámetros utilizados para llevar la cuenta de la información específica de una ruta. El campo NLRI

contiene una lista de identificadores de subredes que se pueden alcanzar por esta ruta. Cada subred se identifica por su dirección IP, en realidad una parte de la dirección IP completa.

El campo atributos de camino contiene una lista de atributos que se aplican a esta ruta particular. Los atributos son:

- **Origen:** indica si la información fue generada por un protocolo de enrutamiento interior o por uno exterior.
- **Camino_AS:** lista de los ASs que son atravesados por la ruta.
- **Siguiente_salto:** Dirección IP del *router* frontera que se debe usar como siguiente salto para alcanzar los destinos indicados en el campo NLRI.
- **Multi_sal_des:** Se usa para comunicar alguna información sobre rutas internas a un AS.
- **Local_pref:** Usado por un *router* para informar a otros *routers* dentro del mismo AS de su grado de preferencia por una ruta particular.
- **Agregado_atómico, Agente_unión:** implementan el concepto de unión de rutas.

Los mensajes de Notificación se envían cuando se detecta una condición de error.

A.4.3 INTERCAMBIO DE INFORMACIÓN DE ENRUTAMIENTO BGP

La esencia de BGP es el intercambio de información de enrutamiento entre dispositivos de enrutamiento participantes en múltiples AS. Este proceso puede ser bastante complejo. A continuación se da una visión simplificada.

Consideremos el *router* E (R1) en el sistema autónomo 300 (AS300), en la figura A.2. Un *router* que implemente BGP también implementará un protocolo de enrutamiento interno como OSPF. Usando OSPF, R1 puede intercambiar información de enrutamiento con otros dispositivos de enrutamiento dentro de AS300 y construir un esquema de la topología de las subredes y *routers* en AS300 para obtener una tabla de enrutamiento. Seguidamente, R1 puede emitir

un mensaje *Update* al *router* A en AS100, este mensaje *Update* podría incluir lo siguiente:

- Camino_AS: la identidad de AS300.
- Siguiente_salto: la dirección IP de R1.
- NLRI: una lista de todas las subredes en AS300.

Este mensaje informa al *router* A que todas las subredes indicadas en NLRI se alcanza mediante el *router* E y que el único sistema autónomo que hay que atravesar es AS300.

A.4.4 EXTENSIONES MULTIPROTOCOLO PARA BGP

Ciertas extensiones al protocolo BGP que provean capacidades adicionales son necesarias para permitir a BGP transportar más información que solamente la dirección IPv4 (y los atributos BGP estándar). Cuando se establece una sesión BGP entre dos pares, un mensaje *Open* intercambia los parámetros BGP iniciales, como el número del sistema autónomo usado por los vecinos BGP. Este mensaje *Open* puede contener parámetros opcionales, uno de los cuales es el parámetro *Capacidades* que describe las capacidades opcionales que puede extender y ejecutar el par. Una de estas capacidades son las extensiones multiprotocolo, denominado MP-BGP (*Multiprotocol* BGP), extensiones que proporcionan a BGP la capacidad de transportar información para protocolos de capa red distintos a IPv4, IPv6 e IPX.

MP-BGP introduce dos nuevos atributos opcionales no transitivos: Multiprotocolo alcanzable NLRI (MP_REACH_NLRI) que publica nuevas rutas multiprotocolo y Multiprotocolo no alcanzable NLRI (MP_UNREACH_NLRI) que anula las rutas anteriormente publicadas por MP_REACH_NLRI. Multiprotocolo alcanzable NLRI (MP_REACH_NLRI) puede utilizarse para tres propósitos:

- Publicar una ruta factible a un par.

- Permitir que un *router* publique la dirección de la capa red del *router* que debería ser utilizado como el próximo salto hacia el destino indicado en el campo NLRI del atributo MP_NLRI.
- Permitir que un *router* dado informe a algunos o todos los puntos de subred de conexión que existen dentro del sistema local.

Multiprotocolo no alcanzable NLRI (MP_UNREACH_NLRI) puede utilizarse para retirar de servicio una o más rutas no factibles.

Estos nuevos atributos introducidos por MP-BGP proporcionan la capacidad de asociar un protocolo de capa red particular con la información del próximo salto, así como asociar un protocolo de capa red particular con NLRI. La información de la familia de direcciones identifica el protocolo de capa red que se transporta en la actualización.

ANEXO B

ESTADO ACTUAL DE LAS RFCs DE MPLS

Un RFC (*Request For Comments*) es un documento oficial del IETF que es el resultado de un bosquejo de realiza un comité y una subsiguiente revisión por las partes interesadas. Algunos RFCs son informativos por naturaleza. De aquéllos que son pretendidos a convertirse en estándares de Internet, la versión final del RFC se vuelve estándar y no se permiten comentarios adicionales o cambios. Sin embargo, el cambio puede ocurrir a través de RFCs subsiguientes que reemplacen o se elaboren en todo o partes de RFCs anteriores.

Actualmente existen solo unos pocos RFCs de MPLS. Además existen alrededor de 100 *drafts* para MPLS. Un *draft* dado tiene un tiempo de vida de 6 meses y tiene un estado de NO STATUS OFICIAL y ni siquiera puede ser respaldado por el grupo de trabajo. Incluso cuando estos *drafts* pasan al estado de RFC, puede pasar varios años antes de que ellos progresen a un STANDARD STATUS.

RFC 3031	*Multiprotocol Label Switching Architecture*	Estándar Propuesto	Enero 2001
RFC 3032	*MPLS Label Stack Encoding* (Reemplazado por el RFC3443)	Estándar Propuesto	Enero 2001
RFC 3443	*Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*	Estándar Propuesto	Enero 2003
RFC 3270	*Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*	Estándar Propuesto	Mayo 2002
RFC 3034	*Use of Label Switching on Frame Relay Networks Specification*	Estándar Propuesto	Enero 2001
RFC 3035	*MPLS using LDP and ATM VC Switching*	Estándar Propuesto	Enero 2001
RFC 3063	*MPLS Loop Prevention Mechanism*	Estándar Propuesto	Febrero 2001
RFC 3036	*LDP Specification*	Estándar Propuesto	Enero 2001

RFC 3037	*LDP Applicability*	Informativo	Enero 2001
RFC 3209	*RSVP-TE: Extensions to RSVP for LSP Tunnels*	Informativo	Diciembre 2001
RFC 3353	*Overview of IP Multicast in a Multi-Protocol Label Switching (MPLS) Environment*	Informativo	Agosto 2002
RFC 3496	*Protocol Extension for Support of Asynchronous Transfer Mode (ATM) Service Class-aware Multiprotocol Label Switching (MPLS) Traffic Engineering*	Informativo	Marzo 2003
RFC 3468	*The Multiprotocol Label Switching (MPLS) Working Group decision on MPLS signaling Protocols*	Informativo	Febrero 2003
RFC 3469	*Framework for Multi-Protocol Label Switching (MPLS)-based Recovery*	Informativo	Febrero 2003
RFC 2917	*A Core MPLS IP VPN Architecture*	Informativo	Septiembre 2000
RFC 2702	*Requirements for Traffic Engineering Over MPLS*	Informativo	Septiembre 1999
RFC 2547bis	*BGP/MPLS VPNs*	Informativo	Marzo 1999
RFC 3471	*Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*	Estándar Propuesto	Enero 2003
RFC 3472	*Generalized Multi-Protocol Label Switching (GMPLS) Signaling Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions*	Estándar Propuesto	Enero 2003
RFC 3473	*Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*	Estándar Propuesto	Enero 2003
RFC 3474	*Documentation of IANA assignments for Generalized Multi-Protocol Label Switching (GMPLS) Resource Reservation Protocol Traffic Engineering (RSVP-TE) Usage and Extensions for Automatically Switched Optical Network (ASON)*	Estándar Propuesto	Marzo 2003

EOL: Cisco 1600 Series Routers

The content in this catalog is updated on a monthly basis—for the most current information please see

http://www.cisco.com/en/US/products/hw/routers/ps214/index.html

Product Overview

The Cisco 1600 series have become the proven cboice for data access for small branch offices and small businesses because they offer a range of features specifically designed for such applications:

- Modular design for wide-area network (WAN) choice and flexibility
- Advanced security, including optional integrated firewall, encryption, and virtual private network (VPN) software
- End-to-end quality of service (QoS) and multimedia support
- Integrated data service unit/channel service unit (DSU/CSU) with up to T1 speed and integrated Network Termination (NT1)
- Low cost of ownership through WAN bandwidth optimization
- Ease of use, deployment, and management

The Cisco 1700 series routers build on the success of the Cisco 1600 routers, delivering multiservice capabilities, as well as greater modularity, security, and integration to small offices.

Cisco 1600 Series Modular Routers

Cisco 1600 series routers connect small offices with Ethernet LANs to WANs through Integrated Services Digital Network (ISDN), asynchronous serial, and synchronous serial connections.

The five basic configurations of the Cisco 1600 product family offer the following ports:

- Cisco 1601 R—one Ethernet, one serial, one WAN interface
- Cisco 1602 R—one Ethernet, one serial with integrated 56-kbps DSU/CSU, one WAN interface card slot
- Cisco 1603 R—one Ethernet, one ISDN Basic Rate Interface (BRI) (S/T interface), one WAN interface card slot
- Cisco 1604 R—one Ethernet, one ISDN BRI with integrated NT1 (U interface), one S-bus port for ISDN phones, one WAN interface card slot
- Cisco 1605 R—two Ethernet slots, one WAN interface card slot

The serial WAN port on the Cisco 1601 R router supports asynchronous serial connections of up to 115.2 kbps and synchronous serial connections—such as Frame Relay, leased lines, Switched 56, Switched Multimegabit Data Service (SMDS), and X.25—of up to 2.048 Mbps. The Cisco 1602 R router integrates a 56-kbps four-wire DSU/CSU, and it supports tbe same synchronous serial connections as the Cisco 1601 R router (except SMDS). The ISDN BRI port on the Cisco 1603 R router has an S/T interface, while the Cisco 1604 R includes an integrated NT1 with a U interface. The Cisco 1605 R router provides a 10BaseT and an AUI port on the first Ethernet interface and a 10BaseT port on the second Ethernet interface.

Run From RAM Architecture

The 1601 R-1605 R routers have a "run-from-RAM" architecture; the "R" suffix designates run from "RAM". The Cisco IOS software image is stored in Flash memory (in compressed form), but is loaded into RAM before being executed by the router.

The Run-from-RAM models offer the following benefits:

1. Greater Performance—The Cisco 1600 R models deliver greater performance for memory-intensive applications such as encryption and compression.

2. Easier Upgradability—The Cisco 1600 R routers permit software upgrades over any interface while the router is running

3. Lower Cost—Because the Cisco 1600 R models store the software in compressed form in Flash memory, less flash memory is required to run advanced feature sets (such as Cisco 1600 series IOS IP Plus). The new Cisco 1600 R routers (1601 R, 1602 R, 1603 R, and 1604 R) are essentially the same as the original models (1601-1604), but they are "run-from-RAM" routers, similar to the Cisco 1605 R model introduced in late 1997. The new Cisco 1600 R models deliver all the features and benefits of the original models, including the same interfaces, the same functionality, the same feature sets, and the same versions of Cisco IOS (R) software and have the same physical dimensions.

Figure 27-7: Cisco 1601 R Rear View

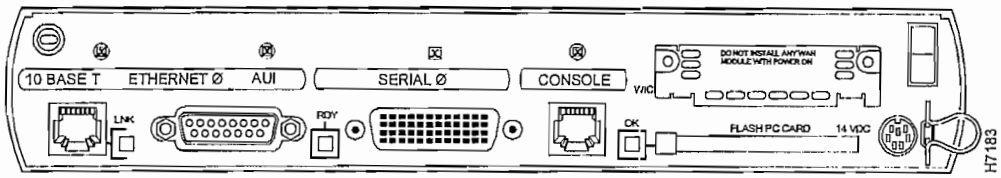


Figure 27-8: Cisco 1602 R Rear View

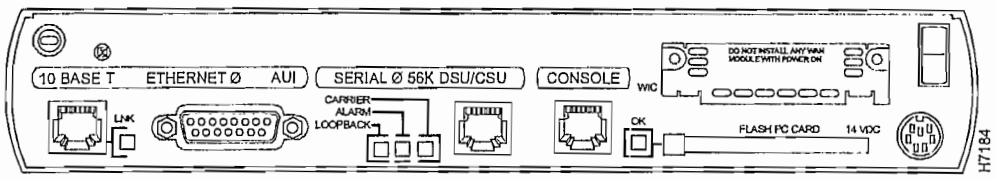


Figure 27-9: Cisco 1603 R Rear View

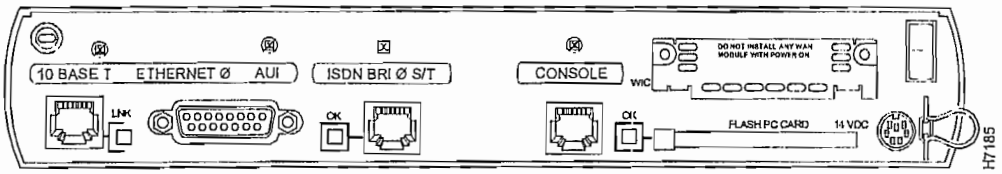


Figure 27-10: Cisco 1604 R Rear View

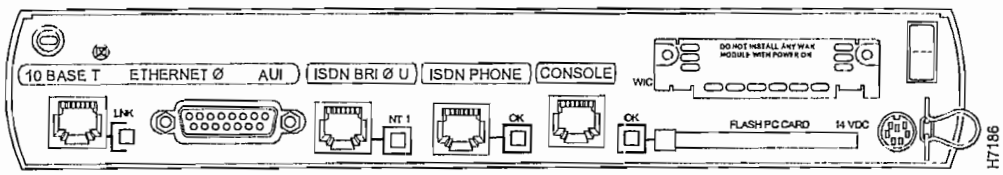
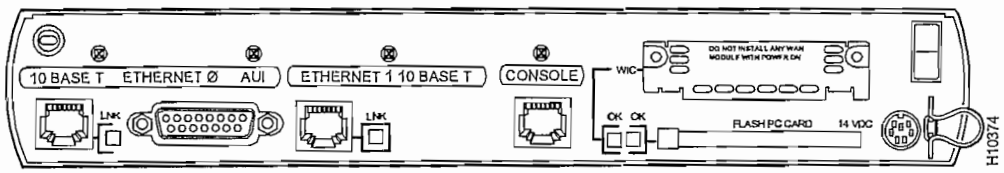


Figure 27-11: Cisco 1605 R Rear View



Options for Cisco 1600 Series

Options for Cisco 3700, 3600, 2600, and 1600 Series: NMs, VICs, WICs, AIMs, and HDSMs in Chapter 18: Routers.

Key Features and Benefits

Flexibility and Investment Protection

The WAN interface card slot allows customers to change or add WAN interface cards as their requirements grow or change. With this feature, the Cisco 1600 series offers more flexibility and investment protection than any other product in its class. What's more, the ability to use the same WAN interface cards in Cisco 1600, 1700, 2600, and 3600 routers reduces requirements for spare parts inventory and protects investments in existing routers.

Table 27-57: Optional WAN Interface Cards Available

WAN Interface Card	1601 R	1602 R	1603 R	1604 R	1605 R
Serial, asynchronous and synchronous	Yes	Yes	Yes	Yes	Yes
T1/Fractional T1 DSU/CSU	Yes	Yes	Yes	Yes	Yes
56/64-kbps four-wire DSU/CSU	Yes	Yes	Yes	Yes	Yes
ISDN BRI with S/T interface (dial & leased line)	Yes	Yes			Yes
ISDN BRI with integrated NT1, U interface (dial & leased line)	Yes	Yes			Yes
ISDN BRI leased line (S/T interface)			Yes	Yes	

The ISDN BRI Leased Line S/T card is designed specifically for the Cisco 1603 R and 1604 R routers. It is intended for users who require a dial-up ISDN BRI line (from the Cisco 1603 R or 1604 R router's fixed-WAN port) and an ISDN leased line (from the ISDN BRI Leased Line card inserted into the Cisco 1603 R or 1604 R router). This card is automatically configured only in ISDN leased line mode.

Device Integration

Cisco 1600 routers deliver a complete solution for remote access for small businesses and small branch offices. They provide not only advanced routing capabilities but also the option to integrate DSU/CSU and ISDN network T1 device (NT1), as well as firewall, encryption, and VPN functionality. This integration reduces deployment time and expense because fewer devices and cables need to be installed and configured. An integrated product also saves space and increases reliability because fewer stand alone devices are required to build the solution. The Cisco 1600 routers simplify ongoing support of small branch offices from a central site through remote configuration, monitoring, and troubleshooting of all integrated functions in the router.

Advanced Security

To leverage the unprecedented opportunities offered by communications and commerce over the Internet, private information must remain secure. Cisco IOS security services provide many technologies to build a custom security solution. The elements of security services include perimeter security, firewalls, encryption, and VPNs.

Perimeter Security

Perimeter security refers to the control of traffic entry and exit between network boundaries, such as between private networks, intranets, extranets, or the Internet. Cisco IOS perimeter security technologies provide a highly flexible, superior solution with features such as:

- Standard and extended access control lists (ACLs)
- Lock and Key (dynamic ACLs)
- Router/route authentication, authorization, and accounting (such as PAP/CHAP, TACACS+, and RADIUS)

Firewall

The optional Cisco IOS Firewall Feature Set, available on all Cisco 1600 models, provides formidable firewall functionality, including:

- Context-based access control (CBAC)
- Java blocking
- Attack detection and prevention
- Improved logging and alerts

CBAC provides stateful application-layer security by examining traffic sessions on a per-application basis and allowing return traffic through the firewall. When a session is initiated internally, CBAC writes a temporary, session-specific ACL entry and deletes the ACL entry upon session termination.

The Cisco 1605 R router—which supports one WAN slot, two Ethernet ports, and the Cisco IOS Firewall Feature Set—makes an ideal integrated and flexible firewall for small offices. This integrated router/firewall effectively segments an internal, secure LAN from a perimeter LAN exposed to an untrusted network (such as the Internet), thus creating a "demilitarized zone."

See the Cisco IOS Firewall Feature Set data sheet for further details.

Virtual Private Networks (VPNs) and Encryption

The Cisco 1600 series routers may be deployed as an entry-level VPN access solution, supporting DES encryption at rates of up to 128 kbps. The Cisco 1720 router is recommended for VPN applications that require greater performance or 3DES or both. Cisco IOS software for the Cisco 1600 series provides a comprehensive set of VPN features, including not only perimeter security and firewalls but also the following key technologies:

- IPSec tunneling with data encryption standard (DES)
- Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP)
- VPN management tools such as support for VPN policy configuration in Cisco ConfigMaker

Cisco IOS Software Features for Small Office Data Access

Cisco 1600 series routers offer small businesses and small branch offices a complete set of internetworking software features. In addition to the features mentions earlier, Cisco IOS software differentiates the Cisco 1600 series from the competition with:

- Multiprotocol routing (IP, IPX, AppleTalk), IBM/SNA, and transparent bridging over ISDN, asynchronous serial, and synchronous serial such as leased lines, Frame Relay, SMDS, Switched 56, X.25, and X.25 over D
- Network Address Translation (NAT), which eliminates the need to re-address all hosts with existing private network addresses and hides internal addresses from public view
- Easy IP—a combination of NAT, Point-to-Point Protocol/Internet Control Protocol (PPP/IPCP) and Dynamic Host Configuration Protocol (DHCP) server—which enables the router to dynamically negotiate its own IP address and dynamically allocate local IP addresses to the remote LAN hosts, simplifies deployment, and minimizes Internet access costs
- End-to-end QoS features such as Resource Reservation Protocol (RSVP), IP Multicast, WFQ, and AppleTalk Simple Multicast Routing Protocol (SMRP), which support multimedia applications such as desktop video conferencing, distance learning, and voice/data integration
- WAN optimization features such as dial-on-demand routing (DDR), bandwidth-on-demand (BOD), and Open Shortest Path First (OSPF)-on-demand circuit, Snapshot routing, compression, filtering, and spoofing to reduce WAN costs

Easy to Use

The Cisco 1600 series includes a variety of easy, user-friendly installation and configuration features such as color coded ports, removable Flash memory PC cards for easy software deployment, the Cisco ConfigMaker configuration tool and the Cisco Fast Step software tool. These features combine to give the lowest total cost of ownership of any small office router.

Each Cisco 1600 series router includes the Cisco Fast Step easy-to-use Windows 95, 98, and NT 4.0-based software tool that simplifies the setup, monitoring, and troubleshooting of Cisco routers. The Cisco Fast Step setup application leads users through simple, step-by-step, wizards-based procedures to configure Cisco routers connected to an Internet service provider and remote corporate network. Cisco Fast Step software includes the Cisco Fast Step monitor application, which provides users with router LAN and WAN performance statistics, fault alarms, and troubleshooting assistance.

The Cisco ConfigMaker application is appropriate for advanced configuration of the Cisco 1600 series routers. A Windows 95, 98, and NT 4.0-based software tool, Cisco ConfigMaker is designed to configure a small network of Cisco routers, switches, hubs, and other network devised from a single PC. Cisco ConfigMaker is designed for resellers and network administrators of small and medium-sized businesses who are proficient in LAN and WAN fundamentals and basic network design. Cisco ConfigMaker includes support for the Cisco IOS Firewall Feature Set (which provides integrated enhanced security capabilities), Network Address Translation (NAT), and Cisco Easy IP software.

In addition to easy-to-use software, the hardware for the Cisco 1600 routers is designed to be "plug-and-play" in four notable areas. First, each of the ports on the Cisco 1600 routers and WAN interface cards is color coded, and optional color-coded cables can be purchased from Cisco. Second, preconfigured software may be loaded into a Flash memory PC card at a central site, and then a user at remote site may deploy the router by simply inserting the Flash card, plugging in cables, and turning on the power. Third, once the router is running, software upgrades and configuration modifications can be downloaded over the WAN from a central site. And finally, the Cisco 1600 series allows for centralized administration and management via Simple Network Management Protocol (SNMP) or Telnet or through the console port.

Specifications

Hardware

Table 27-58: Technical Specifications for Cisco 1600 Series

Feature	Cisco 1601 R	Cisco 1602 R	Cisco 1603 R	Cisco 1604 R	Cisco 1605 R
First Built-in Interface (LAN)	Ethernet: 10Base-T (RJ-45) and AUI (DB-15)	Ethernet: 10Base-T (RJ-45) and AUI (DB-15)	Ethernet: 10Base-T (RJ-45) and AUI (DB-15)	Ethernet: 10Base-T (RJ-45) and AUI (DB-15)	Ethernet: 10Base-T (RJ-45) and AUI (DB-15)
Second Built-in Interface (WAN or LAN)	Serial sync/async DB-60	56K 4 wire DSU/CSU: RJ-48S	ISDN BRI S/T RJ-45	ISDN BRI U with NT1: RJ-45	Ethernet: 10Basse-T (RJ-45) only
Optional WAN Interface Cards, please see Power Requirements for Cisco 1710 Router.					
Processor	Motorola 68360 at 33MHz				
Memory Architecture	Run-from-RAM				
DRAM: Default	8 MB				
DRAM: Maximum	24 MB				
Flash Memory: Default	4 MB				
Flash Memory: Maximum	16 MB				
Console Port	RJ-45				

Table 27-59: Serial Interfaces Supported by the Cisco 1601 R and 1602 R Routers and Serial WAN Interface Cards

	Cisco 1601 R On-board WAN	Cisco 1602 R On-board WAN	WIC-1T Card	WIC-1DSU-56K4 Card	WIC-1DSU-T1 Card (New)
Asynchronous serial connection over basic analog telephone	Up to 115.2 kbps	Not supported	Up to 115.2 kbps	Not supported	Not supported
Synchronous serial connections					
Leased Line / Digital Data Service (DDS)	Up to 2.0 Mbps with external DSU/CSU	56 kbps	Up to 2.0 Mbps with external DSU/CSU	56 or 64 kbps	See footnote[1]
Switched 56	56 Kbps with external DSU/CSU	56 kbps	56 Kbps with external DSU/CSU	56 Kbps	Not applicable

1. Line must be provisioned as T1 or fractional T1, that is N x 64 or N x 56 (N=1 through 24) unchannelized and clocked at 1.544 Mbps. A dedicated 64Kbps leased line would not be supported if clocked at 64Kbps, for example, but would be supported if provisioned as fractional T1 (in other words, clocked at 1.544 Mbps).

Note For detailed information about network modules (NMs) and WAN interface cards (WICs) see the Options for Cisco 3700, 3600, 2600, and 1600 Series: NMs, VICs, WICs, AIMs, and HDSMs in Chapter 18: Routers.

- Asynchronous serial protocols: Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP)
- Asynchronous interface: EIA/TIA-232
- Synchronous serial WAN services: Frame Relay, X.25, SMDS
- Synchronous serial protocols: PPP, HDLC, LAPB, IBM/SNA
- Synchronous serial interfaces supported on Cisco 1601 R and WIC-1T card: EIA/TIA-232, V.35, X.21, EIA/TIA-449, EIA-530

Table 27-60: ISDN Interfaces for Cisco 1600 Series

Feature	Cisco 1603 R/1604 R On-board WAN	WIC-1B-S/T card	WIC-1B-U card	WIC-1B-S/T-LL card
ISDN dialup	Yes	Yes	Yes	Not supported
ISDN Leased Line 64 kbps	Rel 11.1	Rel 11.1	Rel 11.1	Rel 11.2(9)P
ISDN Leased Line 128 kbps	Rel 11.3(1)	Rel 11.3(1)	Rel 11.3(1)	11.3(3)T
Frame Relay encapsulation over ISDN Leased Line	Yes	Yes	Yes	Yes
PPP encapsulation over ISDN Leased Line	Yes	Yes	Yes	Yes
PPP compression (up to 4:1)	Yes	Yes	Yes	Yes

Table 27-61: Power Requirements for Cisco 1600 Series

Description	Specification
Output	27W max.
AC input - Voltage	100 to 240 VAC
AC input - Current	0.2 to 0.4A
Frequency	50 to 60 Hz

Table 27-62: Physical and Environmental Specifications for Cisco 1600 Series

Description	Cisco 1600 Series	WAN Interface Cards
Dimensions (W x H x D)	11.15 x 2.19 x 8.67 in. (28.32 x 5.56 x 22.02 cm)	3.1 x 0.8 x 4.8 in. (7.9 x 2.1 x 12.2 cm)

Description	Cisco 1600 Series	WAN Interface Cards
Weight (min.)	1.65 lb. (0.75 kg)	0.13 lb (57 g)
Weight (max.)	1.80 lb. (0.82 kg)	0.19 lbs (85 g)
Temperature	Operating	–32 to 104°F (0 to 40°C)
	Storage	–4 to 149°F (--20 to 65°C)
Humidity	Operating	0 to 85%
	Storage	5 to 95%

Software

All software part descriptions and part numbers for Cisco products can be accessed using the online Cisco Pricing Tool at http://www.cisco.com/cgi-bin/order/pricing_root.pl

Ordering Information

Product Part Numbers

All part descriptions and part numbers for Cisco products can be accessed using the online Cisco Pricing Tool at http://www.cisco.com/cgi-bin/order/pricing_root.pl

The Cisco Pricing Tool requires a user name and password. If you are not already registered, go to http://www.cisco.com/register and follow the instructions. After you have registered, you can access the Pricing Tool.

Cisco Systems

Overview

Cisco 1700 Series Modular Access Routers

Cisco 1700 Series Modular Access Router Solutions

The Cisco 1700 Series of modular access routers are designed to provide a cost-effective integrated platform for small and medium-sized businesses and enterprise small branch offices. They provide flexibility and manageability to meet the most demanding and evolving business requirements such as multiservice data/voice/video/fax integration, business-class digital subscriber line (DSL), and comprehensive network security. See Figure 1.

The Competitive Advantage

Today's businesses are recognizing that business success relies on more than simply using e-mail or putting up a Web site. Companies that want to streamline operations and reduce costs while gaining the competitive advantages of the Internet need to integrate business processes into their everyday business practices by adopting applications such as Web-based transaction processing, telecommuting, and e-learning. These kinds of business tools improve communications between employees, customers, and suppliers; increase productivity and efficiency; and enhance customer satisfaction to make businesses more competitive. The effectiveness of business solutions depends on the performance and capabilities of the access solution.

To fully realize all the competitive advantages companies need a flexible and affordable access solution that supports a full range of technologies and applications. The Cisco 1700 Series of modular access routers are optimized to provide comprehensive features such as virtual private networks (VPNs), security firewalls, business-class DSL, and multiservice integration of data, voice, video, and fax. The routers deliver high-speed WAN connectivity for communications over the Internet and between remote office sites. For an overview of Cisco 1700 Series features, refer to Table 1.

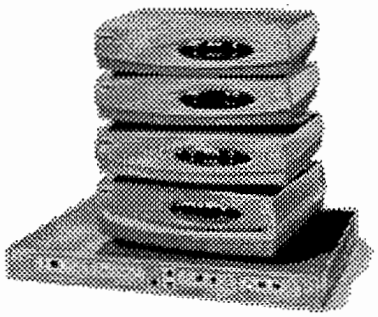


Figure 1
Cisco 1700 Series

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 1 Overview of Cisco 1700 Series Features

Benefits	Features
Flexibility and investment protection	• Offers modular data and voice slots (except Cisco 1701, 1711, 1712) • Provides customization through a wide range of WAN and voice interface cards (except Cisco 1701, 1711, 1712) • Presents migration path to multiservice voice and data integration (Cisco 1751 and 1760)
Security	• Offers Cisco IOS® stateful inspection firewall • Provides VPN IP Security (IPSec) encryption (Digital Encryption Standard [DES] and Triple DES [3DES]) • Enables encryption up to T1/E1 speeds (4-Mbps full duplex) using optional VPN module (included in Cisco 1711 and 1712—optional for the other Cisco 1700 Series models)
Business-class DSL	• Supports ADSL and G.shdsl • Offers enhanced quality of service (QoS) over DSL • Offers toll-quality voice over DSL
Multiservice data and voice integration (Cisco 1751 and 1760)	• Provides support for analog and digital voice calls • Supports IP telephony • Interoperates with next-generation voice-enabled business applications such as integrated messaging and Web-based call centers • Works with existing telephone infrastructure: phones, fax machines, key telephone system (KTS) units, and private branch exchanges (PBXs) (including digital PBXs)
Remote Manageability	• Supports CiscoWorks management applications • Enables QoS and traffic prioritization through Cisco IOS Software

The Cisco 1760 Modular Access Router provides multiservice voice/video/data solutions in a 19-inch rackmount chassis. Four modular slots are available to support a variety of WICs and VICs. The Cisco 1751 Modular Access Router designed in a desktop form factor also provides multiservice voice/video/data integration.

The Cisco 1721 Modular Access Router is optimized for flexible data-access solutions supporting dual WAN applications for high availability.

The Cisco 1711 and 1712 Security Access Router provides a cost-effective integrated security and routing solution in a single device for secure broadband access.

The Cisco 1701 ADSL Security Access Router provides secure and reliable Internet and corporate network connectivity and business-class ADSL over basic telephone service (POTS) with a redundant ISDN WAN link.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 2 Cisco 1700 Series Comparison

	Cisco 1701	Cisco 1711	Cisco 1712	Cisco 1720	Cisco 1751	Cisco 1751-V	Cisco 1760	Cisco 1760-V
Application	ADSL Security	Broadband Security	Broadband Security	Data Access	Data and Voice	Data and Voice	Data and Voice	Data and Voice
Form Factor	Desktop	Desktop	Desktop	Desktop	Desktop	Desktop	19" Rack-mount	19" Rack-mount
Fixed/ Modular	Fixed	Fixed	Fixed	Modular	Modular	Modular	Modular	Modular
Default Memory (Flash/ DRAM MB)	32/64	32/64	32/64	32/96	32/64	32/96	32/64	32/96
Maximum Memory (Flash/ DRAM MB)	32/128	32/128	32/128	32/128	32/128	32/128	64/128	64/128
WAN Access								
Modular Slots				2	3	3	4	4
Integrated WAN Port	ADSL	10/100	10/100					
Backup WAN	ISDN	Analog Modem	ISDN	optional	optional	optional	optional	optional
LAN								
LAN Ports	1–10/100	4–10/100	4–10/100	1–10/100	1–10/100	1–10/100	1–10/100	1–10/100
802.1Q VLAN								
Multiservice Voice								
Voice over IP								
Analog/ Digital Voice								
QoS								
Integrated Security								
Hardware Accelerated VPN	optional			optional	optional	optional	optional	optional
VPN Tunnels	100	100	100	100	100	100	100	100

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 2 Cisco 1700 Series Comparison

	Cisco 1701	Cisco 1711	Cisco 1712	Cisco 1721	Cisco 1751	Cisco 1751-V	Cisco 1760	Cisco 1760-V
Stateful Firewall				optional	optional	optional	optional	optional
IDS (Intrusion Detection)				optional	optional	optional	optional	optional
Easy VPN Remote/ Server				optional	optional	optional	optional	optional
Websense URL Filtering				optional	optional	optional	optional	optional
SDM Embedded Web Tool								

The Cisco 1700 Series Key Benefits

The Cisco 1700 Series routers are designed to enable small/medium-sized businesses and small enterprise branch offices to successfully deploy networked applications by providing:

- Flexibility and investment protection
- Comprehensive security
- Business-class DSL
- Multiservice data/voice/video/fax integration
- Enhanced manageability

Flexibility and Investment Protection

The modularity of the Cisco 1700 Series allows it to easily fit the needs of growing companies. Interchangeable WICs and voice interface cards (VICs) enable easy additions or changes in WAN technologies without requiring a forklift upgrade of an entire platform. The wide range of available WIC and VIC solutions gives customers a choice when implementing WAN and voice technologies. It allows customers to start out with a solution that meets current needs and easily expand as business demands grow. WAN technologies supported include broadband DSL, ISDN, leased lines, and Frame Relay. Voice technologies supported are VoIP and VoFR. These WICs and VICs are also shared with the Cisco 2600, 3600, and 3700 Series routers.

Comprehensive Security

To succeed, companies must deploy robust network security measures. Business applications often involve storing and transmitting sensitive data, such as customer credit information, and this data can be an attractive target for hackers and other malicious agents. To keep networks secure and protect sensitive information, businesses deploy a range of security technologies, including firewalls, VPNs, and intrusion detection systems.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Cisco IOS Software is the industry's widely accepted standard for the Internet and private network operations. Based on Cisco IOS security technology, the Cisco 1700 Series routers provide powerful, integrated firewall, VPN, and IDS capabilities. As new security technologies are developed, they often can be simply uploaded to a Cisco 1700 Series Router—there is no need for costly hardware replacements.

Firewall

Just as physical businesses require security measures for protection against theft of physical assets, businesses also require tools to maintain the security and confidentiality of its intellectual property. Firewalls provide this protection by preventing unauthorized users from accessing confidential corporate data.

The Cisco 1700 Series routers offer integrated security features, including stateful inspection firewall functionality as an optional Cisco IOS Software feature. By deploying Cisco IOS Software firewall functionality, customers do not need to purchase or manage multiple devices, simplifying network management and reducing capital costs.

Cisco IOS Software firewall security features include access control lists (ACLs), user authentication, authorization, and accounting (such as Password Authentication Protocol/Challenge Handshake Authentication Protocol [PAP/CHAP], TACACS+, and Remote Access Dial-In User Service [RADIUS]). These security features provide the optimal level of firewall protection to customers.

Virtual Private Networks

The Cisco 1700 Series is part of the end-to-end Cisco VPN solution. VPNs create secure tunnel connections via the Internet to connect geographically dispersed offices, business partners, and remote users while providing security, traffic prioritization, management, and reliability equal to that of private networks. VPNs significantly reduce WAN costs, and they can be set up and torn down rapidly to provide secure extranet links to customers, business partners, and remote employees on demand.

By supporting industry standards such as IPSec, Layer 2 Tunneling Protocol (L2TP), and DES, 3DES, and AES Cisco 1700 Series routers deliver robust VPN solutions to ensure data privacy, integrity, and authenticity.

The optional* VPN Hardware Encryption Module for Cisco 1700 Series routers further optimizes VPN encryption performance. Through offloading encryption tasks to the VPN module, the router processor is freed to handle other operations. The VPN module accelerates the rate at which encryption occurs, speeding the process of transmitting secure data, and this factor is critical when using 3DES encryption.

*The VPN hardware encryption module is included on Cisco 1711 and 1712 Security Access Routers and optional on all other Cisco 1700 Series routers.

Intrusion Detection

Preventing unauthorized users from entering the corporate network is an essential role of any security system. A network-based IDS provides around-the-clock network surveillance, analyzing packets and data streams and searching for signs of unauthorized activity. When it identifies unauthorized activity, the IDS can generate alarms to alert network managers for immediate response and corrective action.

Through Cisco IOS Software, Cisco 1700 Series routers can provide customers with an integrated IDS solution. With this feature deployed, businesses can benefit from continuous security monitoring to detect unauthorized activity that may occur over the Internet or other unsecured networks.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

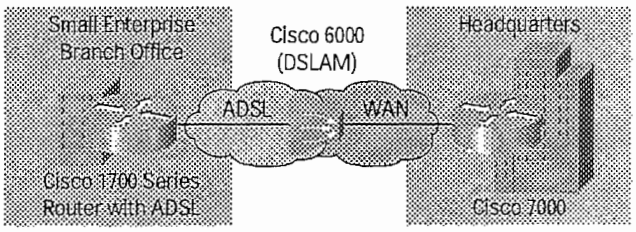
Security Device Manager (SDM)

Cisco SDM is an intuitive, Web-based device management tool embedded within the Cisco 1700 access routers. Cisco SDM simplifies router and security configuration through smart wizards enabling customers to quickly and easily deploy, configure and monitor a Cisco 1700 access router without requiring knowledge of Cisco IOS Software Command Line Interface (CLI).

Business-Class DSL

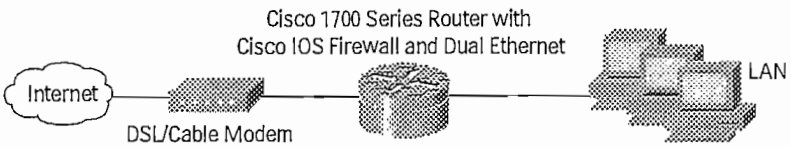
The Cisco 1700 Series supports business-class DSL through the optional ADSL or symmetrical high-bit-rate DSL (G.shdsl) WICs, or with the 1701 which has a built in ADSL port. The Cisco 1700 Series business-class DSL solution combines the cost benefits of DSL service with the advanced routing capability required for business use of the Internet. Cisco business-class DSL delivers advanced QoS and industry-proven reliability. Through enhanced DSL QoS features, performance levels for mission-critical applications and toll-quality voice/data integration are maintained. (Refer to Figure 2.)

Figure 2
The Cisco 1700 Series Deployed with an ADSL WIC



Cisco 1711 and 1712 routers, and Cisco 1721, 1751, 1760 routers with optional Ethernet WIC, support dual Ethernet configuration, enabling deployment with an external broadband modem (such as DSL, cable modem, or wireless modem)—often supplied by a service provider (Figure 3).

Figure 3
The Cisco 1700 Series Deployed with an Ethernet WIC and an External DSL or Cable Modem



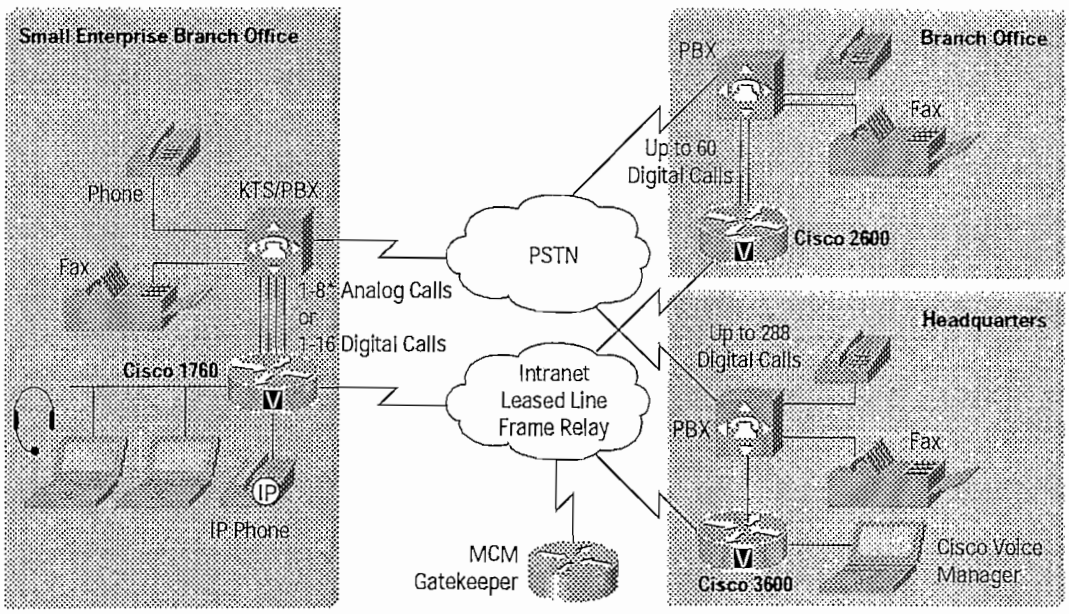
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Multiservice Data/Voice/Video/Fax Integration

In addition to supporting the same security and business-class DSL features as the entire Cisco 1700 Series, the Cisco 1751 and 1760 provide a cost-effective way to extend multiservice (data and voice) networks to branch offices. Using the sophisticated QoS features of Cisco IOS Software, the Cisco 1751 and 1760 allow voice traffic to be digitized, encapsulated in data packets, and prioritized over other data traffic. Data/voice/video/fax integration using IP protocols over the Internet enables administrators to reduce long-distance toll charges between offices and support voice-enabled desktop applications such as integrated messaging and packet video.

The Cisco 1751 and 1760 support analog and digital voice communications while working with the existing telephone infrastructure—such as phones, fax machines, KTSs, and PBXs—thus minimizing capital costs by reducing the need for additional equipment expenditure. In addition, these routers provide for easy deployment of IP telephony. (Refer to Figure 4.)

Figure 4
Multiservice Data/Voice/Fax Integration



* 1 WIC slot is left for WAN access. The maximum number of analog calls for the Cisco 1760 is 8.

Enhancements to Cisco IOS Software allow the Cisco 1751 and 1760 to support survivable remote site telephony (SRST). This feature allows branch offices to utilize key telephony features such as hold and call forwarding if the main call server fails. Recently introduced VIC cards support direct inward dial (DID), allowing customers to directly reach key employees and caller ID (CLID) ensures that employees can identify and respond to important customer calls.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Manageability

Cisco 1700 Series routers support a wide range of network installation and management tools:

- *SDM*—Cisco SDM is a Web-based device management tool embedded within the Cisco IOS access routers. Using smart wizards, SDM simplifies router and security configuration enabling customers to quickly and easily deploy, configure and monitor a Cisco access router without requiring knowledge of Cisco IOS Software Command Line Interface (CLI).
- *CiscoView*—This GUI-based device management software application for UNIX and Windows platforms provides dynamic status, statistics, and comprehensive configuration information.
- *CiscoWorks*—This industry-leading, Web-based network management suite simplifies tasks such as network inventory management and device change, rapid software image deployment, and troubleshooting from a central location.
- *Cisco Secure Policy Manager*—This Windows NT-based application allows users to define, configure, distribute, enforce, and audit network-wide security policies, simplifying Cisco IOS firewalls, VPNs, and IDS deployments.
- *Cisco QoS Policy Manager*—This tool offers the ability to define QoS policies across multiple devices, easing the task of creating and configuring QoS policies for users and applications.
- *Cisco Voice Manager*—This application enables configuration and provisioning of voice ports, and creation and modification of dial plans on voice-enabled Cisco routers for VoIP and VoFR.

Cisco 1700 Series Business Features

The Cisco 1700 Series offers a comprehensive feature set designed to enable small to medium-sized businesses and small enterprise branch offices to connect to the Internet and to the corporate intranet. For a complete description of platform features and benefits, refer to Table 3.

Table 3 Benefits and Features of the Cisco 1700 Series

Features	Benefits
Flexibility	
Full Cisco IOS Software support, including multiprotocol routing (IP, IPX[1], AppleTalk, IBM/SNA[2]) and bridging	• Provides the industry's most robust, scalable, and feature-rich internetworking software support using the accepted standard networking software for the Internet and private WANs • Constitutes part of the Cisco end-to-end network solution
Integrated voice and data networking	
Cisco 1751 and 1760 routers accept both WAN and voice interface cards	• Reduces long-distance toll charges by allowing the data network to carry interoffice voice and fax traffic • Works with existing handsets, key units, and PBXs, eliminating the need for a costly phone-equipment upgrade

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 3 Benefits and Features of the Cisco 1700 Series

Features	Benefits
Modular architecture	
Accepts an array of WICs and VICs	• Adds flexibility and investment protection
WICs are shared with Cisco 1700, 2600, and 3600 routers	• Reduces cost of maintaining inventory • Lowers training costs for support personnel • Protects investments through reuse on various platforms
Autosensing 10/100 Fast Ethernet	• Simplifies migration to Fast Ethernet performance in the office
Expansion slot on motherboard	• Allows expandability to support hardware-assisted encryption at T1/E1 speeds • Allows support for future technologies
Dual DSP slots (Cisco 1751 and 1760)	• Allows expandability to support additional voice channels
Security	
SDM	• Simplifies router and security configuration through smart wizards to enable customers to quickly and easily deploy, configure and monitor a Cisco access router without requiring knowledge of Cisco IOS Command Line Interface (CLI).
Cisco IOS Firewall feature set includes context-based access control for dynamic firewall filtering, denial-of-service detection and prevention, Java blocking, real-time alerts, IDS, and encryption	• Allows internal users to access the Internet with secure, per-application-based dynamic access control, while preventing unauthorized Internet users from accessing the internal LAN
IPSec DES and 3DES	• Enables creation of VPNs by providing industry-standard data privacy, integrity, and authenticity as data traverses the Internet or a shared public network • Supports up to 168-bit encryption
Hardware-based encryption module	• Supports wire-speed encryption up to T1/E1 speeds
Easy VPN server/remote	• Allows router to act as VPN server to terminate VPN client sessions initiated by Cisco VPN clients • Easy VPN Remote provides ease of deployment by allowing centralized VPN policy pushed from a VPN concentrator to Cisco 1700 router
Device authentication and key management	
IKE[3], X.509v3 digital certification, and support for Certificate Enrollment Protocol (CEP) with certification authorities such as Verisign and Entrust	• Ensures proper identity and authenticity of devices and data • Enables scalability to very large IPSec networks through automated key management
User authentication	
PAP/CHAP, RADIUS, TACACS+	• Supports all leading user identity-verification schemes

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 3 Benefits and Features of the Cisco 1700 Series

Features	Benefits
VPN tunneling	
IPSec, generic routing encapsulation (GRE), L2TP, Layer2 Forwarding (L2F)	• Offers choice of standards-based tunneling methods to create VPNs for IP and non-IP traffic • Allows standards-based IPSec or L2TP client to interoperate with Cisco IOS tunneling technologies • Is fully interoperable with public certificate authorities and IPSec standards-based products • Constitutes part of the scalable Cisco end-to-end VPN solution portfolio
Management	
IEEE 802.1Q VLAN	• Enables efficient traffic separation, provides better bandwidth utilization, and alleviates scaling issues by logically segmenting the physical LAN infrastructure into different subnets
Manageable via SNMP[4] (CiscoView, CiscoWorks2000), Telnet, and console port	• Allows central monitoring, configuration, and diagnostics for all functions integrated in the Cisco 1700 Series Router, reducing management time and costs
Integrated analog modem (optional)	• Allows out-of-band remote management for monitoring and configuration of Cisco 1700 Series routers
Ease of use and installation	
Cisco ConfigMaker, setup configuration utility, color-coded ports/cables, and LED status indicators	• Simplifies and reduces deployment time and costs • Allows quick diagnostics and troubleshooting
Network Address Translation (NAT)	• Simplifies deployment and reduces Internet access costs
QoS	
CAR[5], Policy Routing, WFQ[6], PQ/CBWFQ[7], GTS[8], RSVP[9], DSCP[10], cRTP[11], MLP[12], and LFI[13]	• Allocates WAN bandwidth to priority applications for improved performance
Reliability and scalability	
Cisco IOS Software, dial-on-demand routing, dual-bank Flash memory, scalable routing protocols such as OSPF[14], EIGRP[15], and HSRP[16]	• Improves network reliability and enables scalability to large networks
Broadband connectivity options	
DSL connectivity delivers business-class broadband access	• Takes advantage of broadband access technologies such as DSL to increase WAN connectivity speeds and reduce WAN access costs • Supports ADSL connectivity with ADSL WIC • Supports G.shdsl connectivity with the G.shdsl WIC • Supports cable connectivity with the Cisco 1700 Series and optional integrated Cisco uBR 910 Series Universal Broadband Router cable DSU to deliver business-class broadband access

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 3 Benefits and Features of the Cisco 1700 Series

Features	Benefits
Device integration	
Integrated router, voice gateway, firewall, encryption, VPN tunnel server, DSU/CSU[17], and NT1 in a single device	• Reduces costs and simplifies management • Offers voice gateway functionality (Cisco 1751/1760)

1. Internetwork Packet Exchange
2. Systems Network Architecture
3. Internet Key Exchange
4. Simple Network Management Protocol
5. Committed Access Rate
6. Weighted Fair Queuing
7. Priority Queuing/Class-Based WFQ
8. Generic traffic shaping
9. Resource Reservation Protocol
10. Differentiated services code point
11. Real-Time Transport Protocol
12. Multilink PPP
13. Link Fragmentation and Interleaving
14. Open Shortest Path First
15. Enhanced Interior Gateway Routing Protocol
16. Hot Standby Router Protocol
17. Data service unit/Channel service unit

Cisco IOS Technology

Cisco IOS Software is an innovative and feature-rich network system software that offers networks intelligence and agility. It allows the effective deployment of new applications and services quickly and without disruption—applications and services that enable your customer's business to generate revenue, reduce costs, and improve customer service.

Service and Support

Technical Support Services

Technical Support Services for the Cisco 1700 Series are available through Cisco SMARTnet™ and SMARTnet Onsite service programs. Cisco SMARTnet support augments the resources of business operations staff; it provides access to a wealth of expertise, both online and via telephone; it provides the ability to refresh system software at will; and it offers a range of hardware Advance Replacement options. Table 4 details the features and benefits of Cisco SMARTnet offerings.

Table 4 Cisco SMARTnet Features and Benefits

Technical Support Services	Features	Benefits
Cisco SMARTnet Support Cisco SMARTnet Onsite Support	Access 24 x 7 to software updates Web access to technical repositories Telephone support through the Technical Assistance Center (TAC) Advance Replacement of hardware parts	Enables proactive or expedited issue resolution Lowers cost of ownership by utilizing Cisco expertise and knowledge Minimizes network downtime

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Cisco SMARTnet Onsite provides all Cisco SMARTnet services and complements the hardware Advance Replacement feature by adding the services of a field engineer, offering support that can be critical for those locations where staffing is insufficient or unavailable to perform parts replacement activities.

Technical Support Services Delivery

Cisco SMARTnet support is available to customers from both Cisco directly and through Cisco's channel partners.

How to Order

To order a Cisco 1700 Series Modular Access Router contact your local Cisco reseller. To find the one nearest you, visit the Cisco Reseller Locator at:

http://www.cisco.com/warp/partner/psp/locator.html

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

LW4881 07/03 MS9/03