ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REDISEÑO DE LA RED MPLS CON SOPORTE DE IPv6 EMPLEANDO LAS MEJORES PRÁCTICAS DE SEGURIDAD PARA EL SISTEMA AUTÓNOMO DE TELCONET S.A. DE LA CIUDAD DE QUITO

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

LIZETH PATRICIA AGUIRRE SÁNCHEZ
lizeth.aguirre@ieee.org

DIRECTOR: RAÚL DAVID MEJÍA NAVARRETE
david.mejia@epn.edu.ec

CODIRECTOR: FABIO MATÍAS GONZÁLEZ GONZÁLEZ
fabio.gonzalez@epn.edu.ec

Quito, Marzo 2013

DECLARACIÓN

Yo, Lizeth Patricia Aguirre Sánchez, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis 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.

Lizeth Patricia Aguirre Sánchez

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Lizeth Patricia Aguirre Sánchez, bajo mi supervisión.

MSc. David Mejía
DIRECTOR DE PROYECTO

Ing. Fabio González
CODIRECTOR DE PROYECTO

AGRADECIMIENTOS

Las palabras nunca serán suficientes para agradecerles, no solo su apoyo sino su gran amistad a todos quiénes forman parte del personal de Telconet S.A. En especial, mi eterno agradecimiento al Ing. Hugo Proaño que con su cariño me ha facilitado la realización de este proyecto. A él, por ser la persona de quién nunca conocí un “no”, sino siempre un “con mucho gusto”.

Al Ing. Gustavo Alarcón y todo el departamento de ventas, por su gran acogida y apoyo. Al Ing. Jorge Pazos y al departamento IAC. A la Ing. Anita Carpio por su paciencia. Al Ing. Javier Cervantes por su ayuda y amistad.

De corazón mi indiscutible agradecimiento al departamento de *Networking* que con su apoyo hicieron única mi estadía en Telconet S.A. A los ingenieros: Patricio García, Milton Tipán, Ma. Isabel Proaño, Milton Simbaña, Rouse Muñoz y en especial, a Víctor Álvarez que más que un jefe fue un verdadero amigo. Finalmente, a quién considero mi hermano mayor, no solo por su ayuda en este proyecto sino por sus consejos, el Ing. Adrián Bonilla.

Al Ing. Andrés Almeida por su guía y colaboración, por abrirme las puertas a la solución práctica. A los ingenieros: Patricio Cueva, Javier Villagrán, Ernesto Rodríguez, Carlos Medina, Óscar Herrán, Miguel Vaca, Diana Apolo, John Paredes, Johanna Fonte y Milton Chanatasig.

Al Ing. Juan Pablo Jiménez por su comprensión y ayuda en los trámites de este proyecto, pero sobre todo por ser un gran amigo. A mi gran profesor, el Ing. Andrés Cervantes que sin duda, ha sido el mejor hermano que pude haber deseado. A David Domínguez, Diego Gallo, Víctor López, Cristian Arévalo, Fabián Enríquez y cada persona del proyecto 3G de quiénes he aprendido mucho; pero en especial, mi eterno agradecimiento a Diego Mina por ser mi confidente, mi apoyo y la persona de quién menos he esperado, pero sin duda de la que más he recibido. Muchas Gracias.

Al Ing. Enrique Proaño por su guía y comprensión en Cisco y en la realización de este proyecto. A Telmo Puente, por su apoyo incondicional y gran corazón.

A mi Universidad y sus profesores. A la MSc. Ma. Soledad Jiménez por ser más que mi profesora, una gran amiga. Al Ing. Pablo Hidalgo por sus consejos e inculcarme el amor a mi carrera. Pero en especial a los mentores de este proyecto, a mi director MSc. David Mejía y codirector Ing. Fabio González muchas gracias, no solo por el apoyo durante este tiempo sino por los últimos 5 años de mi vida, les estaré eternamente agradecida.

A todos gracias, siempre podrán contar conmigo.

DEDICATORIA

A mi Dios, por ser mi camino y la primera persona con la que hablo en el día. A Él por acompañarme en mis problemas y alegrías.

A mi papi, que con su ejemplo me ha impulsado a ser mejor. A ese mi hombre perfecto con los deseos más grandes de superación, por quién aprendí a conducir y amar con todo mi corazón a la naturaleza.

A mi mami, que ha sabido guiarme en cada decisión de mi vida. A ella por ser una gran mujer, amiga y la mejor madre de este mundo. Pude haberla deseado diferente pero no mejor, su grandeza es única.

A las dos personitas que más problemas me han traído en esta vida pero indiscutiblemente las que más adoro, mis hermanas Andy y Cris.

A la familia Sánchez Vaca, por ser mis segundos padres. Por apoyarme y confiar en mí siempre, por su amor y hacerme parte de su familia. ¡Los adoro!

A la familia Carrión Sánchez, por quererme como una hija más y compartir conmigo momentos únicos. Gracias.

A mi familia por su cariño. Abuelitos, tíos y primos por ser mi base en la ciudad de Quito y en especial, al Sr. Roberto Sánchez por ser más que mi tío, mi amigo.

A las personas con quién compartí estos cinco años de carrera. A Fernando Guaygua, Jorge Guijarro, Rodrigo Jarrín, Daniel Dávalos, Sergio Narváez, Fernanda Quezada, Gissela Cabezas, Álvaro López, César Palacios, Luis Paredes, Bruno Samaniego, Jorge Live, Genny Enríquez, Diana Talavera y Diego Mediavilla.

A todos, quiénes se han ganado mi corazón con el tiempo.

ÍNDICE

CAPÍTULO 1

FUNDAMENTOS TEÓRICOS

1.1 TECNOLOGÍA *MULTIPROTOCOL LABEL SWITCHING* (MPLS)..... 1
1.1.1 INTRODUCCIÓN 1
1.1.2 DEFINICIÓN Y CARACTERÍSTICAS DE MPLS..... 1
1.1.3 COMPONENTES DE MPLS 2
1.1.3.1 *Label Switched* Routers (LER)..... 2
1.1.3.2 *Label Edge* Routers (LER)..... 3
1.1.3.3 *Forwarding Equivalence Class* (FEC)..... 4
1.1.3.4 *Label Switched Path* (LSP)..... 5
1.1.4 ETIQUETA..... 7
1.1.5 FORMATO DE LA ETIQUETA..... 7
1.1.5.1 Etiqueta MPLS..... 8
1.1.5.2 Bits EXP..... 9
1.1.5.3 Bit S 9
1.1.5.4 TTL..... 9
1.1.6 ARQUITECTURA DE LOS NODOS MPLS..... 10
1.1.6.1 Plano de Control 11
1.1.6.2 Plano de Datos 12
1.1.6.3 Funcionalidades de los routers LSR y LER..... 12
1.1.7 EXTRACCIÓN DE ETIQUETAS EN EL PENÚLTIMO SALTO (PHP).... 15
1.1.8 PROTOCOLO DE DISTRIBUCIÓN DE ETIQUETAS (LDP)..... 16
1.1.9 APLICACIONES DE MPLS..... 17
1.1.9.1 Redes Privadas Virtuales (VPN)..... 17
1.1.9.2 Calidad de Servicio (QoS)..... 22
1.1.9.3 Ingeniería de Tráfico (TE)..... 30

1.2 PROTOCOLO DE INTERNET VERSIÓN 6..... 34
1.2.1 INTRODUCCIÓN..... 34
1.2.2 PROTOCOLO DE INTERNET VERSIÓN 4 (IPv4)..... 34

1.2.2.1 Definición de IPv4 34
1.2.2.2 Formato de la cabecera IPv4 35
1.2.2.3 Direccionamiento en IPv4 37
1.2.3 PROTOCOLO DE INTERNET VERSIÓN 6 38
1.2.3.1 Definición de IPv6 38
1.2.3.2 Antecedentes de IPv6 39
1.2.3.3 Formato de la cabecera IPv6 39
1.2.3.4 Cabeceras de extensión de IPv6 41
1.2.3.5 Direccionamiento en IPv6 42
1.2.3.6 Motivos para migrar a IPv6 45

1.3 MECANISMOS DE TRANSICIÓN IPv4/IPv6 SOBRE MPLS 46
1.3.1 IPv6 SOBRE CIRCUITOS DE TRANSPORTE EN MPLS 47
1.3.2 IPv6 CON TÚNELES EN LOS ROUTERS CE 48
1.3.3 IPv6 EN ROUTERS PE (6PE/6VPE) 49
1.3.4 IPv6 SOBRE UNA RED MPLS/IPv6 50

1.4 SEGURIDAD EN IPv6 51
1.4.1 INTRODUCCIÓN 51
1.4.2 SEGURIDAD EN LAS REDES IPv4/IPv6 52
1.4.3 SEGURIDAD EN REDES IPv4 53
1.4.4 SEGURIDAD EN REDES IPv6 54
1.4.5 MEJORES PRÁCTICAS DE SEGURIDAD EN IPv6 55
1.4.5.1 VLAN 56
1.4.5.2 Listas de Control de Acceso en IPv6 58
1.4.5.3 Acceso remoto seguro en IPv6 59

CAPÍTULO 2

SITUACIÓN ACTUAL DEL PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES TELCONET S.A.

2.1 BREVE DESCRIPCIÓN DE LA RED DE TELCONET S.A. 68
2.1.1 INTRODUCCIÓN 68

2.1.2 SITUACIÓN ACTUAL DEL *BACKBONE* DE TELCONET S.A. 69
2.1.2.1 Interconexión del *backbone* hacia las Salidas Internacionales 72
2.1.2.2 Descripción de los componentes de la red de Quito de Telconet S.A. 72
2.1.2.2.1 Componentes de la capa núcleo 73
2.1.2.2.2 Componentes de la capa distribución 76
2.1.2.2.3 Componentes de la capa acceso 79
2.1.2.3 Componentes de los nodos 81
2.1.2.4 Descripción de la fibra óptica de Telconet S.A. 84
2.1.3 TIPOS DE CLIENTES DE TELCONET S.A. 86
2.1.3.1 Clientes corporativos VIP 86
2.1.3.2 Clientes corporativos 86
2.1.4 DESCRIPCIÓN DE LOS ACUERDOS DE NIVEL DE SERVICIOS (SLA) DE TELCONET S.A. 86
2.1.5 PROTOCOLOS UTILIZADOS EN LA RED DE TELCONET S.A. 88

2.2 DIMENSIONAMIENTO DE TRÁFICO DE TELCONET S.A. 89
2.2.1 NÚMERO DE CLIENTES 91
2.2.1.1 Porcentaje de crecimiento 93
2.2.1.2 Regresión y extrapolación logarítmica 96
2.2.2 VENTAS FACTURADAS 99
2.2.2.1 Porcentaje de crecimiento 100
2.2.2.2 Regresión y extrapolación polinomial de segundo orden 101
2.2.3 PORCENTAJE DE CRECIMIENTO DE TELCONET S.A.-QUITO 104
2.2.4 REQUERIMIENTOS Y ANÁLISIS DE TRÁFICO PARA EL REDISEÑO DE LA RED MPLS DE TELCONET S.A.-QUITO 104
2.2.4.1 Mecanismo 1: Análisis de tráfico mediante las capacidades contratadas 105
2.2.4.2 Mecanismo 2: Análisis de tráfico mediante la herramienta Cacti . 116
2.2.4.3 Resultado del análisis de los mecanismos 1 y 2 125
2.2.5 ANÁLISIS DEL USO DEL CPU DE LOS EQUIPOS 126

CAPÍTULO 3

REDISEÑO DE LA RED MPLS CON SOPORTE PARA IPV6

3.1 INTRODUCCIÓN 132

3.2 IPv6 SOBRE LA TECNOLOGÍA MPLS 133
3.2.1 SELECCIÓN DEL MECANISMO DE TRANSICIÓN IPv4/IPv6 135
3.2.2 MECANISMO: IPv6 EN ROUTERS PE (6PE/6VPE) 135

3.3 REDES PRIVADAS VIRTUALES (VPN) EN LA TECNOLOGÍA MPLS 136
3.3.1 LAS VPN DE MPLS DE CAPA 2 (VPWS)..... 136
3.3.2 LAS VPN DE MPLS DE CAPA 3..... 138

3.4 CALIDAD DE SERVICIO (QoS) EN LA TECNOLOGÍA MPLS 140
3.4.1 REQUERIMIENTOS DE QOS Y PARÁMETROS DE LOS SLA DE TELCONET S.A. 140
3.4.2 DESIGNACIÓN DE LOS PHB 142
3.4.3 MAPA DE CORRESPONDENCIAS DSCP - EXP..... 143
3.4.4 DEFINICIÓN DE LA POLÍTICA PARA LIMITAR LA CAPACIDAD DE TRÁFICO 143
3.4.5 DEFINICIÓN DE LA POLÍTICA PARA DEFINIR EL MAPA DE CORRESPONDENCIAS ENTRE LOS CAMPOS DSCP Y EXP DEL PAQUETE144
3.4.6 DEFINICIÓN DE LAS POLÍTICAS PARA EL MANEJO DE LA CONGESTIÓN DE LA CAPA NÚCLEO..... 144
3.4.7 MANEJO DE LA CONGESTIÓN EN LAS CAPAS DISTRIBUCIÓN Y ACCESO..... 146

3.5 INGENIERÍA DE TRÁFICO EN LA TECNOLOGÍA MPLS..... 147
3.5.1 BALANCEO DE CARGA..... 148
3.5.2 REDUNDANCIA DE ENLACES 149
3.5.3 PROTOCOLO DE ENRUTAMIENTO PARA REDES MPLS CON TE .. 150
3.5.4 PROTOCOLO DE SEÑALIZACIÓN PARA REDES MPLS CON TE..... 151

3.6 MEJORES PRÁCTICAS DE SEGURIDAD EN IPv6..... 152
3.6.1 VLAN..... 152

3.6.1.1 Definición de las VLAN 153
3.6.1.2 Definición de la VLAN de administración 153
3.6.1.3 Definición de la puerta de salida por defecto 154
3.6.2 LISTAS DE CONTROL DE ACCESO EN IPv6 (ACL)..... 154
3.6.3 ACCESO REMOTO SEGURO EN IPv6..... 155

3.7 TOPOLOGÍA FÍSICA DE LA RED DE TELCONET S.A. 157
3.7.1 CAPA NÚCLEO 158
3.7.1.1 Routers LSR 158
3.7.1.2 Routers LER 160
3.7.2 CAPA DISTRIBUCIÓN..... 164
3.7.3 CAPA ACCESO 167
3.7.4 DIRECCIONAMIENTO IP 169
3.7.4.1 Direccionamiento IPv4 169
3.7.4.2 Direccionamiento IPv6 172

3.8 SELECCIÓN DEL HARDWARE Y SOFTWARE 173
3.8.1 CAPA NÚCLEO 174
3.8.2 CAPA DISTRIBUCIÓN..... 179
3.8.3 CAPA ACCESO 182

3.9 COSTOS REFERENCIALES..... 185

CAPÍTULO 4

CONFIGURACIÓN E IMPLEMENTACIÓN DEL PROTOTIPO DE LA RED DISEÑADA

4.2 CONFIGURACIÓN DE LA RED DISEÑADA 193
4.2.1 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO OSPF.. 196
4.2.2 CONFIGURACIÓN DE LAS VLAN EN LOS SWITCHES..... 197
4.2.3 CONFIGURACIÓN DE LA TECNOLOGÍA MPLS 199
4.2.4 CONFIGURACIÓN DE MP-BGP..... 200
4.2.5 CONFIGURACIONES DE IPv6 EN ROUTER PE (6PE/6VPE)..... 201

4.2.5.1 Configuración de 6PE 201
4.2.5.2 Configuración de 6VPE 203
4.2.6 APLICACIONES DE MPLS 206
4.2.6.1 Configuraciones de VPN de MPLS 206
4.2.6.2 Configuración de Calidad de Servicio 210
4.2.6.3 Configuración de Ingeniería de Tráfico 226
4.2.7 CONFIGURACIÓN DE SEGURIDAD EN IPv6 230
4.2.7.1 VLAN 230
4.2.7.2 Listas de Control de Acceso (ACL) en IPv6 232
4.2.7.3 Gestión de acceso remoto seguro 233

4.3 PROTOTIPO DE LA RED DISEÑADA 235
4.3.1 CONFIGURACIÓN BÁSICA DE LOS DISPOSITIVOS DE RED 239
4.3.2 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO OSPF .. 240
4.3.3 CONFIGURACIÓN DE LAS VLAN EN LOS SWITCHES 241
4.3.4 CONFIGURACIÓN DE LA TECNOLOGÍA MPLS 242
4.3.5 CONFIGURACIÓN DE MP-BGP 244
4.3.6 CONFIGURACIONES DE IPv6 EN ROUTERS PE (6PE/6VPE) 245
4.3.6.1 Configuración de 6PE 245
4.3.6.2 Configuración de 6VPE 246
4.3.7 APLICACIONES DE MPLS 249
4.3.7.1 Configuraciones de las VPN de MPLS 249
4.3.7.1.2 Las VPN de MPLS de capa 3 en IPv4 253
4.3.7.1.3 Las VPN de MPLS de capa 3 de doble pila 255
4.3.7.2 Configuración de Calidad de Servicio 256
4.3.7.3 Configuración de Ingeniería de Tráfico 265
4.3.8 CONFIGURACIÓN DE SEGURIDAD EN IPv6 274
4.3.8.1 VLAN 274
4.3.8.2 Listas de Control de Acceso (ACL) en IPv6 274
4.3.8.3 Gestión de acceso remoto seguro 275

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES 280

5.2 RECOMENDACIONES 283

REFERENCIAS BIBLIOGRÁFICAS

ANEXOS

ÍNDICE DE FIGURAS

CAPÍTULO 1

Figura 1.1 Enrutador LSR 3
Figura 1.2 Enrutador LER 4
Figura 1.3 Asignación de un paquete a una clase FEC 5
Figura 1.4 Camino de etiquetas conmutadas 6
Figura 1.5 Cabecera MPLS 8
Figura 1.6 Campo TTL en la Red MPLS 10
Figura 1.7 Arquitectura de los LER 14
Figura 1.8 Arquitectura de los LSR 14
Figura 1.9 Red MPLS **(a)** sin PHP **(b)** con PHP 15
Figura 1.10 Definición de las VRF en un router 21
Figura 1.11 Campo DiffServ (DS) 24
Figura 1.12 Diferencias entre SRR y WRR 28
Figura 1.13 Cabecera IPv4 35
Figura 1.14 Cabecera IPv6 fija 40
Figura 1.15 Paquete IPv6 41
Figura 1.16 IPv6 sobre Circuitos de Transporte sobre MPLS 48
Figura 1.17 IPv6 con Túneles en los routers CE 49
Figura 1.18 IPv6 Provider Edge Routers 50
Figura 1.19 IPv6 sobre un Core MPLS/IPv6 51

CAPÍTULO 2

Figura 2.1 Interconexión nacional de la red de Telconet S.A. 71
Figura 2.2 Equipos P de la capa núcleo 73
Figura 2.3 Equipos PE de la capa núcleo..... 75
Figura 2.4 Equipos de las capas: núcleo y distribución 78
Figura 2.5 Dispositivos de la red de la sucursal Quito de Telconet S.A. 80
Figura 2.6 APC Smart-UPS 82
Figura 2.7 Banco de baterías del nodo Gosseal..... 83
Figura 2.8 Aire acondicionado del nodo Gosseal 83
Figura 2.9 Racks de Gosseal 84
Figura 2.10 Bobina de FO 85
Figura 2.11 Ventas por producto Quito-2011..... 90
Figura 2.12 Clientes actuales por nodo PE 92
Figura 2.13 Crecimiento anual de clientes de Quito 2007-2012 93
Figura 2.14 Clientes anual de clientes nuevos de Quito 2007-2012..... 94
Figura 2.15 Crecimiento de clientes nuevos 2007-2012..... 95
Figura 2.16 Extrapolación logarítmica 99
Figura 2.17 Ventas facturadas 2007- 2012..... 100
Figura 2.18 Crecimiento de las ventas facturadas 2007-2012..... 101
Figura 2.19 Extrapolación polinomial de segundo orden 104
Figura 2.20 Instituciones del proyecto CEDIA 108
Figura 2.21 Transmisión de vídeo 110
Figura 2.22 Esquema de servicios del Data Center de Telconet S.A.-Quito 114
Figura 2.22 Tráfico PE1SUR2, 2007-2012 117
Figura 2.23 Tráfico PE1SUR2, mayo 2011- mayo 2012..... 117
Figura 2.24 Tráfico PE1SUR2, enero - mayo 2012 118
Figura 2.25 Tráfico PE1ARMENIA, mayo 2011 - mayo 2012..... 119
Figura 2.26 Tráfico PE1ARMENIA, enero - mayo 2012 119
Figura 2.27 Tráfico PE1BORROMONI, mayo 2011 – mayo 2012 120
Figura 2.28 Tráfico PE1BORROMONI, febrero - mayo 2012 120
Figura 2.29 Tráfico PE1DATACENTER, mayo 2011 - mayo 2012..... 121
Figura 2.31 Tráfico PE1GOSSEAL, junio 2011- mayo 2012 122

Figura 2.32 Tráfico PE1GOSSEAL, enero - mayo 2012 122
Figura 2.33 Tráfico PE1MUROS, mayo 2011- mayo 2012 123
Figura 2.34 Tráfico PE1MUROS, enero - mayo 2012 123

CAPÍTULO 3

Figura 3.1 VPN de capa 2 punto a punto 137
Figura 3.2 VPN de capa 3 en IPv4 e IPv6 139
Figura 3.3 Esquema de balanceo de carga 148
Figura 3.4 Esquema de redundancia de enlaces 149
Figura 3.5 Accesos remotos permitidos y denegados 156
Figura 3.6 Interconexión de los LSR 160
Figura 3.7 Dispositivos LER y LSR 161
Figura 3.8 Capacidades de los enlaces de los agregadores 165
Figura 3.9 Red rediseñada de la sucursal Quito de Telconet S.A. 168
Figura 3.10 Esquema de direccionamiento IPv4 para los switches 170
Figura 3.11 Esquema de direccionamiento para los switches de acceso 171
Figura 3.12 Esquema de direccionamiento IPv6 173

CAPÍTULO 4

Figura 4.1 Prototipo de la red MPLS con soporte para IPv6 de Telconet S.A.-UIO 237
Figura 4.2 Acceso al dispositivo mediante nombre de usuario y contraseña 239
Figura 4.3 Verificación resumida del estado de las interfaces 239
Figura 4.4 Verificación de la tabla de enrutamiento 240
Figura 4.5 Verificación de la tabla de enrutamiento con OSPF 240
Figura 4.6 Verificación de los vecinos OSPF establecidos 241
Figura 4.7 Verificación de las interfaces asociadas a cada VLAN 241
Figura 4.8 Verificación de las interfaces troncales 242
Figura 4.9 Verificación de la tabla LFIB 242
Figura 4.10 Verificación de los parámetros LDP 243
Figura 4.11 Verificación de la tabla FIB 243
Figura 4.12 Verificación de los vecinos LDP 244

Figura 4.13 Verificación de las sesiones BGP establecidas 244
Figura 4.14 Verificación de las sesiones MP-BGP establecidas 245
Figura 4.15 Verificación de la tabla de enrutamiento de IPv6..... 245
Figura 4.16 Verificación del estado de la conexión remota con PE1GOSSEAL 246
Figura 4.17 Verificación del estado de la conexión remota con PE1MUROS ... 246
Figura 4.18 Verificación de la tabla de enrutamiento de la VRF INTERNET 246
Figura 4.19 Verificación de la sesión MP-BGP IPv6 activada 247
Figura 4.20 Comando “ping” a la red del cliente en IPv6 desde el PE1MUROS 247
Figura 4.21 Verificación del estado resumido de las interfaces en IPv6..... 248
Figura 4.22 Verificación de la tabla de enrutamiento en IPv6..... 248
Figura 4.23 Comando “ping” a la red del cliente en IPv6 desde el CE 249
Figura 4.24 Verificación del estado de la VPN de capa 2..... 250
Figura 4.25 Verificación detallada del estado de la VPN de capa 2 250
Figura 4.26 Prototipo de la red con las VPN de capa 2..... 251
Figura 4.27 Verificación de la conectividad hacia la PC remota 252
Figura 4.28 Verificación de las direcciones físicas MAC en las P_CCOLON 252
Figura 4.29 Verificación de la Tabla MAC 253
Figura 4.30 Verificación tabla de enrutamiento de la VRF CLIENTE 253
Figura 4.31 Verificación de la sesión vpnv4 254
Figura 4.32 Comando “ping” a la red del CLIENTE desde el PE1MUROS 254
Figura 4.33 Verificación de la tabla de enrutamiento de la VRF CLIENTE..... 255
Figura 4.34 Comando “ping” a la red del CLIENTE desde el PE1MUROS 255
Figura 4.35 Verificación de la conectividad desde el PE1MUROS..... 256
Figura 4.40 Diagrama Nodos MPLS Prototipo QoS 257
Figura 4.36 Prototipo de la red con QoS 257
Figura 4.37 Verificación de la conectividad desde el CE1COLON 258
Figura 4.38 Verificación de la velocidad de tráfico de entrada de 2 Mbps..... 258
Figura 4.39 Verificación de la configuración de la política..... 259
Figura 4.40 Verificación de la configuración de las clases 259
Figura 4.41 Verificación de los paquetes descartados 260
Figura 4.42 Verificación de los parámetros de la política de la interfaz gi0/0 260
Figura 4.43 Verificación de la configuración de MLS..... 261
Figura 4.44 Verificación de los parámetros de las colas de entrada 261

Figura 4.45 Verificación de los parámetros de las colas de salida 261
Figura 4.46 Verificación de la política de entrada en la gi0/1.11 262
Figura 4.47 Verificación del comando “ping” con saturación 263
Figura 4.48 Verificación del tráfico de llegada al router CE 263
Figura 4.49 Verificación de la política de entrada en la gi0/1.22 264
Figura 4.50 Verificación del comando “ping” en IPv4 y ToS en 184 264
Figura 4.51 Verificación del comando “ping” en IPv6 y ToS en 184 265
Figura 4.52 Prototipo de la red con TE - balanceo de carga 266
Figura 4.53 Verificación de RSVP 266
Figura 4.54 Verificación detallada de las configuraciones del túnel 1 267
Figura 4.55 Verificación de la tabla de enrutamiento..... 267
Figura 4.56 Verificación del balanceo de carga asimétrico 268
Figura 4.57 Verificación del balanceo de carga asimétrico 268
Figura 4.58 Verificación del estado de los túneles 268
Figura 4.59 Prototipo de la red con TE – redundancia de enlaces túneles 1 y 10 269
Figura 4.60 Verificación de la configuración de Fast Re-Route..... 270
Figura 4.61 Verificación de los estados de los túneles creados 270
Figura 4.62 Verificación del estado listo de la interfaz gi0/1 con el túnel 10..... 271
Figura 4.63 Comando “ping” continuo 2500 271
Figura 4.64 Verificación del estado del túnel de respaldo en activo 272
Figura 4.65 Prototipo de la red con TE – redundancia de enlaces túneles 3 y 30 272
Figura 4.66 Verificación del estado del túnel 3 273
Figura 4.67 Comando “ping” continuo hacia 1.1.1.1 273
Figura 4.68 Habilitar la plantilla de doble pila 274
Figura 4.69 Verificación de la configuración de las ACL 275
Figura 4.70 Verificación de las ACL configuradas 275
Figura 4.71 Verificación de las configuraciones de las líneas VTY 276
Figura 4.72 Verificación de la gestión remota..... 276

ÍNDICE DE TABLAS

CAPÍTULO 1

Tabla 1.1 Assured Forwarding PHB 26
Tabla 1.2 Clases de direcciones IPv4 37
Tabla 1.3 Direcciones privadas IPv4 38
Tabla 1.4 Direcciones privadas IPv6 43

CAPÍTULO 2

Tabla 2.1 Proveedores internacionales de Telconet S.A. 72
Tabla 2.2 Características técnicas de los P 74
Tabla 2.3 Módulos de las interfaces de los P 74
Tabla 2.4 Características técnicas de los PE 76
Tabla 2.5 Módulos de las interfaces de los PE 76
Tabla 2.6 Características técnicas de los agregadores 78
Tabla 2.7 Módulos de las interfaces de los agregadores 79
Tabla 2.8 Características técnicas de los switches de acceso 81
Tabla 2.9 Módulos de las interfaces de los switches de acceso 81
Tabla 2.10 Crédito Mensual de Telconet S.A. 88
Tabla 2.11 Número de clientes actuales y velocidades contratadas por servicio 90
Tabla 2.12 Número de clientes actuales y velocidades contratadas por PE 92
Tabla 2.13 Número de clientes 2007-2012 93
Tabla 2.14 Cálculos de la regresión logarítmica 97
Tabla 2.15 Regresión y extrapolación logarítmica 98
Tabla 2.16 Ventas facturadas 2007- 2012 99
Tabla 2.17 Cálculos de la regresión polinomial 102
Tabla 2.18 Regresión Polinomial 103
Tabla 2.19 Requerimientos de Internet dedicado 106
Tabla 2.20 Requerimientos de trasmisión de datos 107
Tabla 2.21 Requerimientos de la IP PBX Gestionado 112
Tabla 2.22 Requerimientos de totales de tráfico del mecanismo 1 115

Tabla 2.23 Valores máximos de las velocidades de subida 124
Tabla 2.24 Valores máximos de las velocidades de bajada 124
Tabla 2.25 Requerimiento totales de tráfico del mecanismo 2..... 125
Tabla 2.26 Requerimientos totales de tráfico..... 126
Tabla 2.27 Uso del CPU de los equipos del backbone de la ciudad de Quito ... 126

CAPÍTULO 3

Tabla 3.1 Cuadro comparativo de los mecanismos de transición IPv4/IPv6..... 134
Tabla 3.2 Numeración de las VPN de capa 2 137
Tabla 3.3 Numeración de las VPN de capa 3 138
Tabla 3.4 Parámetros comprometidos de la voz y el vídeo..... 141
Tabla 3.5 Per-Hop Behaviors..... 142
Tabla 3.6 Mapas de correspondencias 143
Tabla 3.7 Encolamiento de los switches Catalyst 147
Tabla 3.8 Cuadro comparativo OSPF e IS-IS 150
Tabla 3.9 Cuadro comparativo RSVP-TE y CR-LDP 151
Tabla 3.10 Numeración de las VLAN..... 153
Tabla 3.11 Tipos de ACL en IPv4 155
Tabla 3.12 Características de los Ps 159
Tabla 3.13 Versiones de los IOS de Cisco 162
Tabla 3.14 Cambios en los routers LER 163
Tabla 3.15 Cambios en los agregadores 166
Tabla 3.16 Direccionamiento IPv4 para la nube MPLS..... 170
Tabla 3.17 Direccionamiento IPv4 para la nube MPLS..... 173
Tabla 3.18 Cuadro comparativo: routers LER..... 177
Tabla 3.19 Matriz de decisión: LER 178
Tabla 3.20 Cuadro comparativo: agregadores..... 181
Tabla 3.21 Matriz de decisión: agregadores 182
Tabla 3.22 Cuadro comparativo: switches de acceso..... 184
Tabla 3.23 Matriz de decisión: switches de acceso 185
Tabla 3.24 Costos referenciales 186

CAPÍTULO 4

Tabla 4.1 Parámetros de QoS para las colas de entrada 223
Tabla 4.2 Parámetros de QoS para las colas de salida 224
Tabla 4.3 Direccionamiento del prototipo..... 239

ÍNDICE DE ECUACIONES

CAPÍTULO 2

Ecuación 2.1 Disponibilidad de Telconet S.A..... 87
Ecuación 2.2 Regresión logarítmica, sumatoria de (a) 1er grado (b) 2do grado ... 96
Ecuación 2.3 Constante a 97
Ecuación 2.4 Constante b 97
Ecuación 2.5 Obtención de la constante a..... 97
Ecuación 2.6 Obtención de la constante b..... 98
Ecuación 2.7 Función logarítmica estimada..... 98
Ecuación 2.8 Regresión polinomial, sumatoria de (a) 1er grado (b) 2do grado (c) 3er grado 101
Ecuación 2.9 Reemplazo de las sumatorias de (a) 1er grado (b) 2do grado(c) 3er grado 102
Ecuación 2.10 Función polinomial estimada 103

ACRÓNIMOS

AFRINIC	*African Network Information Center*
APNIC	*Asia-Pacific Network Information Centre*
ARIN	*American Registry for Internet Numbers*
ATM	*Asynchronous Transfer Mode*
AToM	*Any Trasport over MPLS*
Bc	*Committed Burst*
Be	*Excess Burst*
BGP	*Border Gateway Protocol*
bps	*bits per second*
CE	*Customer Edge*
CEF	*Cisco Express Forwarding*
CIDR	*Classless Inter-Domain Routing*
CIR	*Committed Information Rate*
CNT	Corporación Nacional de Telecomunicaciones
CoS	*Class of Service*
CPU	*Central Processing Unit*
CR-LDP	*Constrained Based - Routing Label Distribution Protocol*
DEC	*Digital Equipment Corporation*
DNS	*Domain Name System*
DoS	*Denial of Service*
DSCP	*Differentiated Services Code Point*
DWDM	*Dense wavelength Division Multiplexing*
eBGP	*External Border Gateway Protocol*
EEQ	Empresa Eléctrica Quito
EIGRP	*Enhanced Interior Gateway Routing Protocol*
EOMPLS	*Ethernet over MPLS*
ER-LSP	*Explicit Routing - Label Switched Path*
FEC	*Forwarding Equivalence Class*
FIB	*Forwarding Information Base*
HD	*High Definition*
HIM	*Hardware Interface Modules*

HWIC	*High-Performance Wan Interface Cards*
IAC	*Internet Access Control*
IANA	*Internet Assigned Numbers Authority*
iBGP	*Internal Border Gateway Protocol*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IGP	*Interior Gateway Protocol*
IP	*Internet Protocol*
IPng	*Internet Protocol New Generation*
IPSec	*Internet Protocol Security*
IPv4	*Internet Protocol Version 4*
IPv6	*Internet Protocol Version 6*
IS-IS	*Intermediate System - Intermediate System*
ISO	*International Organization for Standarization*
ISP	*Internet Service Provider*
LACNIC	*Latin America & Caribbean Network Information Centre*
LAN	*Local Area Network*
LDP	*Label Distribution Protocol*
LER	*Label Edge Router*
LFIB	*Label Forwarding Information Base*
LIB	*Label Information Base*
LPU	*Line Processing Unit*
LSR	*Label Switched Router*
MAC	*Media Access Control*
MP-BGP	*Multiprotocolo - Border Gateway Protocol*
MPLS	*Multiprotocol Label Switching*
MSTP	*Multi-Spanning Tree*
MTTR	*Mean Time To Repair*
MTU	*Maximum Transmission Unit*
NAT	*Network Address Translation*
NBAR	*Network Based Application Recognition*
NOC	*Network Operation Control*
OSI	*Open Source Interconnection*

OSPF	*Open Shortest Path First*
P	*Provider*
PBX	*Private Branch Exchange*
PDU	*Protocol Data Unit*
PE	*Provider Edge*
PHB	*Per-Hop Behavior*
PHP	*Penultimate Hop Popping*
PKI	*Public-Key Infraestructure*
QoS	*Quality of Service*
RADIUS	*Remote Authentication Dial-In User Server*
RD	*Route Distinguisher*
RFC	*Request For Comments*
RIB	*Routing Information Base*
RIPE	*Réseaux IP Européens*
RIR	*Regional Internet Registry*
RSA	*Rivest, Shamir y Adleman*
RSP	*Route Switch Processor*
RSVP	*ReSource Reservation Protocol*
RSVP-TE	*Resource Reservation Protocol - Traffic Engineering*
RT	*Route Target*
SEND	*SEcure Neighbor Discovery*
SFP	*Small Form-factor Pluggable*
SFU	*Switched Fuse Unit*
SIPP	*Simple Internet Protocol Plus*
SIT	Sistema Integrado de Telconet
SLA	*Service Level Agreement*
SNMP	*Simple Network Management Protocol*
SRU	*Switch and Route Processing Unit*
SSH	*Secure SHell*
TACACS	*Terminal Access Controller Access Control System*
Tc	*Time Committed*
TCP	*Transmission Control Protocol*
TDP	*Tag Distribution Protocol*

TE	*Traffic Engineering*
TINET	*Technology and Infrastructure for Emerging Regions*
TIWS	*Telefónica International Wholesale Services*
TTL	*Time To Live*
UDP	*User Datagram Protocol*
UPS	*Uninterruptible Power Supply*
UTP	*Unshielded Twisted Pair*
VLAN	*Virtual Local Area Network*
VLL	*Virtual Leased line*
VLSM	*Variable Length Subnet Masking*
VNC	*Virtual Network Computing*
VPLS	*Virtual Private LAN Service*
VPN	*Virtual Private Network*
VPWS	*Virtual Private Wire Service*
VRF	*Virtual Routing Forwarding*
VSI	*Virtual Switch Instance*
VTP	VLAN *Trunking Protocol*
WAN	*Wide Area Network*

RESUMEN

El presente proyecto de titulación tiene por objetivo rediseñar la red MPLS con soporte a IPv6, para la sucursal de Quito del Proveedor de Servicios de Internet “Telconet S.A.”. Con el fin de brindar una red más eficiente y segura, se optimiza el uso de los recursos mediante la implementación de las aplicaciones de MPLS y se analizan las Mejores Prácticas de Seguridad en IPv6.

En el primer capítulo, se revisan los conceptos básicos sobre los cuales se desarrolla el proyecto. Se analizan las características de la tecnología MPLS como: su arquitectura, sus componentes, el formato de la cabecera y sus aplicaciones más significativas: Redes Privadas Virtuales (VPN), Calidad de Servicio (QoS) e Ingeniería de Tráfico (TE). Se describen las características más sobresalientes del protocolo de Internet IP en sus versiones 4 y 6, los mecanismos de transición de IPv4 a IPv6 sobre MPLS, y las Mejores Prácticas de Seguridad en IPv6.

En el segundo capítulo, se analiza la situación actual de la infraestructura de la red de TELCONET S.A., el hardware, el software, los Acuerdos de Nivel de Servicio (SLA), los tipos de clientes y los servicios que brinda a nivel nacional, entre otras características de la empresa. Para el dimensionamiento de tráfico, se analizan el número de clientes nuevos y las ventas facturadas en los últimos cinco años (marzo 2007- marzo 2012), a fin de determinar el crecimiento del proveedor y obtener los requerimientos.

En el tercer capítulo, a partir del dimensionamiento de tráfico, se procede a rediseñar la red MPLS/IPv4 del ISP para que tenga soporte a IPv6. En lo referente a QoS, se trabaja con la arquitectura de la IETF Servicios Diferenciados, donde se especifican diferentes clases de servicios (CoS) y prioridades en base a los Acuerdos de Nivel de Servicio (SLA) firmados entre el proveedor y sus clientes. Se implementa Ingeniería de Tráfico para optimizar el uso de los recursos; y las

VPN de MPLS entre las sucursales de los clientes VIP para el servicio de datos, con el fin de mantener garantías de QoS extremo a extremo.

Se selecciona el mejor mecanismo de transición IPv4/IPv6 sobre MPLS para el diseño y se aplican las mejores prácticas de seguridad en IPv6. Se recomiendan el hardware y el software necesarios; y para los equipos que no soportan IPv6, se analiza la posibilidad de cambiar su hardware y/o software a través de una matriz de decisión. Se selecciona aquel equipo o IOS que cumpla con los requerimientos y se estiman los costos referenciales del diseño.

En el cuarto capítulo, se detalla la configuración para el desarrollo del esquema diseñado y se implementa el prototipo de una parte del mismo. Se consideran solo los nodos: Muros y Gosseal para este último.

El quinto capítulo abarca las conclusiones y las recomendaciones obtenidas durante la realización del proyecto.

Los anexos que complementan la información mostrada en los capítulos no se imprimen en este documento debido a su gran extensión.

PRESENTACIÓN

En la última década, el crecimiento de las telecomunicaciones ha sido significativo. Las nuevas aplicaciones, los nuevos servicios y los cambios tecnológicos han dado lugar a que los Proveedores de Servicios de Internet trabajen en adaptar las mejores tecnologías del mercado para brindar a sus clientes servicios de calidad.

La tecnología de Conmutación Multi-protocolo mediante Etiquetas (MPLS) permite transportar diferentes servicios en una misma red y a bajo costo; por lo que ha tenido gran aceptación en los ISP a nivel nacional. Con el crecimiento continuo de los clientes, las aplicaciones y sobre todo con la implementación de los Data Centers, Telconet S.A. necesita potencializar las aplicaciones que ofrece MPLS de tal manera que se optimicen sus recursos, se brinde QoS de extremo a extremo, flexibilidad y seguridad en la red.

Por otro lado, el agotamiento de las direcciones IPv4 es una realidad, así como que IPv6 desplazará progresivamente a IPv4. Los ISP deben tener una red lista para soportar los dos protocolos simultáneamente, e ir migrando conformen lo ameriten sus clientes. Un mecanismo de transición de IPv4/IPv6 sobre MPLS brinda grandes ventajas competitivas a un proveedor, pero su selección debe ser cuidadosa de tal manera que implique los cambios y costos adecuados.

Aventurarse en un nuevo protocolo, concierne dejar ventanas abiertas a las amenazas de la red. Es por ello, que se debe fortalecer la infraestructura con un análisis de su seguridad y aplicar las Mejores Prácticas de Seguridad para IPv6.

El presente proyecto se orienta a empresas proveedoras de servicios de telecomunicaciones, a mejorar su infraestructura de red utilizando no solo la tecnología MPLS sino sus aplicaciones, a tener soporte de IPv4 e IPv6 simultáneamente y brindar a sus clientes servicios de calidad al menor costo posible, logrando impulsar el desarrollo tecnológico de Ecuador.

CAPÍTULO 1

FUNDAMENTOS TEÓRICOS

1.1. TECNOLOGÍA *MULTIPROTOCOL LABEL SWITCHING* (MPLS)

1.1.1. INTRODUCCIÓN[1][2][3][21][22]

El auge de la Internet con el crecimiento exponencial de usuarios y el incremento de tráfico en la red han dado lugar a que los diferentes Proveedores de Servicios de Internet (ISP) realicen cambios tecnológicos importantes con el fin de ofrecer mayor velocidad y calidad en los servicios.

La Internet tradicional no podía transmitir diferentes tipos de aplicaciones con la calidad que requerían, mucho menos después que aparecieron aplicaciones en tiempo real, como: VoIP, Vídeo, Internet móvil, videoconferencias, vídeo-chat, entre otras. Manejar IP implica brindar un servicio del tipo *Best Effort*, haciendo que todas las aplicaciones tengan el mismo trato y aquellas que necesiten ser priorizadas no puedan ser transmitidas con calidad.

Entonces en 1997, el Grupo de Trabajo de la *Internet Engineering Task Force* (IETF) estudia la posibilidad de la creación de una nueva arquitectura. *Multiprotocol Label Switching* (MPLS) resultó del estudio profundo de las ventajas y desventajas de cada una de las tecnologías predecesoras y de los aportes de las empresas de networking, como la tecnología: *Tag Switching* de Cisco.

1.1.2. DEFINICIÓN Y CARACTERÍSTICAS DE MPLS[1][2][24]

MPLS es una arquitectura de transporte estandarizada por la IETF en el RFC 3031 en enero de 2001. Opera entre las capas: enlace de datos y red del modelo ISO/OSI; armonizando la velocidad de envío de capa 2 y la inteligencia de enrutamiento de capa 3.

MPLS utiliza etiquetas simples de tamaño fijo y pequeño para realizar la conmutación y brindar rapidez en el reenvío de paquetes. Es una tecnología multiprotocolo gracias a que mantiene independencia de los protocolos de capas vecinas y soporta tecnologías existentes, como: *Frame Relay*, ATM[1], y *Ethernet*, entre otras.

MPLS ofrece: un mecanismo para manejar tráfico de diferentes aplicaciones con los requerimientos originales de Calidad de Servicio (QoS) de extremo a extremo; seguridad al implementar Redes Privadas Virtuales (VPN); optimización del uso de los recursos de red con Ingeniería de Tráfico (TE); escalabilidad; alta velocidad de conmutación; flexibilidad; entre otras ventajas que superan las características de las tecnologías precedentes.

1.1.3. COMPONENTES DE MPLS

La tecnología MPLS presenta nuevos componentes que forman parte de su funcionamiento, como se indican en las secciones 1.1.3.1, 1.1.3.2, 1.1.3.3 y 1.1.3.4.

1.1.3.1. *Label Switched* Routers (LER)[2][3]

Los LSR**,** o también conocidos como *Provider* (P)*,* son equipos de conmutación de alta velocidad ubicados dentro de la red MPLS con el fin de enrutar los paquetes en base a la etiqueta ubicada en su cabecera. Todas las interfaces de este tipo de dispositivos tienen activado MPLS y nunca se conectan directamente a los equipos de los clientes.

Los LSR se encargan de realizar el intercambio de etiquetas (función denominada *swap*) y utilizan los protocolos de distribución de etiquetas para tener conocimiento de sus adyacencias correctamente distribuidas.

En la Figura 1.1 se muestran los LSR ubicados en el centro de la nube MPLS, los cuales se conectan en los extremos a equipos periféricos pero nunca

[1] Para mayor información sobre *Frame Relay* y ATM se recomienda consultar [2].

directamente a las interfaces de los clientes. Si un paquete llega al LSR, este intercambia la etiqueta de la cabecera MPLS por una o varias hasta llegar al equipo de borde respectivo, cumpliendo con el proceso de conmutación.

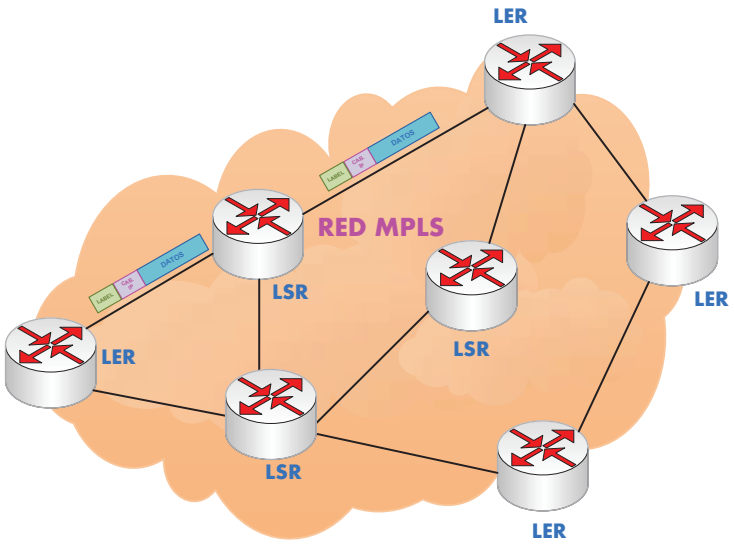


Figura 1.1 Enrutador LSR
Fuente: Autor

1.1.3.2. *Label Edge* Routers (LER)[2][3]

Los LER, también conocidos como: *Provider Edge* (PE) o LSR *Edge*, son equipos de borde o frontera llamados así porque se encuentran en la periferia de la red MPLS. Administran el tráfico entrante y saliente al mantener contacto con redes externas como: *Frame Relay,* ATM, *Ethernet* u otras.

A diferencia de los LSR, los LER son dispositivos que tienen interfaces configuradas con MPLS y con otras tecnologías. Los primeros permiten la comunicación con la red interna MPLS a través de los LSR; y los segundos se conectan con las redes externas que pertenecerán a los clientes.

Cuando ingresa tráfico a la red MPLS, los LER se encargan de agregar las etiquetas a cada paquete y reenrutalos al siguiente salto. De lo contrario, si el tráfico sale de la nube MPLS, retiran las etiquetas y enrutan cada paquete a las redes externas conectadas.

En la Figura 1.2 se indican los LER ubicados en la periferia de la nube MPLS, que serán los encargados de transportar el tráfico proveniente de la red IP de MIAMI hacia la red interna MPLS. Los LSR se mantienen en el centro de la nube MPLS y realizan el proceso de conmutación.

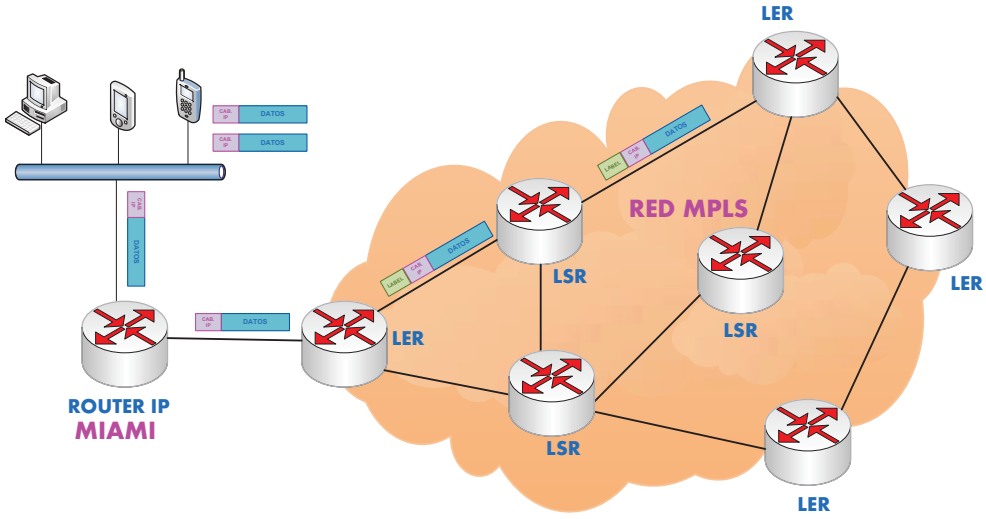


Figura 1.2 Enrutador LER

Fuente: Autor

1.1.3.3. *Forwarding Equivalence Class* (FEC)[2][3]

Las clases FEC son flujos de paquetes que tienen características comunes en trayectoria y tratamiento, como: la dirección de red origen o destino, el campo protocolo de la cabecera IPv4, el valor DSCP de IPv4 o la etiqueta de flujo de la cabecera IPv6.

Durante el ingreso de tráfico a la red MPLS, se realiza la asignación de un paquete a una clase FEC por primera y única vez mediante una etiqueta. Los paquetes de un mismo flujo serán agrupados a una clase FEC y tendrán la misma ruta aunque los destinos finales sean diferentes.

En la Figura 1.3 se puede apreciar un paquete que ingresa a la red MPLS y es asignado a una clase FEC por el equipo de borde. El paquete viajará con el

tratamiento detallado en esta clase hasta llegar a su destino y la red no podrá reasignarle a una clase diferente.

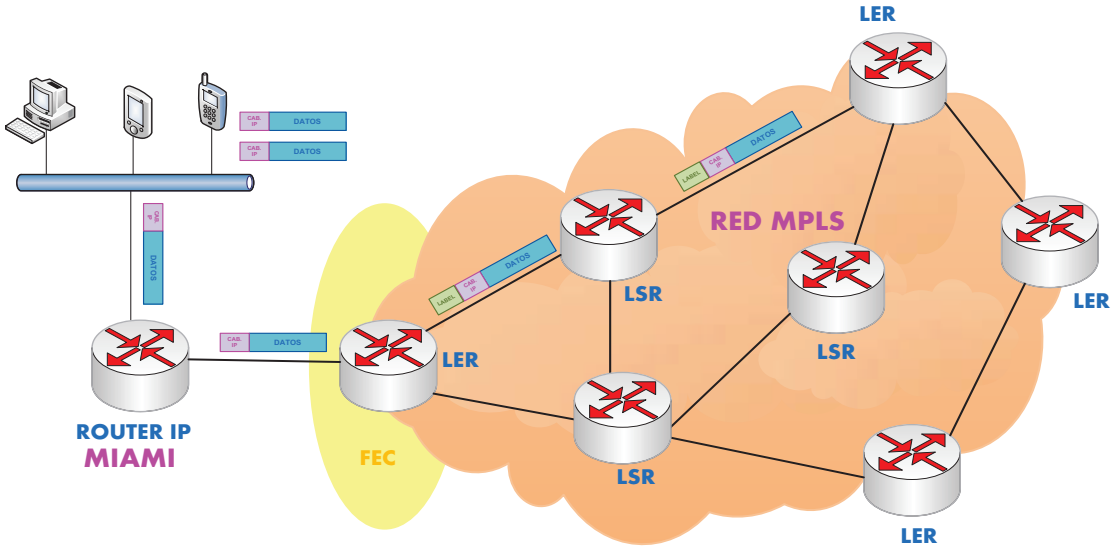


Figura 1.3 Asignación de un paquete a una clase FEC

Fuente: Autor

1.1.3.4. *Label Switched Path* (LSP)[2]

El LSP es el camino o trayecto unidireccional con QoS definido entre dos puntos de la red MPLS, y está formado por una sucesión de etiquetas que indican los saltos que realizarán los paquetes para llegar al destino. El trayecto de ida no necesariamente es el trayecto de regreso debido a que son caminos en una sola dirección.

En la Figura 1.4 se detalla el proceso de transporte de tráfico. Cuando un paquete ingresa a la red MPLS, el LER más cercano lo asigna a una clase FEC mediante una etiqueta, y lo encamina a un LSP a través de los LSR.

En cada salto, los LSR intercambian la etiqueta por otra u otras para enrutar el paquete al siguiente nodo. Este proceso siempre se realiza porque las etiquetas solo tienen significado local. Finalmente, se alcanza al LER que retira la etiqueta y entrega el paquete a una red externa.

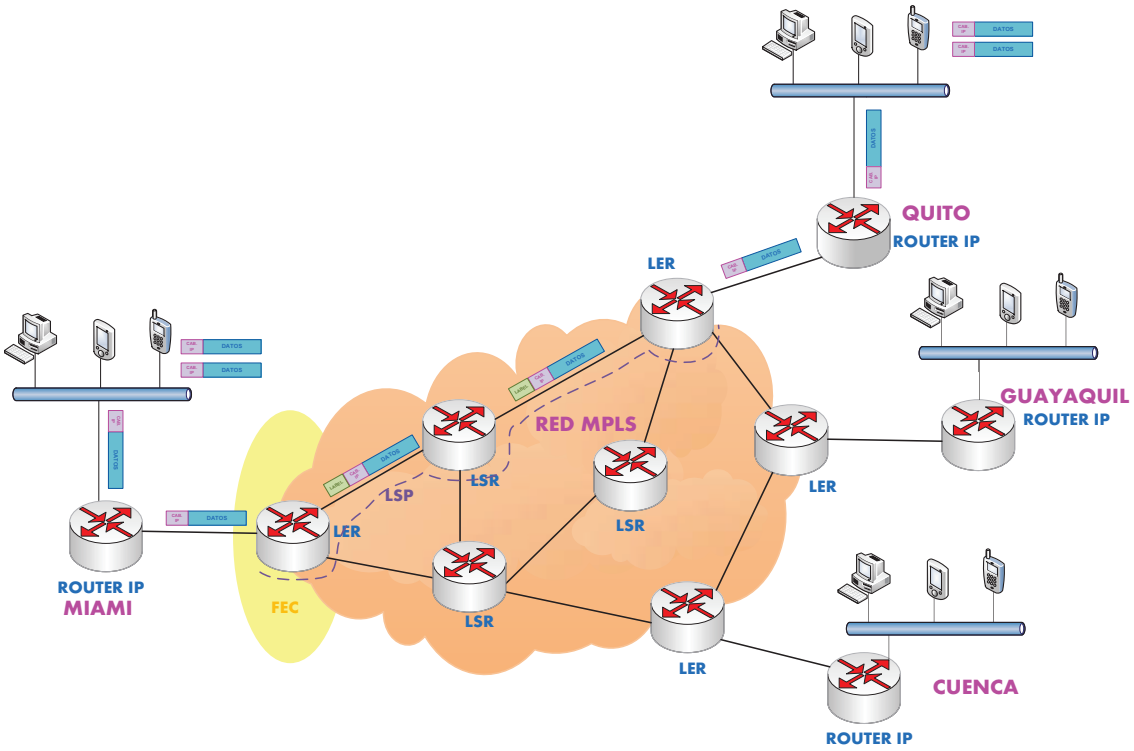


Figura 1.4 Camino de etiquetas conmutadas

Fuente: Autor

MPLS permite dos técninas para seleccionar un LSP:

- Enrutamiento *Hop-by-Hop*
- Enrutamiento Explícito

Enrutamiento *Hop-by-Hop*[2][21]

El enrutamiento *Hop-by-Hop* se caracteriza porque la selección del próximo salto de un paquete la realiza cada LSR de manera independiente. Es decir, los paquetes conocen solo su próximo salto y no toda la trayectoria que les espera recorrer.

Además, brinda alta velocidad de conmutación y tratamiento diferenciado a los paquetes de varias clases FEC, pero no tiene soporte para Ingeniería de Tráfico debido a que no permite reservar recursos. La ideología del enrutamiento *Hop-by-Hop* es similar al enrutamiento tradicional de IP, donde cada equipo toma decisiones independientemente de sus vecinos.

Enrutamiento Explícito (ER-LSP)[2][21]

En el enrutamiento ER-LSP, la lista de los saltos que se van a recorrer en el LSP está previamente determinada, y todos los paquetes que ingresan a la red MPLS tienen conocimiento absoluto de esta lista.

Este mecanismo brinda mayor flexibilidad que el enrutamiento *Hop-by-Hop* porque tiene soporte para Ingeniería de Tráfico, Calidad de Servicio de extremo a extremo y políticas de enrutamiento gracias a la reservación de recursos.

El LER tiene la responsabilidad de determinar la lista de los nodos que se van a recorrer, e informar la trayectoria al resto de paquetes que ingresan. Los LSR no pueden determinar su próximo salto porque se rigen a la lista especificada previamente.

1.1.4. ETIQUETA[2][3]

Una etiqueta MPLS es un conjunto de 32 bits (4 bytes) que se asocia a una clase FEC. Tiene significado local debido a que en cada salto a lo largo del LSP, se la analiza y se intercambia estrictamente por otra. Cuando un paquete alcanza el LER remoto, se retira la etiqueta ya que su uso será innecesario fuera de la red MPLS.

A diferencia de la cabecera IP que tienen direcciones IP origen y destino, la cabecera MPLS tiene un valor numérico acordado entre dos nodos para identificar el siguiente salto y brindar mayor velocidad. La etiqueta no pertenece a ninguna de las capas del modelo en particular, pero se ubica entre las capas 2 y 3 del modelo ISO/OSI.

1.1.5. FORMATO DE LA ETIQUETA[2][3]

La cabecera MPLS o etiqueta está constituida por cuatro campos que se muestran en la Figura 1.5.

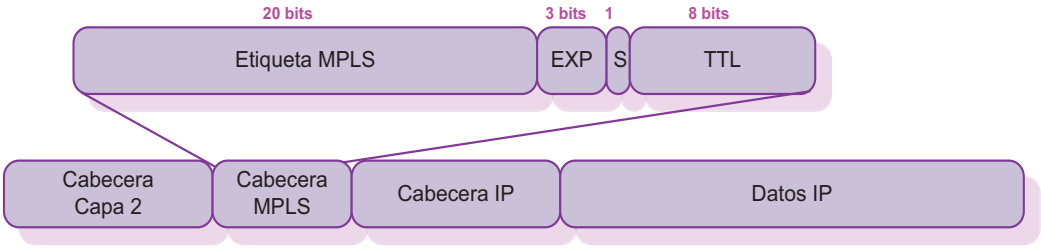


Figura 1.5 Cabecera MPLS

Fuente: [2]

1.1.5.1. Etiqueta MPLS[1]

El primer campo de la cabecera MPLS está formado por 20 bits que identifican la clase FEC asignada y determinan el siguiente salto en la red MPLS. Al tratarse de 20 bits se pueden tener 2^20 combinaciones[2], es decir, más de un millón de posibles etiquetas aunque las primeras 16 se encuentran reservadas.

A continuación se detallan las etiquetas reservadas:

- 0: Etiqueta explícita nula para IPv4
  Esta etiqueta es válida solo cuando se ubica como último ingreso de la pila de etiquetas (*label stack*); e indica que para el enrutamiento del paquete, se debe analizar la cabecera IPv4 ya que la pila de etiquetas será retirada.
- 1: Etiqueta de alerta de enrutamiento
  Esta es la etiqueta de alerta del enrutador indicando que el paquete necesita ser chequeado y corregido para ser reenviado. Puede ubicarse en cualquier lugar de la pila de etiquetas excepto en la parte inferior.
- 2: Etiqueta explícita nula para IPv6
  Tiene la misma funcionalidad de la etiqueta 0, solo que para el enrutamiento no se usa la cabecera IPv4 sino la de IPv6.
- 3: Etiqueta implícita nula
  Esta etiqueta puede ser analizada por cualquier nodo MPLS excepto aquellos que intervienen en el proceso de encapsulación. Tiene por objetivo indicar que la etiqueta fue retirada en el penúltimo salto antes de llegar a su destino, proceso que se conoce como *Penultimate Hop Popping* (PHP).

[2] *2^20= 1'048.576*

- 4-15
  Etiquetas reservadas para aplicaciones futuras.

1.1.5.2. Bits EXP[1][3]

El campo experimental o EXP está constituido por 3 bits que indican la Clase de Servicio (CoS) implementada, similar al campo prioridad del encabezado IP original. Si los 3 bits no son suficientes para detallar las diferentes CoS, se toman en calidad de préstamo 3 bits adicionales del campo etiqueta para este propósito. De esta manera, el límite de combinaciones posibles es de 64 gracias a los 3 bits del campo EXP y 3 bits adicionales del campo etiqueta.

1.1.5.3. Bit S[1][3]

Este campo está constituido por un solo bit e indica la existencia de una pila jerárquica de etiquetas en la cabecera MPLS. Las dos combinaciones posibles son:

- Bit S=0: Indica que la etiqueta no es la última de la pila sino que existen más elementos.
- Bit S=1: El valor de 1 refleja que la etiqueta es la última de la pila y le sigue un encabezado IP.

1.1.5.4. TTL[1][3]

El campo *Time To Live* (TTL) está formado por 8 bits y tiene la misma finalidad del campo TTL del encabezado IP. Es decir, se disminuye el valor TTL en una unidad en cada salto que da el paquete hasta llegar a su destino. Si el valor resultante es igual a cero, el paquete será descartado para evitar lazos en la red.

En la Figura 1.6 se detallan los cambios del campo TTL de un paquete durante su trayecto en la red MPLS. En un inicio, el LER de ingreso copia el campo TTL de la cabecera IP al campo TTL de la cabecera MPLS; y reenvía el paquete a su siguiente salto.

En cada salto, se resta una unidad al campo TTL de MPLS mientras el encabezado IP no se ve alterado. Si el resultado obtenido es equivalente a cero, se descarta el paquete sino se lo reenvía a su siguiente salto.

Finalmente, cuando se llega al LER remoto y este campo es diferente de cero, se copia el valor del campo TTL de MPLS al campo TTL de IP; y se retira la cabecera MPLS para que el paquete pueda salir de la red mientras es transportado por los campos de la cabecera IP.

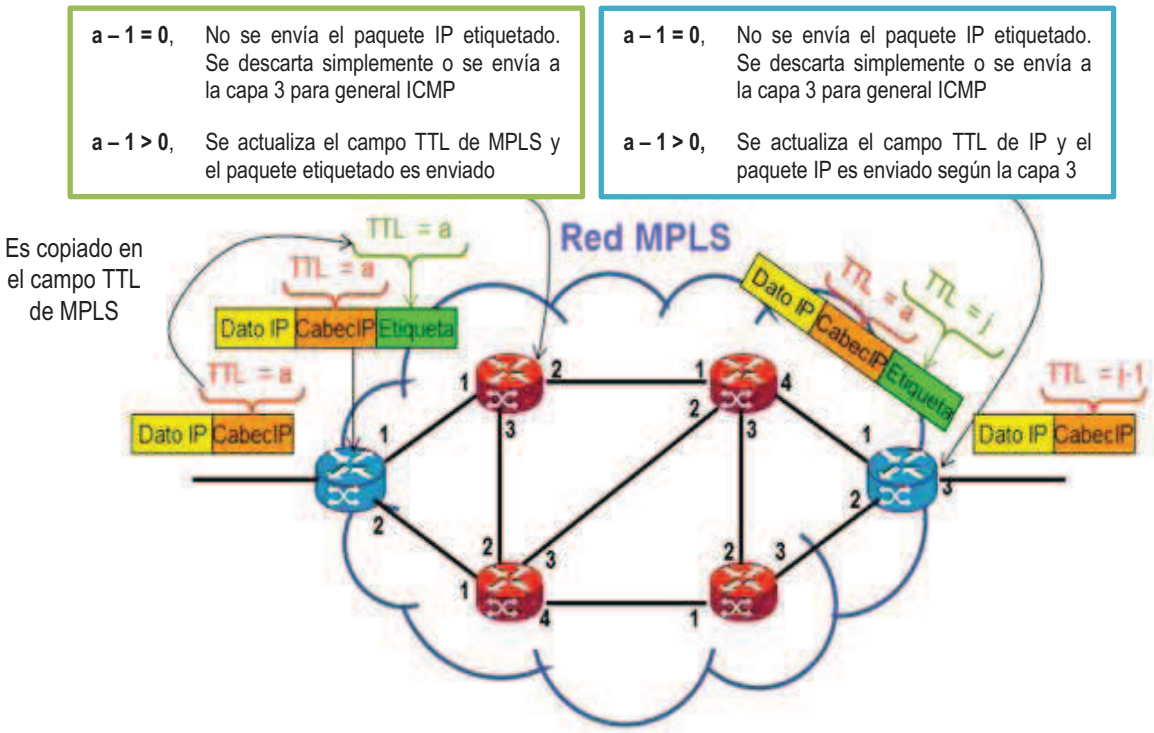


Figura 1.6 Campo TTL en la Red MPLS

Fuente: [3]

1.1.6. ARQUITECTURA DE LOS NODOS MPLS[2][3]

La arquitectura de MPLS presenta dos planos o componentes, y son:

- Plano de Control
- Plano de Datos

1.1.6.1. Plano de Control[2][3]

El Plano de Control es el responsable de: intercambiar información de enrutamiento de capa 3 e información de la distribución de etiquetas; la generación y mantenimiento de las tablas de enrutamiento y etiquetas; y el establecimiento de los LSP.

En el Plano de Control se presentan dos tablas como principales componentes y son:

- *Routing Information Base* (RIB)
- *Label Information Base* (LIB)

Routing Information Base (RIB)[2][3]

La tabla de enrutamiento RIB es generada por un protocolo denominado de *Gateway Interior* (IGP), utilizando los estados de enlace y las políticas de Ingeniería de Tráfico para determinar los próximos saltos de cada red.

Los protocolos IGP soportados son: *Open Shortest Path First* (OSPF), *Border Gateway Protocol* (BGP), *Intermediate System - Intermediate System* (IS-IS) y *Enhanced Interior Gateway Routing Protocol* (EIGRP).

Label Information Base (LIB)[2][3]

La Tabla base de información de etiquetas contiene todas las etiquetas asignadas por un LSR, tanto aquellas que están siendo utilizadas en ese momento y aquellas que no lo están. Esta Tabla se genera gracias al protocolo de distribución de etiquetas configurado e indica la asociación de las etiquetas locales con las recibidas desde sus vecinos.

Los protocolos LDP soportados son: *Label Information Base* (LDP), *Resource Reservation Protocol-Traffic Engineering* (RSVP-TE), *Constrained Based-Routing Label Distribution Protocol* (CR-LDP) y *Border Gateway Protocol* (BGP).

1.1.6.2. Plano de Datos[2][3]

El Plano de Datos se encarga de la conmutación de paquetes en base a la información provista por las etiquetas. Tiene dos componentes importantes y son:

- *Forwarding Information Base* (FIB)
- *Label Forwarding Information Base* (LFIB)

Forwarding Information Base (FIB)[2][3]

Esta Tabla fue creada con el fin de optimizar la búsqueda de una ruta de destino y mejorar el rendimiento de la red. A través de un protocolo de capa 3, se incrementa la velocidad de conmutación del paquete al reducir el tamaño de los encabezados y con ello, los retardos de transmisión. Por ejemplo, en los equipos Cisco se genera la Tabla FIB gracias al protocolo *Cisco Express Forwarding* (CEF)[3].

Label Forwarding Information Base (LFIB)[2][3]

La Tabla LFIB está formada por las etiquetas de entrada y salida que están siendo utilizadas en ese momento, e información adicional, como: la clase FEC, las interfaces de entrada y salida y la dirección IP del siguiente salto.

Esta Tabla se mantiene actualizada gracias a los protocolos de intercambio de etiquetas suministrados por el Plano de Control. Es la última Tabla generada y la más importante a la hora del reenvío de paquetes, debido a que cuenta con toda la información necesaria para la conmutación.

1.1.6.3. Funcionalidades de los routers LSR y LER[3]

Los routers LSR y LER realizan diferentes funciones durante la transmisión de un paquete. Se diferencian en el acceso al Plano de Datos, mientras el acceso al Plano de Control permanece independiente del tipo de router.

---

[3] Para mayor información sobre CEF se recomienda revisar [40].

Las funciones que manejan los routers en una red MPLS son tres: *Push, Swap* y *Pop.*

- Función *Push*

  La función *Push* se encarga de "insertar" una o varias etiquetas en la cabecera del paquete para poder reenviarlo. La realizan los routers LER en el ingreso a la red MPLS, aunque si se tiene una pila de etiquetas la pueden realizar los routers LSR.
- Función *Swap*

  Esta función se encarga de "intercambiar" una etiqueta por otra y la realizan únicamente los routers LSR durante la conmutación de paquetes. Si se trata de una pila de etiquetas, el intercambio puede abarcar no solo una sino varias etiquetas.
- Función *Pop*

  Cuando un paquete sale de la red MPLS, los routers LER se encargan de realizar la función *Pop* para "retirar" la etiqueta insertada. Si se trabaja con una pila de etiquetas, los LSR también pueden ejecutar esta función y retirar las etiquetas.

Los LER realizan exclusivamente las funciones: *Push* durante el ingreso de un paquete a la red MPLS, y *Pop* durante la salida del mismo. Mientras, los LSR se centran en la función *Swap* aunque pueden ejecutar las funciones *Push* y *Pop* cuando existe una pila de etiquetas.

En la Figura 1.7 se indica la arquitectura MPLS de los nodos LER. El Plano de Datos trabaja con las tablas FIB y LFIB para poder enrutar los paquetes desde y/o hacia la red MPLS. Por el contrario, el Plano de Control provee información para la generación y actualización del Plano de Datos a través de las tablas RIB y LIB.

En este tipo de routers, el Plano de Datos está preparado para enrutar paquetes IP y MPLS, gracias a que el Plano de Control intercambia información de enrutamiento y etiquetas utilizando los protocolos IGP y LDP.

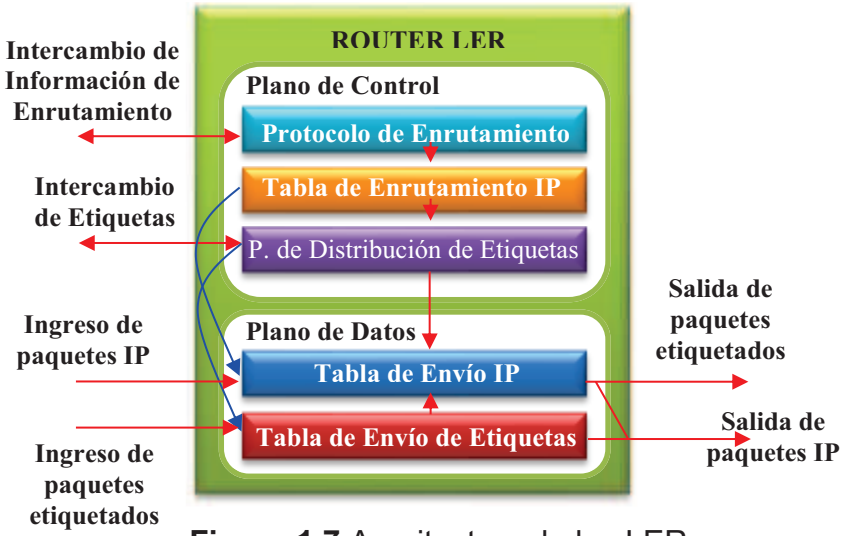


Figura 1.7 Arquitectura de los LER

Fuente: [3]

Los routers LSR son los responsables de la conmutación de paquetes y acceden a la Tabla LFIB para obtener información del siguiente salto, como: las etiquetas de entrada y salida, direcciones IP e interfaces. En la Figura 1.8 se muestran los Planos de Control y Datos de los routers LSR.

A diferencia de los LER, los LSR en el Plano de Datos solo trabajan con la Tabla LFIB debido a que se ubican en el núcleo de la red MPLS y no tienen contacto con otra tecnología que no sea MPLS. Se genera y se actualiza la Tabla LFIB usando la información proveniente del Plano de Control mediante la Tabla LIB.

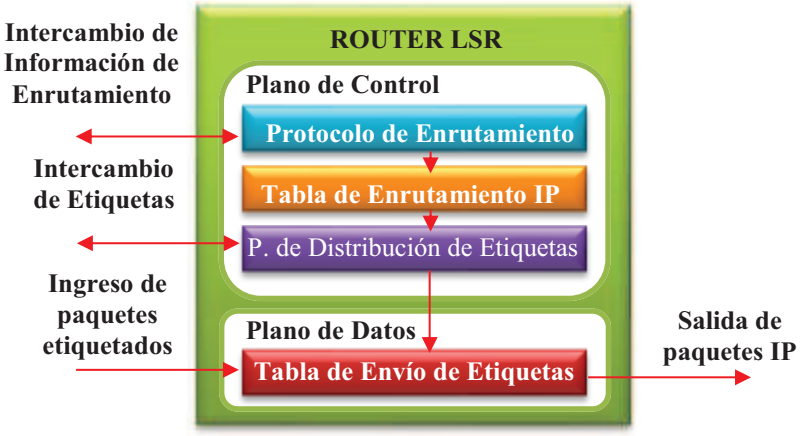


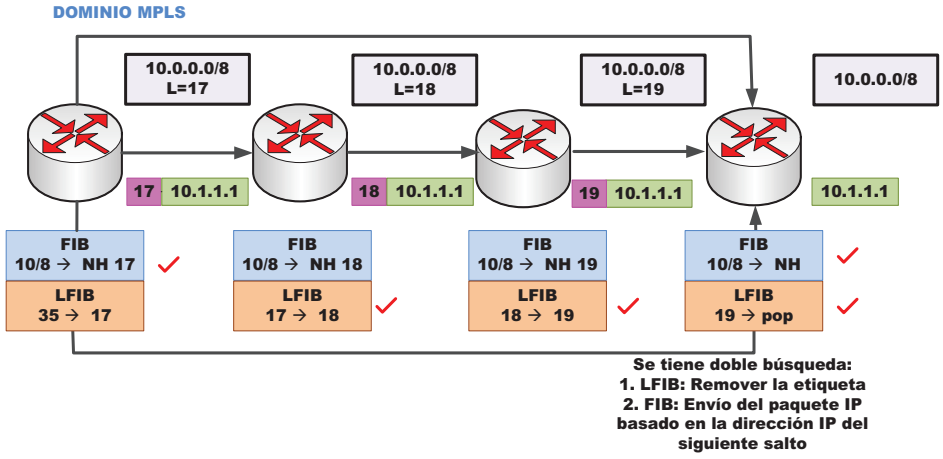
Figura 1.8 Arquitectura de los LSR

Fuente: [3]

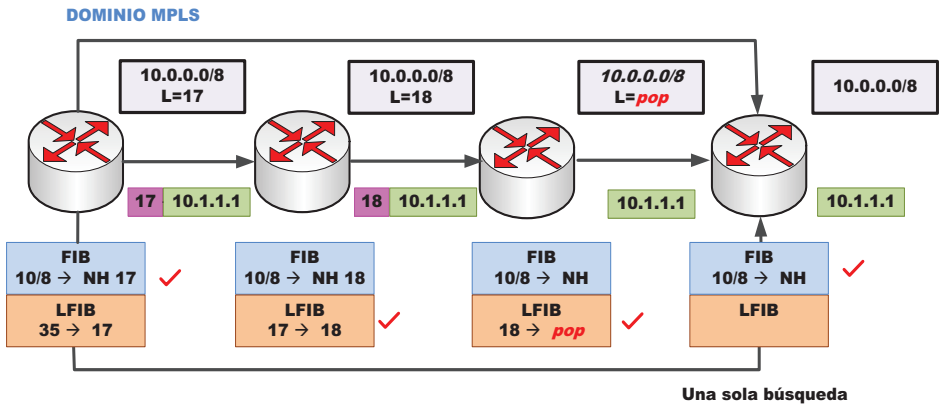
1.1.7. EXTRACCIÓN DE ETIQUETAS EN EL PENÚLTIMO SALTO (PHP)[2][3]

PHP es un mecanismo de optimización de la red MPLS que evita realizar una búsqueda innecesaria en la Tabla LFIB de un LER remoto. Consiste en remover la etiqueta de un paquete en el penúltimo nodo LSR antes de salir de la red MPLS; logrando que el LER lo conmute buscando solo la dirección IP del siguiente salto en la Tabla FIB.

En la Figura 1.9 se muestra el proceso de intercambio de etiquetas de un paquete que viaja hacia la red 10.0.0.0/8. Este paquete utiliza las etiquetas 35, 17 y 18 para llegar al penúltimo salto antes de salir de la red MPLS.



(a) sin PHP



(b) con PHP

Figura 1.9 Red MPLS **(a)** sin PHP **(b)** con PHP

Fuente: [3]

En la parte (a), el LSR intercambia la etiqueta 18 por la 19 proveniente de la Tabla LFIB, y lo conmuta al siguiente salto. Cuando se llega al LER, se realiza nuevamente la búsqueda en la Tabla LFIB; y se determina retirar la etiqueta 19 para que el paquete salga de la red MPLS. Ahora, se enruta utilizando la dirección ubicada en la cabecera IP.

En la parte (b) de la Figura 1.8, el paquete llega al penúltimo salto y el LSR determina retirar la etiqueta. Cuando se alcanza el último salto, el LER enrutará el paquete con la dirección IP; y se evitará el buscar la etiqueta en la Tabla LFIB debido a que esta ya fue retirada en el penúltimo salto, mejorando así el desempeño de la red.

1.1.8. PROTOCOLO DE DISTRIBUCIÓN DE ETIQUETAS (LDP)[2][3]

El protocolo LDP es el responsable de "distribuir" la información para la generación de los LSP. Cuando un LSR asigna una etiqueta a una clase FEC, es importante que sus vecinos tengan conocimiento de esta asociación; y lo obtienen gracias al protocolo LDP. Un paquete podrá llegar a su destino solo si se tienen las tablas actualizadas en cada nodo.

LDP es un protocolo bidireccional, es decir que durante una sesión LDP, un LSR puede aprender simultáneamente información de las etiquetas de sus "pares LDP"[4] adyacentes o no. Utiliza el puerto TCP 646.

Tag Distribution Protocol (TDP)[5] es un protocolo similar a LDP pero propietario de Cisco que utiliza el puerto TCP 711. Nace con la tecnología *Tag Switching* de Cisco y aporta con los principios básicos para la creación de LDP. A diferencia de LDP, TDP no está estandarizado por la IETF por lo que no ha sido ampliamente difundido en las redes.

[4] Los "pares LDP" ("LDP *peers*" en inglés) son LSR que trabajan conjuntamente con el protocolo LDP.
[5] Para mayor información de TDP se recomienda revisar [41].

1.1.9. APLICACIONES DE MPLS[2][3]

MPLS presentó una gran ventaja frente a sus tecnologías predecesoras, gracias al soporte de una serie de nuevas aplicaciones, como: *Unicast* IP *Routing*, *Multicast* IP *Routing*, Redes Virtuales Privadas, Calidad de Servicio e Ingeniería de Tráfico,

En MPLS, todas las aplicaciones manejan la conmutación de etiquetas en su Plano de Datos; logrando que el concepto de convergencia sea una realidad al tener una misma red con todos los servicios de telecomunicaciones. Entre las aplicaciones más sobresalientes se tienen tres, y son:

- Redes Privadas Virtuales
- Calidad de Servicio
- Ingeniería de Tráfico

1.1.9.1. Redes Privadas Virtuales (VPN)[1][3][17]

Una VPN tiene por objetivo extender una red privada sobre una red de uso público como Internet; con funciones y características de seguridad similares a una red privada. Puede enviar cualquier tipo de tráfico de manera eficiente, segura y transparente al usuario a través de túneles privados configurados sobre una red pública. La información estará completamente protegida porque la transmisión será imperceptible para el resto de usuarios de la red.

Las VPN de MPLS son las implementaciones más populares de la tecnología MPLS, gracias a la escalabilidad y facilidad de administración que ofrecen. Permiten dividir la red del proveedor en pequeñas redes con tablas de enrutamiento separadas. A diferencia de las VPN tradicionales, las VPN de MPLS garantizan que la información pueda ser transmitida con QoS de extremo a extremo, y pueden aprovechar la Ingeniería de Tráfico para mejorar el desempeño global de la red.

Las VPN de MPLS se configuran solo en los routers LER para reenviar la información a través de túneles privados. Los LSR no tienen conocimiento de la existencia de las VPN y mucho menos de sus tablas de enrutamiento.

Beneficios de las VPN de MPLS

Los principales beneficios que ofrecen las VPN de MPLS son:

- La facilidad que ofrecen en la configuración ya que no requieren cambios en la *intranet* del cliente.
- Permiten utilizar los mismos rangos de direcciones privadas para comunicarse a través de la red pública.
- Pueden transportar cualquier tipo de tráfico como: voz, datos y vídeo.
- Brindan privacidad y seguridad al publicar las rutas solo a los routers miembros de la VPN.
- Son escalables, ya que soportan varios sitios por VPN y varias VPN por Clase de Servicio para garantizar la Calidad de Servicio de extremo a extremo.
- Menores costos frente a las líneas dedicadas.

Existen dos tipos de VPN de MPLS y se diferencian por la capa del modelo OSI en la que se implementan como son: VPN de capa 2 y VPN de capa 3.

VPN de MPLS de capa 2

Las VPN de capa 2 son soluciones de transporte que mantienen separada la red del cliente de la del proveedor. No existe enrutamiento entre el *Customer Edge* (CE) y los equipos de la nube MPLS ya que el proveedor solo se encarga del transporte de la información. El enrutamiento es responsabilidad exclusiva del cliente y no tiene relación con la red del proveedor.

Para mantener compatibilidad con las tecnologías de capa 2, como: *Frame Relay,* ATM y *Ethernet,* se maneja el concepto de *pseudowires.* Un *pseudowire* es un enlace lógico unidireccional entre dos PE de la red MPLS de un proveedor que

comunica dos puntos finales de un cliente. Cuando las tramas de la tecnología ingresan al PE, son encapsuladas en MPLS y enviadas por un *pseudowire* establecido a través de un LSP.

Existen dos mecanismos de conexión: *Virtual Private Wire Service* (VPWS) y *Virtual Private LAN Service* (VPLS).

- *Virtual Private Wire Service* (VPWS)

  Las VPWS son conexiones punto a punto de capa 2 entre dos sucursales distantes de un cliente a través de la red MPLS de un proveedor. La tecnología de capa 2 configurada en los extremos de la red comúnmente es la misma, por ejemplo *Ethernet; a*unque puede ser diferente, como *Ethernet - ATM*, donde se requerirá un mecanismo de traducción entre las tecnologías.

  En una comunicación dúplex se necesitan establecer dos *pseudowires* mediante LDP, uno en cada sentido. Cuando una trama ingresa al LER de la red MPLS, se añade una pila de etiquetas que identifica a la VPWS. La pila vendrá marcada por: una etiqueta referente al *pseudowire* ubicada en la base y otra que identifique al LSP. Durante la conmutación, los LSR solo analizan la etiqueta del LSP, mientras que los LER examinan las dos etiquetas de la pila y reconstruyen la trama para enviarla al cliente.

  Cuando las redes de los clientes trabajan en capa 2 con la tecnología *Ethernet,* la solución de VPWS se conoce como: *Virtual Leased Line* (VLL).

- *Virtual Private LAN Service* (VPLS)[6]

  Las VPLS son soluciones punto multipunto de capa 2 que conectan diferentes sucursales de un cliente. Utilizan la dirección MAC y establecen los *pseudowires* en una topología *full mesh* para el reenvío de las tramas entre los PE.

[6] Las VPLS se encuentran fuera del alcance de este proyecto porque son conexiones punto multipunto que requieren un mayor número de recursos que los disponibles en el prototipo para comprobar su funcionamiento. Para mayor información de las VPLS se recomienda revisar [47].

Para diferenciar las VPLS en un PE se establecen las *Virtual Switch Instances* (VSI) que son tablas de direccionamiento físico con información de los equipos pertenecientes al dominio VPLS. La conmutación de tramas en la nube se establece mediante etiquetas; pero en los LER, el reenvío es similar a la conmutación *Ethernet* de los switches a través de direcciones MAC.

VPN de MPLS de capa 3 (BGP MPLS/VPN)[18]

Las VPN de capa 3 son las aplicaciones más utilizadas en la tecnología MPLS debido a que permiten manejar múltiples tablas de enrutamiento independientes de la tabla de enrutamiento general en un mismo router. Los ISP obtienen grandes ventajas con las VPN de capa 3, al poder segmentar las redes de los clientes sin implementar muchos equipos. La seguridad se incrementa significativamente gracias a que la información de una VPN no se mezcla con la información de otra.

Cuando un paquete ingresa a la red MPLS, el LER inserta una pila de dos etiquetas: la primera, ubicada en la base, hace referencia al router destino y la interfaz de salida hacia el CE; mientras la segunda, identifica el siguiente salto y es producto del protocolo LDP.

Una VPN de capa 3 asocia tres nuevos conceptos que son: *Virtual Routing Forwarding* (VRF), *Route Distinguisher* (RD) y *Route Target* (RT).

- *Virtual Routing Forwarding* (VRF)[18]

  Una VRF es la instancia de enrutamiento y envío de paquetes de una VPN de capa 3. Su nombre se atribuye a la Tabla FIB del Plano de Datos; es decir, a la combinación de: la tabla de enrutamiento de la VPN, la Tabla CEF de la VPN y los protocolos de enrutamiento asociados.

  Las VRF solo se configuran en los LER ya que son los únicos equipos que tienen conocimiento de ellas. Un router tiene soporte para varias VRF y cada una actúa como un router lógico independiente. La interfaz de un LER puede

ser asignada a una y solo una VRF, mientras que una VRF puede estar configurada en varias interfaces físicas, lógicas y/o subinterfaces.

En la Figura 1.10 se indican tres VRF: azul, naranja y verde en un mismo router, donde cada una maneja su tabla de enrutamiento independiente. Es decir, las direcciones de la VRF azul no presentan conflicto si se las utiliza en el direccionamiento de la VRF naranja y/o verde, ya que la información de la VRF azul será inaccesible desde las VRF naranja y verde.

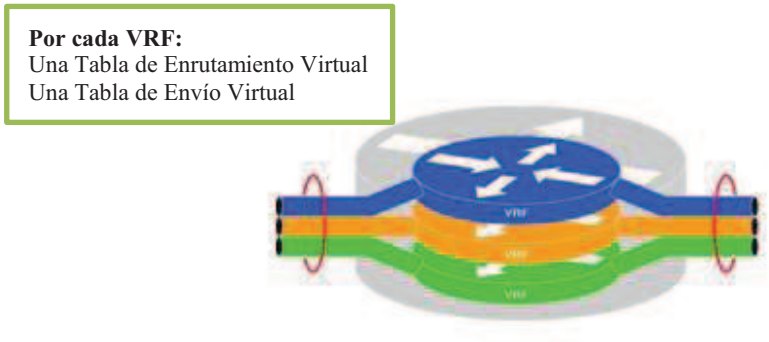


Figura 1.10 Definición de las VRF en un router
Fuente: [46]

- *Route Distinguisher* (RD)[3]
  El RD es un campo formado por 64 bits que identifica las rutas de una VRF. Se agregan a las direcciones IPv4 o IPv6 con el fin de hacerlas únicas en la red MPLS, logrando que una misma dirección IP puede estar configurada en más de dos VRF y no cree conflictos.

- *Route Target* (RT)[3]
  Como los clientes pueden participar en más de una VPN de capa 3, la distribución de la información de enrutamiento de las VPN se controla con la creación de las comunidades de destino de ruta (RT), implementadas por el protocolo BGP. Es decir, en una misma VRF se definen qué sucursales del cliente pueden o no importar y/o exportar información de enrutamiento.

  Un RT está formado por 64 bits. Existen dos tipos y son: el *import* RT que permite seleccionar la ruta que va a ingresar a la tabla de enrutamiento de la

VRF, y el *export* RT que identifica los miembros de la VRF a los cuales se les puede anexar la ruta.

1.1.9.2. Calidad de Servicio (QoS)[3][12][15][20]

QoS es un mecanismo que permite priorizar diferentes aplicaciones que circulan por la red, garantizando uno o más de los cuatro parámetros que la definen, como son: el ancho de banda, el retardo, el *jitter* y la pérdida de paquetes. CoS permiten diferenciar el tráfico que circula por la red en: crítico, como la voz y el vídeo; y no tan crítico, como el correo electrónico y la transferencia de archivos.

Los ISP establecen convenios con sus clientes con el objetivo de definir el nivel de QoS contratado mediante los Acuerdos de Nivel de Servicios (SLA); donde se detallan aspectos como: el tiempo de respuesta, el personal asignado, el soporte, la disponibilidad comprometida, los créditos, las condiciones de incumplimiento, entre otros.

MPLS permite transportar diferentes CoS gracias a que las etiquetas llevan en los bits EXP un identificativo del tipo de servicio utilizado en el LSP. Por ejemplo, para el caso que se esté transmitiendo datos en MPLS y se requiera realizar una videoconferencia simultáneamente, el LSP del vídeo dispondrá de mayor ancho de banda y la ruta menos congestionada posible, con el fin de disminuir la latencia y brindar un servicio de buena calidad.

Parámetros de Calidad de Servicio[3][12][15]

Los parámetros que definen un servicio de calidad son cuatro: el ancho de banda, el retardo, el *jitter* y la pérdida de paquetes.

- Ancho de Banda[20]

  Es la cantidad máxima de transferencia de información entre dos puntos extremos de una red en un periodo determinado. Se expresa en bits por segundo (bps).

- Retardo o latencia

  Es el tiempo que tarda un paquete en ir desde la fuente al destino. El retardo de extremo a extremo es la suma de todos los tiempos de: propagación, transmisión y encolamiento. Se expresa en segundos (s).
- Variación del retardo o *jitter*

  Es la variación que se produce en el retardo promedio de ida y vuelta. Durante la transmisión de paquetes, el incremento en el *jitter* provocará que el receptor obtenga una señal distorsionada la cual no es favorable. Se expresa en segundos (s).
- Pérdida de paquetes o fiabilidad

  La fiabilidad corresponde a la cantidad de paquetes esperados en el receptor menos la cantidad de paquetes recibidos (incluyendo los duplicados). Existen medios no fiables como el aire en las redes inalámbricas, donde la fiabilidad es baja.

Arquitectura de Servicios Diferenciados (DiffServ)[15]

DiffServ nace como una mejora a su predecesor la arquitectura Servicios Integrados (IntServ). IntServ pretendía brindar una sola red IP capaz de soportar tráfico del tipo *Best Effort* y reservar recursos para las aplicaciones en tiempo real; pero presentó problemas de escalabilidad resultando no viable en grandes redes.

DiffServ nace como la oportunidad de brindar QoS en las redes IP. Consiste en brindar tratamiento diferenciado a los flujos asignados de una clase. Los routers ubicados en la periferia de la red identifican la clase, y marcan los paquetes que pertenecen a un determinado flujo; mientras los routers internos, los retransmiten según el tratamiento brindado a la clase.

Campo DiffServ[15][20]

DiffServ es un mecanismo estable debido a que se define QoS en uno de los campos de la cabecera IP y no en cada router de la trayectoria del paquete. En la cabecera IPv4, los bits del campo Tipo de Servicio son los que indican la CoS

implementada, mientras que en IPv6 se consideran los bits del campo Clase de Tráfico.

Estos campos tanto en IPv4 como IPv6 están formados por 8 bits. Los 6 primeros indican el tratamiento que recibirá el paquete en la red y se conocen como: *Differentiated Service Code Point* (DSCP). Los dos restantes sirven para el control de congestión y se denominan *Currently Unused* (CU).

En la Figura 1.11 se muestra la distribución de los 8 bits del campo DiffServ. Los bits 7, 6 y 5 representan CoS; los bits 4 y 3 indican la probabilidad de descarte; el bit 2 define la categoría; y los bits 0 y 1 no se utilizan en la actualidad.

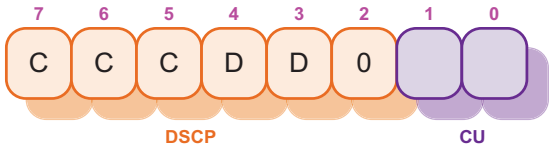


Figura 1.11 Campo DiffServ (DS)
Fuente: [15]

Con 6 bits DSCP se tienen 64 posibles combinaciones, las cuales se dividen en tres categorías, y son:

- Categoría estándar:
  Esta categoría es la más usada y permite definir la CoS implementada para el paquete. La conforman 32 combinaciones; y se diferencian porque el bit 2 está marcado en “0”.
- Categoría experimental:
  Esta categoría es de uso experimental o local. Implica 16 combinaciones que se diferencian porque los bits 3 y 2 son “11”.
- Categoría reservada:
  Esta categoría está reservada para futuras aplicaciones. La conforman 16 combinaciones con sus bits 3 y 2 en “01”.

Per-Hop Behavior (PHB)[15][20]

En DiffServ, un PHB es el mecanismo de envío y encolamiento que recibirá un paquete durante su retransmisión en la red y estará definido en los 6 bits del campo DSCP de la categoría estándar. Todos los paquetes que tengan el mismo PHB, recibirán el mismo tratamiento de retransmisión en la red.

Se presentan cuatro tipos de PHB estándar y son:

- *Default* PHB

  Se define un servicio del tipo *Best Effort* tradicional, detallado por defecto cuando un paquete ingresa a un nodo y no se le asigna otro PHB. Su valor en los 6 bits DSCP es 000000.

- *Class Selector* PHB

  Se definen siete comportamientos que van desde el 001000 hasta el 111000; donde los bits de probabilidad de descarte se mantienen en "00". Cada comportamiento ofrece mayor probabilidad de envío que su anterior; es decir que un paquete con DSCP 111000 se transmitirá con mejores características que uno con DSCP 001000.

- *Assured Forwarding* PHB (AF)

  Se identifican cuatro clases de tráfico marcadas en los bits 7, 6 y 5 del campo DSCP (bits CCC); cada una con tres probabilidades de descarte (bits DD): baja (01), media (10) y alta (11); generando un total de 12 combinaciones que van desde el DSCP 001010 (AF11) hasta el 100110 (AF43). Mientras mayor sea el valor de CoS (bits CCC), mejor será el tratamiento de retransmisión recibido por el paquete.

  En la Tabla 1.1 se detallan las 12 posibles combinaciones AF y el orden en que serían descartados en caso de congestión. Por ejemplo, AF33 recibirá mejores características de transmisión que AF22; pero no mejores que AF31 porque recibirá alta probabilidad de descarte.

COS (bits CCC)	PBBD DE DESCARTE (bits DD)		VALOR DSCP		
			BINARIO	DECIMAL	DSCP
001	alta	11	001110	14	AF13
	media	10	001100	12	AF12
	baja	01	001010	10	AF11
010	alta	11	010110	22	AF23
	media	10	010100	20	AF22
	baja	01	010010	18	AF21
011	alta	11	011110	30	AF33
	media	10	011100	28	AF32
	baja	01	011010	26	AF31
100	alta	11	100110	38	AF43
	media	10	100100	36	AF42
	baja	01	100010	34	AF41

Tabla 1.1 *Assured Forwarding* PHB

Fuente: [15]

- *Expedited Forwarding* PHB (EF)

  EF es el mejor comportamiento que puede recibir un paquete. Su valor DSCP es 101110 y brinda: mayor ancho de banda, alta fiabilidad y mínimo retardo y *jitter*. A esta clase pertenece el servicio de voz.

Mecanismos de Control de Envío[15][20]

Estos mecanismos permiten controlar la tasa de envío de paquetes en un dispositivo de red. Si un flujo de paquetes ingresa por la interfaz, primero se debe aplicar una política de clasificación de tráfico para ejecutar los mecanismos de control de envío.

Existen dos mecanismos y son: *traffic policing* y *traffic shaping.*

- *Traffic policing*

  Este mecanismo se utiliza para controlar la velocidad máxima de envío o recepción de tráfico en una interfaz. Se configura generalmente en las interfaces de borde de la red, con el fin de limitar el tráfico que entra o sale.

Es un excelente mecanismo para controlar el tráfico contratado por los clientes.

Define tres conceptos importantes: c*ommitted information rate* (CIR) como la velocidad media comprometida; c*ommitted burst* (Bc) como la cantidad de información comprometida a enviar en un intervalo de tiempo (Tc); y *excess burst* (Be) como la cantidad de información en exceso. *Traffic policing* descarta los paquetes solo si se supera la tasa CIR.

- *Traffic shaping*

  Este mecanismo permite controlar el tráfico de salida de una interfaz con el objetivo de trabajar a la misma velocidad que la interfaz remota. Garantiza los requerimientos de los clientes, al eliminar los cuellos de botella donde la red se ve afectada. El tráfico se ajusta a las políticas establecidas al limitar el ancho de banda disponible para cada clase de tráfico. En caso de congestión, *traffic shaping* encola los paquetes y los descarta solo cuando la cola supera el umbral máximo.

Mecanismos de Encolamiento[15][20]

Cuando a un router le llegan más paquetes de los que puede procesar y reenviar al medio, se produce la congestión debido a que existen paquetes que no están siendo procesados. Los mecanismos de encolamiento permiten controlar la congestión, a través de la asignación de un orden de salida en la cola de paquetes de la interfaz.

Existen algunos mecanismos de encolamiento, de los cuales los más conocidos son:

- *First-In, First-Out* (FIFO)

  Es el más simple de todos los mecanismos de encolamiento. Consiste en que el primer paquete que entra a la interfaz del router, es el primer paquete que sale de ella. Está limitado por el *buffer* debido a que empieza a descartar los

paquetes una vez alcanzado su límite. No se recomienda en la implementación de QoS porque no asigna probabilidades a CoS.

- *Priority Queuing* (PQ):

  PQ asegura dar prioridad y garantías totales al tráfico importante aunque puede dejar sin servicio al tráfico menos prioritario. Cada paquete deber ser colocado en una de las cuatro colas de: alta, media, normal o baja prioridad. La desventaja es que es un método estático porque no se adapta a los requerimientos de la red.

- *Weighted Round Robin* (WRR)

  Es un mecanismo que permite priorizar las diferentes colas que dispone a través de la asignación de un peso. Por ejemplo, como en la Figura 1.12 se envían cuatro paquetes de la cola 3 (peso 4), dos paquetes de la cola 2 (peso 2) y uno de la cola 1 (peso 1), así hasta terminar con la transmisión de todos los paquetes.

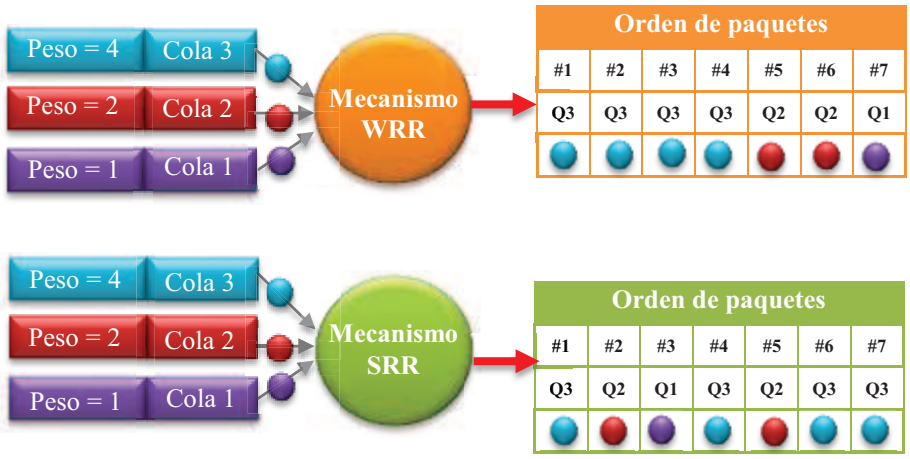


Figura 1.12 Diferencias entre SRR y WRR

Fuente: [53]

- *Shared/Shaped Round Robin* (SRR)

  Es un mecanismo similar a WRR porque asigna prioridades a las clases mediante la asignación de peso, pero con la diferencia en el orden del envío de los paquetes. Por ejemplo, en la Figura 1.12 se muestran tres colas con

sus pesos respectivos, entonces se enviará un paquete de cada cola en la primera vuelta, dos paquetes de la cola 3 y 2 en la segunda, y finalmente, los dos restantes de la cola 3, logrando controlar de mejor manera la tasa de envío de los paquetes.

- *Weighted Fair Queuing* (WFQ)
  WFQ es un mecanismo que fácilmente se adapta a la red porque, por un lado organiza el tráfico prioritario y lo ubica al inicio de la cola; y por otro, comparte el ancho de banda restante entre los flujos menos prioritarios. No es escalable porque analiza cada flujo a través de un algoritmo; pero garantiza que el tráfico menos prioritario no se quede sin servicio por falta de ancho de banda.

- *Class-Based Weighted Fair Queuing* (CBWFQ)
  CBWFQ nace como una solución al problema de escalabilidad de WFQ. Es un mecanismo que se basa en clases para tener mayor control de las colas y mejor asignación del ancho de banda. Las clases serán creadas por el usuario y cada una, estará asociada a una cola con tratamiento diferente. Si a una clase le sobra ancho de banda, las clases restantes podrán utilizarlo optimizando el uso de la red.

- *Low Latency Queuing* (LLQ)
  LLQ acoge las mejores características de PQ y CBWFQ. Está constituido por una cola de alta prioridad y varias colas de prioridad personalizada. La cola de alta prioridad tiene preferencia ante el resto; pero debe ser configurada con un límite de ancho de banda para evitar que el resto de colas se queden sin servicio por falta de ancho de banda. LLQ es el mecanismo adecuado para implementar una red convergente.

Mecanismos de Evasión de la Congestión[15][20]

Estos mecanismos permiten evitar la congestión de la red, anticipándose a los cuellos de botella. Si la interfaz de un router y su cola están saturadas, descartan los paquetes hasta que se elimine por completo la congestión. Existen tres mecanismos y son:

- *Tail drop*

  Este mecanismo brinda el mismo trato a todos los paquetes y los elimina según vayan llegando a la interfaz congestionada. No hay preferencia para ningún paquete; su objetivo es liberar la cola de la congestión, así que cualquiera puede ser descartado.

- *Random Early Detection* (RED)

  Este mecanismo evita la congestión descartando aleatoriamente los paquetes de la cola antes de que la congestión inunde la interfaz. Así, las conexiones reducirán la tasa de paquetes enviados y evitarán la congestión.

- *Weighted Random Early Detection* (WRED)

  Es un mecanismo que analiza las colas para evitar que se llenen y con ello, la congestión. Consiste en calcular la longitud media de la cola y compararla con sus umbrales: mínimo y máximo. Si el resultado está por debajo del umbral mínimo, los paquetes no serán descartados. Si este valor se ubica por encima del máximo, serán descartados indiscutiblemente. Pero, si la longitud se encuentra entre el mínimo y el máximo, los paquetes serán eliminados probabilísticamente. Es decir, mientras más se acerca la longitud al umbral máximo, mayor será el número de paquetes descartados.

1.1.9.3. Ingeniería de Tráfico (TE)[1][3][18]

La Ingeniería de Tráfico es una de las principales aplicaciones ofrecidas por MPLS debido a que permite: mejorar el performance de las redes mediante el control de tráfico y la optimización del uso de los recursos; brindar servicios diferenciados; evitar la congestión y ahorrar costos.

En la selección del LSP, la Ingeniería de Tráfico utiliza el enrutamiento ER-LSP para reservar los recursos y ofrecer diferentes tratamientos a cada Clase de Servicio. El concepto del mejor camino en Ingeniería de Tráfico no implica escoger el camino más corto, sino aquel que para determinado momento está disponible y es el más rápido independientemente de la distancia.

Los beneficios de la Ingeniería de Tráfico en redes MPLS son:

- Logra un uso más eficiente del ancho de banda asegurando que partes de la red no estén sobre utilizadas, mientras otras inutilizadas.
- Mejora las características del *performance* de la red minimizando la pérdida de paquetes, los retardos y el *jitter*.
- Presenta un mecanismo de adaptación dinámico de tolerancia a fallas reenrutando el tráfico por un camino alterno.
- La reducción de los costos es efectiva al tener mejor uso de los recursos de red.

Protocolos de enrutamiento en redes MPLS con TE[1][3][18][19]

En el enrutamiento dinámico, los protocolos estado de enlace han superado significativamente a los protocolos vector distancia sobre todo si se trata de redes grandes que requieren convergencia rápida y alta escalabilidad. MPLS con Ingeniería de Tráfico sugiere solo dos protocolos estado de enlace para el enrutamiento y son:

- *Open Shortest Path First* (OSPF)[19]

  OSFP es un protocolo estado de enlace orientado a cubrir los requerimientos de redes grandes. Utiliza como su métrica, el costo de las interfaces calculado por el algoritmo *Dijkstra*[7]*;* presenta alta convergencia al recrear la topología completa de la red en cada router; soporta máscaras de subred de longitud variable (VLSM) y autenticación de origen antes de analizar los estados de enlace nuevos.

  Para mejorar su administración, este protocolo divide la red en múltiples áreas asignadas a cada interfaz del router, por lo que un router puede pertenecer a una o más áreas. Recibe actualizaciones de los eventos en cada cambio de la topología aunque necesita mayores requerimientos de memoria y procesamiento que los protocolos Vector Distancia.

[7] Para mayor información del Algoritmo Dijkstra se recomienda revisar [19].

OSPF está estandarizado por la IETF en el RFC 1247, aunque para la implementación de IPv6 se ha creado la nueva: versión OSPFv3. Su principal ventaja es que está ampliamente difundido en las redes de los proveedores a nivel nacional.

- *Intermediate System-Intermediate System* (IS-IS)[19]
  IS-IS es un protocolo de enrutamiento dinámico desarrollado por la *Digital Equipment Corporation* (DEC), pero adoptado por la ISO en el RFC 1142. Fue el precursor de los protocolos de estado de enlace al soportar VLSM y autenticación de origen.

  Presenta alta convergencia gracias a que todos los routers disponen de la topología completa de la red. Su métrica es la suma total de los costos de las interfaces, calculada por el algoritmo *Dijkstra*. La distribución de la red se realiza mediante secciones llamadas áreas que se asocian a cada router, por lo que un router puede pertenecer a un área en particular.

  Su ventaja frente a OSPF es que brinda soporte a IPv6 en su versión original, aunque se limita porque no está ampliamente difundido en los proveedores a nivel nacional a diferencia de OSPF.

Protocolos de señalización en redes MPLS con TE[1][3][18]

Los protocolos de señalización en MPLS que soportan Ingeniería de Tráfico son:

- *Resource ReServation Protocol-Traffic Engineering* (RSVP-TE)[21][22]
  Este protocolo es una mejora de RSVP original. Tiene por objetivo reservar los recursos de la red para brindar Ingeniería de Tráfico y transportar servicios con QoS. Utiliza UDP o datagramas IP para la comunicación entre los pares LSR y enrutamiento explícito para la selección de los LSP.

  El proceso consiste en enviar “mensajes de trayectoria” (*path*) hasta el destino con la información del origen y las características de la ruta esperada. Una

vez que el destino recibe el mensaje *path*, contesta con un “mensaje de reserva” (*resv*) que viaja por el trayecto a la inversa del *path*, reservando los recursos para garantizar una camino libre de congestión.

Los *resv* son mensajes que van configurando los estados y los requerimientos de los recursos en cada router a lo largo del camino. Una vez que llegan al origen, se pueden trasmitir los paquetes por la ruta reservada. RSVP-TE permite el reenrutamiento de los túneles LSP para evitar: la congestión, los cuellos de botella y las caídas de la red.

Este protocolo es utilizado para implementar balanceo de carga y tunelización en MPLS. El balanceo de carga consigue que el tráfico pase por enlaces subutilizados logrando descongestionar los enlaces sobreutilizados. El proceso de tunelización permite la creación de rutas con QoS y minimiza el retardo de extremo a extremo.

- *Constrained Based Routing - Label Distribution Protocol* (CR-LDP)[2][21]

  El protocolo CR-LDP es una versión mejorada del protocolo LDP ya que establece sesiones TCP para comunicar los pares LSR. Soporta diferentes CoS e Ingeniería de Tráfico; establece los *Constrained Based Routing-Label Switched Protocol* (CR-LSP); y considera otro tipo de métricas, como: el ancho de banda, el retardo y el número de saltos de un paquete en la red.

  Los CR-LSP son caminos unidireccionales punto a punto y establecidos mediante enrutamiento explícito en los routers de origen. Se crean según los criterios de enrutamiento y las especificaciones de QoS.

  Los mensajes que utilizan son cuatro: *discovery*, para descubrir los pares LDP; *session,* para establecer la sesión; *advertisement,* para mantener y cerrar las conexiones; y *notification,* para rechazar el establecimiento de la conexión cuando el par LDP no acepta los parámetros negociados.

De la misma manera que RSVP-TE, este protocolo se utiliza para implementar balanceo de carga y protección de enlaces mediante túneles MPLS.

1.2. PROTOCOLO DE INTERNET VERSIÓN 6

1.2.1. INTRODUCCIÓN[4][5][6][7][10]

El crecimiento de usuarios en Internet durante las tres últimas décadas, ha sido exponencial. Los usuarios no tienen límite de género ni de edad; ni mucho menos los dispositivos con los que acceden. El mundo se hace más corto gracias a la gran red de redes: Internet.

El problema se centra en que los recursos son limitados y las direcciones IPv4 ya están agotadas. Cuatro millones de direcciones no fueron suficientes para la gran acogida que ha tenido y tiene Internet. La IETF necesitaba mejorar las características de IPv4 o empezar a buscar su reemplazo.

1.2.2. PROTOCOLO DE INTERNET VERSIÓN 4 (IPv4)

1.2.2.1. Definición de IPv4[4][5][6][7][10]

IPv4 es la primera versión comercial del Protocolo de Internet, estandarizado en el RFC 791 en septiembre de 1981. Dispone de aproximadamente 4 millones de direcciones únicas ($\mathbf{2^{32}}$), de las cuales ninguna está disponible para la compra en la actualidad.

IPv4 es un protocolo no confiable y no orientado a conexión, responsable de definir el formato y el enrutamiento de los paquetes IP entre los nodos de la red. Pertenece a la capa Internet de la arquitectura TCP/IP y define al “paquete” como su unidad de datos de protocolo (PDU).

1.2.2.2. Formato de la cabecera IPv4[4][5]

La cabecera IPv4 está formada por: 20 bytes de campos fijos y un campo variable de hasta 40 bytes llamado opciones; como se indica en la Figura 1.13.

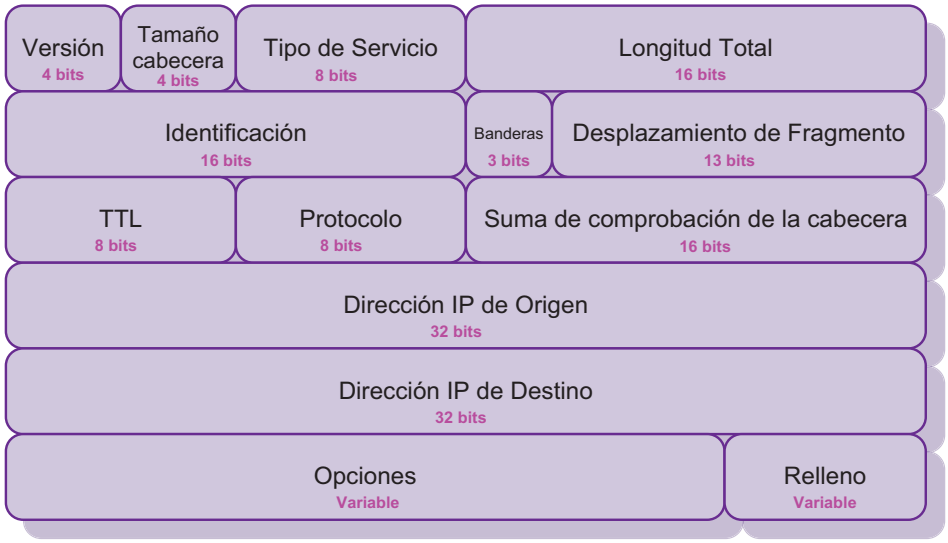


Figura 1.13 Cabecera IPv4
Fuente: [6]

La cabecera IPv4 está formada por los siguientes campos:

a. Versión: Campo formado por 4 bits que indica la versión del Protocolo de Internet. En la cabecera IPv4 se define el valor de 4.

b. Tamaño de la cabecera: Es un campo de 4 bits que refleja la longitud de la cabecera del paquete IP. Se representa en palabras de 32 bits con una longitud mínima de 5 (20 bytes).

c. Tipo de Servicio: Campo de 8 bits que indica la prioridad del paquete durante su reenvío por la red.

d. Longitud total: Campo de 16 bits que detalla la longitud total del paquete, incluyendo la cabecera y los datos. Se representa en octetos con una longitud mínima de 5 (20 bytes).

e. Identificación: Campo de 16 bits que permite identificar los fragmentos de un paquete.

f. Banderas: Campo de 3 bits utilizado para el control de la fragmentación de un paquete.

   Bit 0: Reservado para futuras aplicaciones. Debe ser 0.
   Bit 1: *Bit Don't Fragment*. 1L el paquete no puede ser fragmentado, 0L es fragmentado.
   Bit 2: Bit *More Fragments.* 1L fragmento intermedio, 0L último fragmento.

g. Desplazamiento de Fragmento: Campo de 13 bits que indica la posición de un fragmento en el datagrama. Se expresa en unidades de 8 bytes.

h. Tiempo de Vida (TTL): Campo de 8 bits que indica el número máximo de saltos que un paquete puede recorrer. En cada salto, el router disminuye este valor en una unidad y lo elimina si llega a cero.

i. Protocolo: Campo de 8 bits que contiene el código numérico del protocolo de capa superior que recibirá el paquete en el destino.[8]

j. Suma de comprobación de la cabecera: Campo de 16 bits que permite detectar errores en la cabecera de un paquete IP, a fin de garantizar su integridad.

k. Dirección IP Origen: Campo de 32 bits con la dirección IP del host origen.

l. Dirección IP Destino: Campo de 32 bits que indica la dirección IP del host destino.

m. Opciones: Campo de longitud variable (entre 0 y 40 bytes) para la implementación de pruebas y control de la red.

[8] Para mayor información sobre los números de los protocolos se recomienda revisar [50].

1.2.2.3. Direccionamiento en IPv4[9][23][42][43]

Para la mente humana le es difícil recordar los 32 bits con los que está formada una dirección IPv4. Es por ello que, se las representa en formato decimal dividiendo los 32 bits en cuatro grupos de 8 bits y separados por puntos (.).

Se detallan cinco clases de direcciones nombradas alfabéticamente de A hasta E. Definiendo, las clases A, B y C para ser asignadas a países y/o empresas que las requieran, la clase D para uso multicast y la clase E para uso experimental. Se tienen los bloques de direcciones detallados en la Tabla 1.2.

CLASES DE DIRECCIONES IP						
CLASE	BITS 1ER. OCTETO	RANGO DE DIRECCIONES	PREFIJO	MÁSCARA	NÚM. REDES	NÚM. HOST DISPONIBLES
A	0xxxxxxx	De 0.0.0.0/8 a 127.0.0.0/8	/8	255.0.0.0	$2^7 = 128$	$2^{24} - 2 = 16'777.214$
B	10xxxxxx	De 128.0.0.0/16 a 191.255.0.0/16	/16	255.255.00	$2^{14} = 16.384$	$2^{16} - 2 = 65.534$
C	110xxxxx	De 192.0.0.0/16 a 223.255.255.0/16	/24	255.255.255.0	$2^{21} = 2'097.152$	$2^8 - 2 = 254$
D	1110xxxx	De 224.0.0.0 a 239.255.255.255	-	-	-	-
E	1111xxxx	De 240.0.0.0 a 255.255.255.254	-	-	-	-

Tabla 1.2 Clases de direcciones IPv4
Fuente: [9]

Además, se diferencian dos tipos de direcciones según su uso: públicas y privadas. Las direcciones públicas son aquellas que pueden ser enrutadas en Internet; mientras las direcciones privadas se utilizan en las redes internas de los sistemas autónomos y no pueden ser usadas en Internet.

Los rangos de direcciones privadas se detallan en el RFC 1918 y se resumen en la Tabla 1.3. Mientras, las direcciones públicas son todas aquellas que no pertenecen a los rangos de direcciones privadas.

DIRECCIONES PRIVADAS (RFC 1918)		
CLASE	RANGO DE DIRECCIONES	
A	10.0.0.0/8	10.0.0.0 - 10.255.255.255
B	172.16.0.0/12	172.16.0.0 - 172.31.255.255
C	192.168.0.0/16	192.168.0.0 - 192.168.255.255

Tabla 1.3 Direcciones privadas IPv4

Fuente: [9]

1.2.3. PROTOCOLO DE INTERNET VERSIÓN 6

1.2.3.1. Definición de IPv6[4][5][6][7][10]

IPv6, o *Internet Protocol New Generation* (IPng), es la versión más reciente del Protocolo de Internet creado con los objetivos de reemplazar al protocolo IPv4 y seguir impulsando el crecimiento de Internet. Fue estandarizado por la IETF mediante el RFC 2460 el 25 de julio de 1994.

IPv6 dispone de 340 sextillones de direcciones ($\mathbf{2^{128}}$) asignadas por el *Internet Assigned Numbers Authority* (IANA)[48], y distribuidas por los cinco *Regional Internet Registries* (RIR) a nivel mundial, como son:

- *American Registry for Internet Numbers* (ARIN)
- *Réseaux IP Européens* (RIPE)
- *Asia-Pacific Network Information Centre* (APNIC)
- *Latin America & Caribbean Network Information Centre* (LACNIC)
- *African Network Information Center* (AFRINIC)

1.2.3.2. Antecedentes de IPv6[4][5][10][11][22]

La primera y más usada versión del Protocolo de Internet es IPv4, que a mediados de la década de los 90 se despliega con el auge de Internet. IPv1, IPv2 e IPv3 fueron versiones de prueba para el desarrollo de IPv4, pero nunca se los asignó como Protocolos de Internet.

Años después prediciendo el agotamiento de las direcciones IPv4, la IETF mediante el RFC 1550 solicita propuestas para hallar el protocolo que será el futuro reemplazo de IPv4. Muchas de las ideas presentadas consistían en desechar a IPv4 y reemplazarlo por protocolos completamente diferentes. En cambio otras, preferían realizar mejoras substanciales y conservar la idea original de IPv4.

Se receptaron en total 21 propuestas, de las cuales en diciembre de 1992, se seleccionaron 7; pero finalmente, en 1993 se publicaron las tres mejores: Deering, Francis y Katz-Ford. Todas aportaban al crecimiento y mejora de IPv4, pero se optó por crear una versión combinada de Deering y Francis conocida como: Protocolo Simple de Internet Mejorado (SIPP).

Internet Stream Protocol (ST o IPv5) fue el protocolo TCP/IP experimental para las transmisiones en tiempo real de SIPP, y su versión comercial se estandarizó años después como *Internet Protocol version* 6 (IPv6). Esta versión no es compatible con su predecesor: IPv4.

1.2.3.3. Formato de la cabecera IPv6[4][5]

El paquete IPv6 está formado por: una cabecera fija de 40 bytes distribuidos en 8 campos que se detallan en la Figura 1.14, una o varias cabeceras de extensión y el PDU de capas superiores.

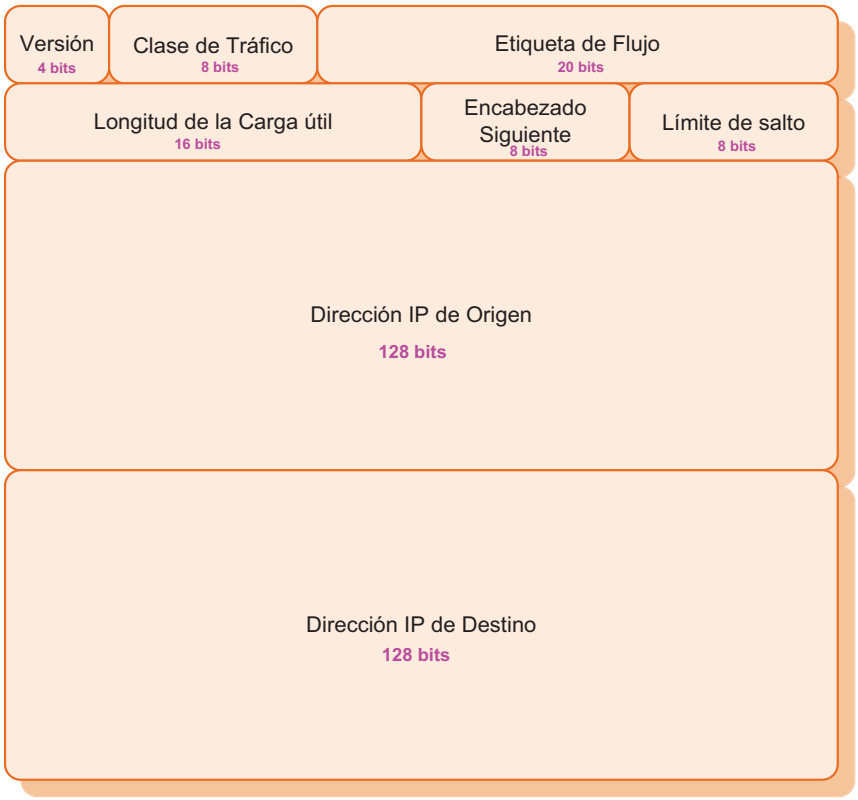


Figura 1.14 Cabecera IPv6 fija

Fuente: [4]

La cabecera IPv6 está formada por los siguientes campos:

a. Versión: Este campo está constituido por 4 bits que especifican la versión del Protocolo de Internet. Para una cabecera IPv6 se define el valor de 6.

b. Clase de tráfico: Campo de 8 bits que indica la prioridad del paquete durante su reenvío por la red. Su valor lo establecen los protocolos de capas superiores, permitiendo que los routers discriminen e identifiquen los requerimientos de transporte para cada paquete.

c. Etiqueta de flujo: Es un campo formando por 20 bits que identifica el tratamiento especial que recibirá el paquete por la red. Si su valor es diferente de cero, el router que lo analiza, le asignará un trato diferencial según la política configurada.

d. Longitud de la carga útil: Está constituido por 16 bits que detallan la longitud de los campos que le siguen a la cabecera fija; es decir, las cabeceras extendidas y el PDU de capas superiores.

e. Encabezado siguiente: Es un campo de 8 bits que indica si existen o no cabeceras de extensión después de la cabecera fija y de qué tipo son. Si no se agregan más cabeceras de extensión, en este campo se incluye el código del protocolo de transporte que recibirá el paquete (TCP o UDP).

f. Límite de saltos: Campo de 8 bits que indica el número de saltos máximos que le quedan por recorrer a un paquete. En cada salto que un router lo analiza, disminuye este valor en una unidad y puede eliminarlo si el valor llega a cero.

g. Dirección IP origen: Campo de 128 bits que indica el origen del paquete.

h. Dirección IP destino: Campo de 128 bits que especifica el destino del paquete.

1.2.3.4. Cabeceras de extensión de IPv6[4][5]

Las cabeceras de extensión de IPv6 se crearon debido a que muchos campos de la cabecera IPv4 son necesarios en ciertas ocasiones, pero no siempre como para integrarlos de manera obligatoria en la cabecera fija.

IPv6 enlista 6 tipos de cabeceras de extensión que se ubican después de los 40 bytes de la cabecera fija y antes del PDU de la capa transporte, como se indica en la Figura 1.15.

Figura 1.15 Paquete IPv6

Fuente: [4]

El campo “encabezado siguiente” tiene el identificador de la cabecera que viene a continuación de los 40 bytes, de lo contrario especifica el protocolo de la capa transporte que recibirá el paquete IPv6. Si se agregan más de una cabecera de extensión, estas deben respetar el orden establecido a continuación:

1. Cabecera de Opciones Salto-a-Salto[9]
2. Cabecera de Opciones para el destino (orientado al siguiente salto que no sea el destino final del paquete)
3. Cabecera de Encaminamiento
4. Cabecera de Fragmentación
5. Cabecera de Autenticación
6. Cabecera de Encapsulado de la Carga de Seguridad
7. Cabecera de Opciones para el destino (orientado al destino final del paquete)

1.2.3.5. Direccionamiento en IPv6[4][5]

Las direcciones IPv6 sirven para identificar de manera única a la interfaz de un dispositivo de red, de tal forma que los paquetes puedan ser enrutados de un host a otro. A diferencia de IPv4, una interfaz puede disponer de una o varias direcciones IPv6, logrando que los usuarios puedan trabajar con diferentes ISP y optimicen el servicio brindado.

En la versión 4, las direcciones IP eran de 32 bits; y en IPv6, de 128 bits, lo que genera un espacio mucho más amplio de direcciones. En la actualidad, los cinco registros RIR están distribuyendo el bloque 2001::/16.

Tipos de direcciones IPv6[4][5][8][11][19][23]

De la misma manera que en IPv4, se tienen direcciones: privadas y públicas. Las direcciones privadas se diferencian porque su primer octeto comienza con el valor

[9] Para mayor información sobre las cabeceras de extensión se recomienda revisar [4].

hexadecimal: “0xFE”; y se subdividen en direcciones: *link-local* y *site-local,* como se detallan en la Tabla 1.4.

PREFIJO HEXADECIMAL	TIPO DE DIRECCIÓN	DESCRIPCIÓN
FE80::/10	*link-local*	Se utilizan para la comunicación de enlaces físicos, como: las configuraciones automáticas y los descubrimientos de los vecinos. No se pueden enviar paquetes a través de estas subredes.
FEC0::/10	*site-local*	Permiten enrutar paquetes en las redes internas de una empresa. Equivalentes a las direcciones IPv4 del RFC 1918.

Tabla 1.4 Direcciones privadas IPv6

Fuente: [19]

Además, IPv6 maneja tres tipos de direcciones y son:

- Direcciones *unicast*s (Unidistribución)

  De la misma forma que en IPv4, un paquete con destino a una dirección unicast IPv6 será enviado únicamente a la interfaz que representa esta dirección.

- Direcciones *anycasts* (Monodistribución)

  Esta dirección identifica un conjunto de interfaces de un dispositivo de red o de diferentes. Si un paquete es enviado a esta dirección, se lo entregará a la interfaz más cercana identificada.

- Direcciones *multicasts* (Multidistribución)

  Esta dirección representa un conjunto de interfaces, generalmente de varios nodos. La diferencia con las direcciones *anycasts* es que si un paquete se envía a esta dirección, se lo entregará a todas y cada una de las interfaces que estén representadas. IPv6 optimiza el uso de *multicast* para evitar las direcciones *broadcast* en la red.

Representación de direcciones IPv6[4][5][28]

Las direcciones IPv6 se presentan en ocho grupos de cuatro *nibbles*[10] separados por dos puntos (:). La dirección *loopback* en IPv6 viene representada por ::1, a diferencia de IPv4 donde se tiene un rango de direcciones 127.0.0.0/24. Esta dirección está reservada para pruebas mediante el envío de paquetes a sí mismo y no puede ser asignada a ninguna interfaz.

Las direcciones IPv6 se sujetan a ligeras reglas para lograr disminuir y optimizar su representación. Como ejemplo, se ha seleccionado la dirección IPv6 mostrada a continuación para aplicarle las reglas y obtener una dirección equivalente pero más corta.

2100:1234:0000:0000:065B:293A:034B:3ABC

- Primera regla

  Se pueden omitir los ceros ubicados a la izquierda de cada grupo de cuatro *nibbles.* Entonces, los valores: 065B y 034B del ejemplo, se los puede reescribir como: 65B y 34B.

  La dirección IPv6 de ejemplo resultaría:

  2100:1234:0000:0000:**65B**:293A:**34B**:3ABC

- Segunda regla

  Los grupos de cuatro *nibbles* que estén encerados y sean continuos pueden ser remplazados por 4 puntos (::) en un solo. Esta regla puede ser ejecutada solo una vez en cada dirección IPv6, a fin de evitar confusiones de reemplazo.

  Para el ejemplo quedaría:

  2100:1234**::**65B:293A:34B:3ABC

[10] Un *nibble* es el grupo de cuatro dígitos binarios. Un número hexadecimal también puede estar representado en *nibbles* ya que 4 dígitos binarios son 1 dígito hexadecimal.

- Tercera regla

  El número de ceros que se deben aumentar en una dirección IPv6 optimizada, es el resultado de la diferencia entre los 128 bits y el número de bits de la dirección optimizada.

  Para el ejemplo quedaría:

  Dirección IPv6 optimizada: 2100:1234**::**65B:293A:34B:3ABC
  Número de bits: 16 + 16 + 16 + 16 + 16 + 16
  Número de bits a aumentar: 128 – 6 (16) = 32

  Dirección IPv6 representada en 128 bits:
  2100:1234:**0000:0000**:065B:293A:034B:3ABC

- Cuarta regla

  Si una dirección no está especificada, se la representa con dos puntos (::) e indica que está formada por 128 ceros lógicos. Se utiliza cuando un dispositivo no conoce su propia dirección y requiere referenciarse a sí mismo.

1.2.3.6. Motivos para migrar a IPv6[4][5]

El agotamiento de direcciones IPv4 fue el factor primordial que impulsó a la IETF a buscar un nuevo protocolo de Internet que lo reemplace. No solo por el crecimiento exponencial de usuarios en Internet que se registraron durante la última década; sino por la gran cantidad de usuarios que se incorporarán gracias a los nuevos dispositivos, como: *laptops*, teléfonos móviles, PDA y *tablets*. IPv6 brinda mayor flexibilidad para soportar los usuarios existentes y aquellos, que con seguridad se incrementarán. Mejora las debilidades de IPv4 y ofrece la oportunidad de que Internet siga creciendo.

A continuación, se muestran las mejores características de IPv6 que hacen que IPv4 sea un protocolo del pasado.

- IPv6 ofrece más de 340 sextillones de direcciones IP que posibilitan la conexión de más usuarios a Internet.
- La multiconexión de usuarios para que un host pueda conectarse no solo a uno sino a varios ISP.
- Direccionamiento de extremo a extremo sin hacer uso de la traducción de direcciones públicas a privadas y viceversa.
- Un encabezado mucho más eficiente y simplificado que IPv4, para brindar mayor rapidez en el procesamiento de los paquetes cuando atraviesan los dispositivos de la red. Establece cabeceras de extensión para no sobrecargar al encabezado con campos innecesarios.
- Mayor eficiencia en la implementación de direcciones: *anycast* y *multicast,* para brindar una red sin tormentas de *broadcast.*
- Mayor movilidad (estándar IP móvil).
- Mayor seguridad (IPSec), con autenticación y privacidad como características propias.
- Calidad de Servicio de extremo a extremo para trabajar con aplicaciones multimedia en Internet.

1.3. MECANISMOS DE TRANSICIÓN IPv4/IPv6 SOBRE MPLS[31][32]

Los proveedores de servicios de telecomunicaciones han empezado a migrar su tecnología de red a MPLS con el fin de brindar mejores servicios a sus clientes, a través de la implementación de: Ingeniería de Tráfico, Calidad de Servicio, VPN de MPLS, entre otras. El despliegue de IPv6 también se ha incrementado, y la demanda por parte de los clientes aún más. Sin embargo, migrar por completo a IPv6 todavía no es una opción, sobre todo porque IPv4 forma parte activa de las redes actuales.

Entonces, lo mejor será recurrir a un mecanismo de transición que permita implementar IPv6 sobre una red MPLS con núcleo en IPv4. Un mecanismo que brinde la mayor efectividad al menor costo, evitando en lo posible cambios en la infraestructura de la red.

Se diferencian tres mecanismos que permiten trabajar con IPv6 sobre redes MPLS y son:

- IPv6 sobre Circuitos de Transporte en MPLS
- IPv6 con Túneles en los routers CE
- IPv6 en routers PE (6PE/6VPE)

1.3.1. IPv6 SOBRE CIRCUITOS DE TRANSPORTE EN MPLS[33][34][35]

Es un mecanismo de transición que a través de circuitos de transporte estáticos, permite el uso de IPv6 sobre una infraestructura MPLS. Una de sus ventajas es que no implica reconfiguraciones en los routers LSR de la nube MPLS/IPv4; y por lo tanto, no se altera su funcionamiento normal. Resultando un mecanismo fácil de implementar y transparente al usuario.

La comunicación IPv6 entre los CE se la realiza sobre enlaces dedicados y la ejecución nativa de IPv6, mediante túneles de capa 2 configurados en los LER. Las tramas provenientes de tecnologías de capa 2 como: *Frame Relay*, ATM o *Ethernet*, son encapsuladas en MPLS y transportadas mediante etiquetas. El verdadero problema radica en la escalabilidad que enfrentan, ya que si la red empieza a crecer, el mallado de los enlaces dedicados se hará más tedioso.

Un ejemplo de este mecanismo es: *Any Trasport over MPLS* (AToM)[11], como se indica en la Figura 1.16. Una solución de transporte de capa 2 sobre redes IPv4/MPLS que ofrece Cisco, donde el tráfico IPv6 nativo viaja a través de circuitos estáticos. El uso de AToM para el despliegue y desarrollo de IPv6 sobre redes MPLS, no afecta el funcionamiento ni la infraestructura de la nube MPLS. No implica cambios en el software ni en la configuración de los LSR, aunque los LER deben soportar AToM.

[11] Para mayor información de AToM se recomienda revisar [49].

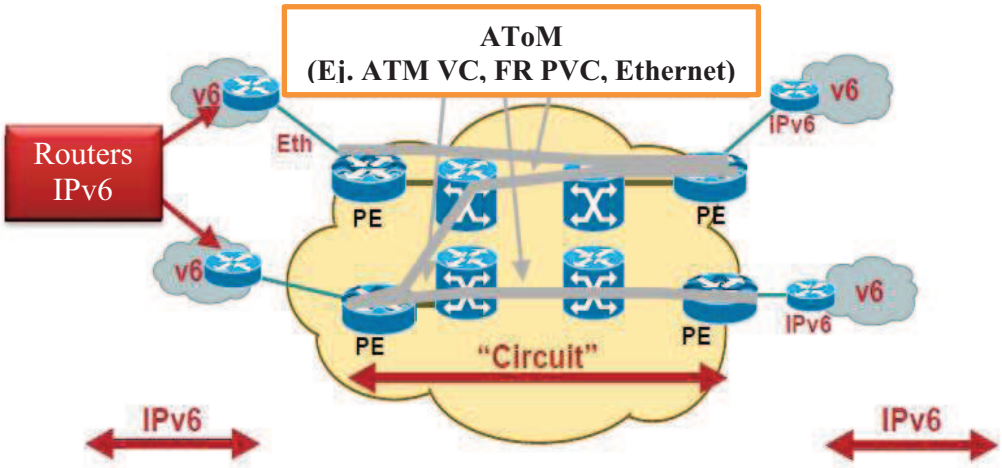


Figura 1.16 IPv6 sobre Circuitos de Transporte sobre MPLS

Fuente: [35]

1.3.2. IPv6 CON TÚNELES EN LOS ROUTERS CE[33][34]

Este mecanismo es quizá el más simple para brindar servicios IPv6 en redes MPLS. Implementa túneles tradicionales configurados en los routers CE, mientras el funcionamiento y la infraestructura de la red MPLS/IPv4 no se ve alterada. Los CE deben ser de doble pila para poder soportar las dos versiones de IP (IPv4 e IPv6).

La principal desventaja radica en la escalabilidad. Si la red es muy grande, el número de túneles por configurar lo es aún mayor; ya que se requiere un túnel entre cada CE IPv6 de la red (*full mesh*). Resultando un mecanismo estático y poco escalable.

Las configuraciones de los túneles se establecen por el administrador de la red en cada uno de los CE. Los paquetes IPv6 se encapsulan con encabezados IPv4 para ser transportados a través de túneles en la red MPLS/IPv4.

En la Figura 1.17 se indican cuatro túneles para poder transportar información de cuatro CE con IPv6. La red MPLS/IPv4 no se ve altera en su configuración; mientras los CE requieren ser de doble pila para soportar IPv4 e IPv6.

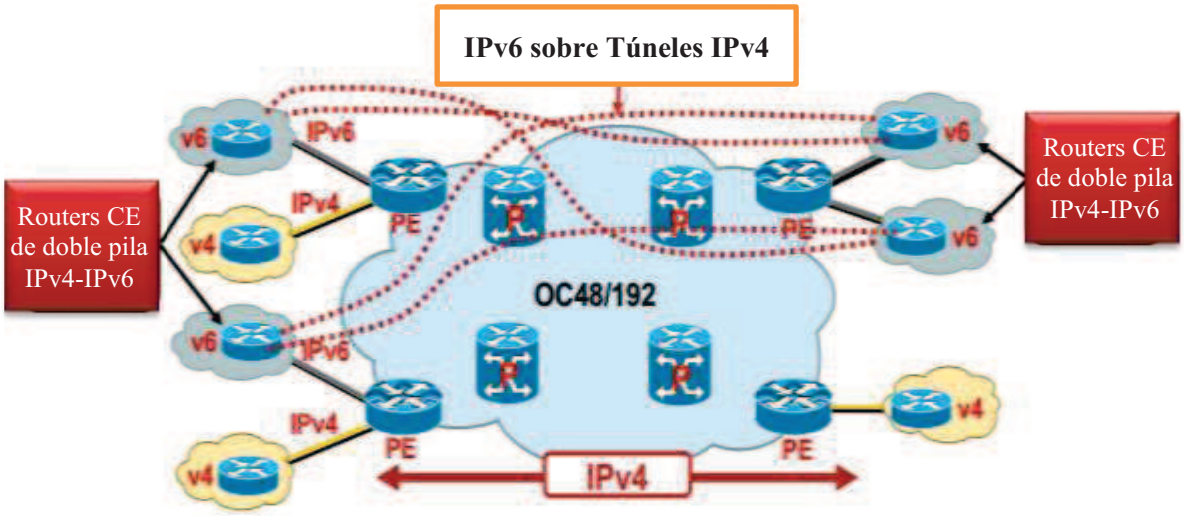


Figura 1.17 IPv6 con Túneles en los routers CE

Fuente: [35]

1.3.3. IPv6 EN ROUTERS PE (6PE/6VPE)[33][34][35]

Este mecanismo permite transportar los paquetes IPv6 a través de la red MPLS, utilizando el protocolo BGP. Cuando BGP se configura para soportar IPv4 e IPv6 se conoce como *Multiprotocolo - Border Gateway Protocol* (MP-BGP). 6PE es un mecanismo sumamente escalable, dinámico y excelente para trabajar en redes de ISP pequeñas y/o grandes. No amerita cambios en las configuraciones de los LSR, pero si actualizaciones en los LER para que soporten los dos protocolos: IPv4 e IPv6.

Como se muestra en la Figura 1.18, los LSR de la red MPLS no son conscientes de lo que están enviando. Usan un protocolo IGP para establecer la comunicación interna de la nube, y el protocolo LDP para el intercambio de etiquetas. Mientras, los LER son de doble pila para establecer las sesiones MP-BGP entre los dominios IPv4 e IPv6.

La implementación de este mecanismo en una red MPLS/IPv4 permite que los paquetes IPv6 de un cliente en particular, puedan enviarse a través de una VPN de capa 3. Al mecanismo que soporta VPN en IPv6 se conoce como: IPv6 VPN *Provider Edge Router* (6VPE).

6VPE es un mecanismo escalable que requiere configuraciones solo en los LER de la red MPLS. Permite que los dominios IPv6 se comuniquen usando tablas de enrutamiento separadas por cada VRF; y con ello, logren mayor seguridad en la transmisión porque una VRF en IPv6 tiene las mismas características de seguridad y transporte que una VRF en IPv4.

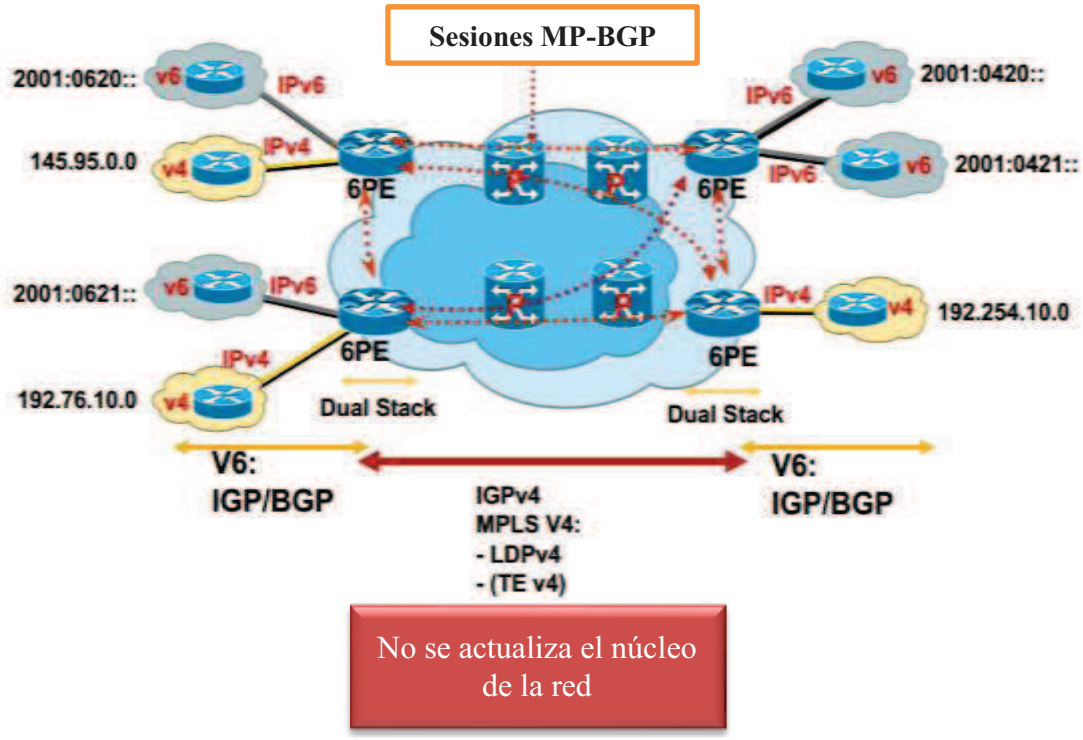


Figura 1.18 IPv6 *Provider Edge Routers*

Fuente: [35]

1.3.4. IPv6 SOBRE UNA RED MPLS/IPv6[35]

El objetivo final de la transición a IPv6 es que todos los ISP migren su infraestructura por completo a IPv6 y desplacen a IPv4; pero en la actualidad, un cambio de este tipo representa altos costos económicos ya que toda la red MPLS se verá afectada.

Manejar IPv6 sobre una red MPLS/IPv6 tiene una ventaja, y es ofrecer servicios en un contexto completo de IPv6; pero resulta improductivo en redes donde

todavía los servicios de IPv4 predominan. De lo contrario, sería necesario analizar un mecanismo que adopte el tráfico IPv4 a la red MPLS/IPv6.

En la Figura 1.19 se detalla una red MPLS migrada por completo a IPv6, donde tanto los routers de la nube MPLS como los CE están configurados en IPv6, y no existe ningún nodo con IPv4.

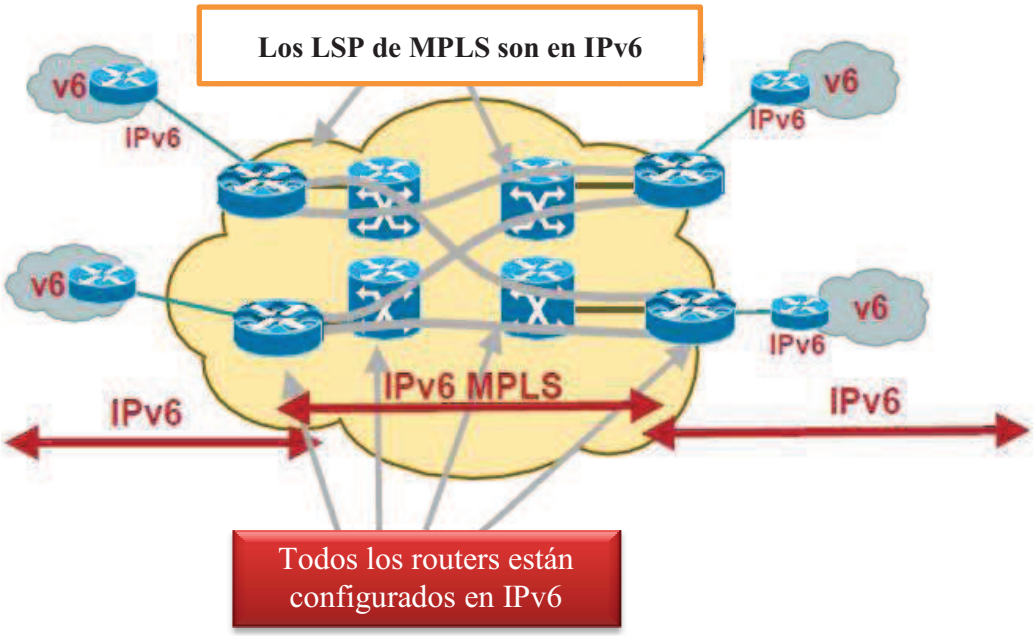


Figura 1.19 IPv6 sobre un Core MPLS/IPv6

Fuente: [35]

1.4. SEGURIDAD EN IPv6

1.4.1. INTRODUCCIÓN[4][5][8]

Las redes de computadoras se crearon con el objetivo de compartir recursos como una impresora, donde la seguridad no era un factor importante. En la actualidad, millones de personas acceden a las redes para realizar transacciones bancarias, compras y exámenes on-*line*, etc; donde la seguridad resulta crítica.

Aunque el término “seguridad” es amplio por la gran variedad de temas que abarca; es imprescindible analizar las posibles amenazas de las que puede ser víctima una red y los mecanismos para protegerla. Se puede definir a la seguridad

de redes como un grupo de estrategias y métodos que permitirán hacer a una red lo suficientemente robusta frente a ataques.

Las medidas de seguridad se pueden diferenciar en base a los servicios que se ofrecen, las cuales son: confidencialidad, integridad, disponibilidad, autenticación y no repudio. La confidencialidad impide que usuarios no autorizados conozcan la existencia de la información y la examinen. La integridad asegura que la información enviada no ha sido modificada por un ente malicioso. La disponibilidad garantiza que la información está lista para ser usada en el momento necesario. La autenticación controla que la entidad origen y/o destino es quién dice ser antes de publicar la información. Mientras, el no repudio se encarga de evitar que la entidad emisora y/o receptora niegue que envió y/o recibió la información.

La seguridad no pertenece a una capa del modelo OSI en particular sino que se encuentra implícita en todas. La autenticación y el no repudio se controlan en la capa aplicación, la seguridad de extremo a extremo en la capa transporte, los *firewalls* usualmente en la capa red, la encriptación en la capa enlace de datos y los candados en la capa física.

1.4.2. SEGURIDAD EN LAS REDES IPv4/IPv6[13][16]

La transición de IPv4 a IPv6 no garantiza que las redes sean más seguras. Todo lo contrario, ahora se requiere analizar las vulnerables en cada versión de IP. Este tipo de redes pueden ser víctimas de ataques desde cualquiera de los dos protocolos; por lo que si se deniega o permite un *host,* el análisis de seguridad se debe establecer para las direcciones IPv4 e IPv6 que disponga el *host,* considerando que son dos versiones incompatibles.

Lo importante es establecer estrategias de seguridad que permitan cumplir con los objetivos de la empresa, independientemente de la versión IP que se tenga configurada. En las secciones 1.4.3 y 1.4.4 se detallan los conceptos básicos de seguridad en los protocolos de Internet: IPv4 e IPv6.

1.4.3. SEGURIDAD EN REDES IPv4[4][5][8]

La seguridad en IPv4 se logra mediante IPSec, que es un conjunto de estándares que establecen conexiones seguras punto a punto a través de algoritmos de encriptación de llave pública, garantizando la integridad, la confidencialidad y la autenticación de la información.

En vista de que la seguridad no pertenece a ninguna capa del modelo OSI en particular y con el fin de mantener el enfoque de extremo a extremo, se ha definido a IPSec como un mecanismo de la capa de red incorporado en el protocolo IPv6. La ventaja de IPSec es que está integrado de forma nativa en IPv6, mientras en IPv4 su implementación es opcional pero ampliamente difundida. Aunque esto es relativo, porque en la actualidad existen redes IPv4 configuradas con IPSec y redes IPv6, sin IPSec[12].

IPSec detalla en su arquitectura dos modos: transporte y túnel. El modo transporte se caracteriza porque la cabecera IPSec se inserta después de la cabecera IP. En el campo protocolo de la cabecera IP se detallan los valores 50 o 51, para indicar que a continuación le sigue una cabecera IPSec.

Por el contrario, el modo túnel encapsula todo el paquete en un nuevo paquete IP agregando otra cabecera. Este modo es útil cuando el túnel tiene en su extremo remoto un equipo de seguridad, como un *firewall;* que será el encargado de desencapsular el paquete para que al destino, IPSec le sea transparente. También, es útil en conexiones TCP cifradas para evitar que ningún intruso conozca la existencia de los datos, el origen y el destino del paquete.

La desventaja del modo túnel en relación al modo transporte, es que tiene que agregar una cabecera IP adicional, disminuyendo el rendimiento de la red. Además, existen otros mecanismos que permiten, a las redes IPv4, brindar seguridad en la transmisión, como son[13]: los *firewalls*, las Listas de Control de

[12] Para mayor información de IPSec se recomienda revisar [5], páginas 629-635.
[13] La seguridad en redes IPv4 abarca el estudio de varios subtemas como: los *firewalls, los protocolos seguros, etc;* que salen del alcance de este proyecto. Para mayor información redes se recomienda revisar [4], capítulo 8, páginas 721-828.

Acceso (ACL), los algoritmos de encriptación, las Redes Privadas Virtuales (VPN), la implementación de protocolos seguros y las VLAN.

1.4.4. SEGURIDAD EN REDES IPv6[13][14][16]

La seguridad en IPv6 es un tema que aún no ha sido profundizado. El protocolo IPv6 fue diseñado para ser más seguro gracias a la encriptación y autenticación que IPSec conlleva de forma nativa. Las debilidades de IPSec fueron corregidas en IPv6, pero esto no garantiza que la seguridad en IPv6 es 100% fiable.

Los problemas de seguridad son prácticamente los mismos en IPv4 e IPv6 con excepción de la fragmentación de paquetes. En IPv6, los *host* finales pueden fragmentar los paquetes evitando que los routers intermedios agreguen datos maliciosos.

Además, IPv6 tiene una gran ventaja de seguridad frente a IPv4, y es que dificulta la realización de *brute force scanning* ya que maneja un rango de direcciones bastante grande; aunque no se descarta la posibilidad de que las herramientas de escáner mejoren.

Las amenazas de seguridad en IPv6 pueden tener el mismo comportamiento que en IPv4, como[14]: los ataques *man-in-the-middle,* cuando no se garantiza la integridad del paquete ya que es alterado durante su trayecto; *sniffing,* cuando se atenta contra la confidencialidad porque un ente está analizando la información; *spoofing,* cuando existe suplantación de identidad afectando la autenticación*;* y los ataques de denegación de servicio (DoS) que atentan contra la disponibilidad de los servicios y/o equipos.

En IPv6 existen técnicas de mitigación de amenazas, como: las restricciones en el acceso a la red con las ACL; los algoritmos de encriptación; las VPN; la implementación de protocolos seguros; las VLAN; los *firewalls*, aunque todavía se

[14] Las amenazas de seguridad son un tema sumamente amplio que están fuera del alcance de este proyecto, para mayor información se recomienda revisar [5], capítulo 18, páginas 605-636.

tiene problemas de compatibilidad con IPv6; y el mecanismo de descubrimiento seguro de vecinos (SEND)[15] que no ha sido ampliamente difundido porque resulta difícil de implementar gracias a las llaves *public-key infraestructure* (PKI) que maneja.

Las redes IPv6 todavía no han sido el centro de atacantes. No se tienen muchas herramientas para debilitarla aunque se espera que estas herramientas evolucionen. Con seguridad se descubrirán más vulnerabilidades en redes que están funcionando, aunque falta tiempo para ello. Lo importante es capacitar a los ingenieros y los técnicos de red en IPv6; y definir en lo posible, las políticas de seguridad en IPv6 e IPv4 para obtener resultados favorables.

1.4.5. MEJORES PRÁCTICAS DE SEGURIDAD EN IPv6[26]

Las Mejores Prácticas de Seguridad de una red se definen con el fin de crear una estrategia de seguridad óptima para la empresa. La responsabilidad del administrador de seguridad viene establecida no solo por la parte técnica, sino por la alineación con los objetivos del negocio de manera que las políticas cumplan con el marco interno de la empresa.

La seguridad de una red en IPv4 es un tema complejo, y más, si se agrega el protocolo IPv6. Ahora, el administrador de red no solo debe establecer las estrategias de seguridad para IPv4, sino también para IPv6. La lista de estrategias puede ser muy extensa, pero si se consideran las más eficaces, con seguridad se obtendrá una mejora substancial en el tiempo de operación de la red ya que se disminuye la probabilidad de ataque.

Las Mejores Prácticas de Seguridad serán analizadas considerando: las VLAN, Listas de Control de Acceso en IPv6 y la gestión mediante acceso remoto seguro; como se indican en las secciones 1.4.5.1, 1.4.5.2 y 1.4.5.3.

[15] Para mayor información de SEND y la implementación de llaves PKI se recomienda revisar [45].

1.4.5.1. VLAN[14][19][36][37]

Una Red de Área Local Virtual (VLAN) es una medida de seguridad sencilla de capa 2 que permite dividir una red física, en varias redes independientes lógicamente. Cada VLAN representa un dominio de *broadcast* separado que permite intercambiar información en capa 2 solo entre los usuarios miembros de la VLAN; aunque se implementa el enrutamiento inter-VLAN mediante un dispositivo de capa 3.

Las ventajas de implementar VLAN son: la facilidad para agregar nuevos usuarios, el traslado físico de un equipo de acceso sin la necesidad de cambiar su configuración de direccionamiento IP y de VLAN, el ahorro económico al segmentar la red en dominios de *broadcast* más pequeños con switches y no con routers, y lo más importante, la seguridad que conlleva separar el tráfico de las VLAN.

Los administradores de red implementan las VLAN con el objetivo de administrar de mejor manera su red ya sea por departamentos o proyectos de la empresa. Mientras, un ISP recurre a las VLAN para segmentar su red por servicios y/o tipos de usuarios en los dispositivos de capa 2.

A continuación se detalla la creación de VLAN en un dispositivo de capa 2 Cisco:

- Desactivar todas las interfaces del switch

  Como medida de seguridad, es importante desactivar todas las interfaces del switch para evitar que usuarios no autorizados se conecten a la red.

  ```
  SWITCH(config)#interface <tipo_interface> <número_interfaz>
  SWITCH(config-if)#shutdown
  ```

- Crear las VLAN

  Se definen las VLAN con un número y un nombre opcional. El número de VLAN máximo viene definido por el modelo del dispositivo.

  ```
  SWITCH(config)#vlan <número_vlan>
  SWITCH(config)#name <nombre_vlan>
  ```

- Configurar la dirección IP en la VLAN administrativa

```
SWITCH(config)#interface vlan <número_vlan_administración>
SWITCH(config-if)#ip address <dirección_ip> <máscara>
```

Si se desea configurar la VLAN de administración con una dirección IPv6 en los switches Catalyst, se debe primero cambiar la plantilla de administración de la base de datos a doble pila (IPv4 e IPv6).

```
SWITCH(config)#sdm prefer dual-ipv4-and-ipv6 default
```

Se reinicia el dispositivo guardando los cambios.

```
SWITCH(config)#reload
```

Se habilita IPv6 en el switch.

```
SWITCH(config)#ipv6 unicast-routing
SWITCH(config)#interface vlan <número_vlan_administración>
```

Se habilita IPv6 en la interfaz.

```
SWITCH(config-if)# ipv6 enable
```

Se configura la dirección IPv6 y la máscara.

```
SWITCH(config-if)# ipv6 address <dirección_ipv6/máscara>
```

- Configurar la interfaz troncal

La interface troncal es aquella por donde pasa la información de las VLAN del switch hacia un dispositivo de capa 3.

```
SWITCH(config)#interface <tipo_interface> <número_interfaz>
```

Se configura la encapsulación 802.1q[16] en el enlace troncal.

```
SWITCH(config-if)#switchport trunk encapsulation dot1q
```

Se configura el modo de la interfaz a troncal.

```
SWITCH(config-if)#switchport mode trunk
```

Se define la interfaz nativa.

```
SWITCH(config-if)#switchport trunk native vlan <número_vlan>
```

Se definen las VLAN permitidas en la interfaz.

```
SWITCH(config-if)#switchport trunk allowed vlan <número_VLAN>
```

Se habilita la interfaz.

```
SWITCH(config-if)#no shutdown
```

[16] IEEE 802.1q es el protocolo responsable del etiquetado de las tramas a fin de que se permita compartir un mismo medio físico, entre varias redes asociadas a diferentes VLAN. Para mayor información del protocolo de la IEEE 802.1Q se recomienda revisar [4].

- Asociar la interfaz a una VLAN de acceso

  Se configuran la interfaces o rangos de ellas en modo acceso y se asocia la VLAN designada.

```
SWITCH(config)#interface <tipo_interface> <número_interfaz>
SWITCH(config-range)#switchport mode access
SWITCH(config-range)#switchport access vlan <número_vlan>
SWITCH(config-range)#no shutdown
```

- Configurar la puerta de salida

  Se configura la puerta de enlace con el fin de que el tráfico tenga una interfaz de salida cuando el enrutamiento se activa.

```
SWITCH(config)#ip default-gateway <dirección_ip>
```

  Si la interfaz VLAN tiene configurada una dirección IPv6 se debe configurar una ruta por defecto en calidad de puerta de salida.

```
SWITCH(config)#ipv6 route ::0/0 <dirección_ipv6>
```

1.4.5.2. Listas de Control de Acceso en IPv6[8][14][29][30][36][37][38][39][52]

Una lista de control de acceso (ACL) es un filtro para permitir o denegar el acceso a los recursos de la red. Son analizadas según: las direcciones IP de origen y destino, los protocolos de capa superiores y los puertos configurados.

El orden de las líneas de comandos en una ACL es importante, debido a que el control se hace en el mismo orden en el que fueron creadas. Cada lista de acceso tiene una línea de comandos implícita al final, con el objetivo de denegar todo lo que no esté detallado en la ACL.

La funcionalidad de las ACL en IPv6 es similar a las ACL en IPv4 con ciertas limitaciones. En IPv4 se tienen ACL: estándares, extendidas, nombradas y numeradas; mientras en IPv6 solo se soportan las extendidas nombradas. El comando para asociar un interfaz con una ACL IPv6 es diferente en relación a IPv4, aunque tienen el mismo significado. Una dirección IPv6 no utiliza la máscara *wildcard* sino la barra inclinada “/” para ser representada.

A continuación se detalla la configuración de una ACL en IPv6 para dispositivos Cisco:

- Definir la ACL

  Las ACL en IPv6 solo tienen soporte para ACL extendidas nombradas. Las ACL extendidas tienen que especificar las direcciones IPv6 origen y destino en cada entrada.

  ```
  ROUTER(config)#ipv6 access-list <nombre_ACL>
  ```

  Una ACL IPv6 puede permitir o denegar una red IPv6 o un host específico. Para mayor control se puede relacionar la ACL con un protocolo o puerto.

  ```
  ROUTER(config-ipv6-acl)#<permit|deny> ipv6 [<direc_ipv6/másc>|
  host <direc_ipv6>|any] [<direc_ipv6/másc>|host <dire_ipv6|any]
  <eq|neq> <protocol|puerto>
  ```

  Línea de denegación implícita al final de la ACL.

  ```
  ROUTER(config-ipv6-acl)#deny ipv6 any any
  ```

- Asociar la ACL IPv6 a una interfaz

  Una vez definida la ACL se puede aplicarla a la entrada o salida de las interfaces de un dispositivo de red. En IPv4 el comando utilizado es: *ip access-group*; mientras en IPv6 lo es: *ipv6 traffic-filter.*

  ```
  Router(config)# interface Fa0/1
  Router(config-if)# ipv6 traffic-filter <nombre_ACL> [in|out]
  ```

1.4.5.3. Acceso remoto seguro en IPv6[14][25][36][37][51]

El acceso remoto puede ser una puerta abierta de seguridad si no está correctamente configurado y protegido. La información de la empresa, el acceso a los dispositivos y el funcionamiento de la red en sí, se exponen cuando el acceso remoto es ligero.

Telnet (puerto 23) es el protocolo de gestión remota que se configura por defecto en los dispositivos de red, pero tiene una gran desventaja, envía la información en texto plano. *Telnet* no es una solución segura de acceso, todo lo contrario es una solución vulnerable a ataques.

Secure SHell (puerto 22) trabaja de manera análoga a *telnet* ya que permite el acceso remoto a máquinas y/o dispositivos a través de la red. La diferencia es que usa conexiones seguras, implementa autenticación y proporciona terminales con sesiones cifradas.

Existen dos versiones de SSH: la primera, utiliza algoritmos de cifrado propietarios que no se han seguido desarrollando por lo que presentan huecos de seguridad; mientras, la segunda implementa algoritmos de encriptación de llave pública como *Rivest, Shamir y Adleman* (RSA)[17] que lo hacen más robusto. La versión 2 es compatible y soporta las conexiones de la versión 1; así como direcciones IPv4 e IPv6.

SSH en IPv6 tiene las mismas funcionalidades que SSH en IPv4, como: la generación de claves públicas, la versión, el modo de acceso en los terminales virtuales, etc; pero en la actualidad solo existe una limitante para IPv6 y es la autenticación. La autenticación local de nombre de usuario y contraseña es el único mecanismo que permite autenticar direcciones IPv6, mientras TACACS+ y RADIUS[18] no tienen soporte para IPv6.

A continuación se detalla el proceso para implementar SSH en dispositivos Cisco:

- Configurar los parámetros básicos de SSH

  Se establece: el nombre de dominio de la empresa, la versión de SSH requerida, el tiempo de la conexión abierta sin actividad y el número de reintentos de autenticación SSH de un usuario.

```
ROUTER(config)#ip domain-name <dominio_empresa>
ROUTER(config)#ip ssh version <1|2>
ROUTER(config)#ip ssh time-out <0-120s>
ROUTER(config)#ip ssh authentication-retries <0-5>
```

- Generar las llaves

  Se generan las llaves pública y privada para la autenticación RSA.

[17] Para mayor información de RSA se recomienda revisar [4], páginas 753-755.
[18] Para mayor información de TACACS+ y RADIUS se recomienda revisar [27] y [44].

```
ROUTER(config)#crypto key generate rsa general-keys modulus
1024
```

- Configurar una ACL en IPv6

  Para tener mayor control de acceso, es opcional configurar una ACL que permita o deniegue el tráfico de un *host* o de una red en particular.

```
ROUTER(config)#ipv6 access-list <nombre_ACL_IPv6>
ROUTER(config-ipv6-acl)#deny ipv6 host <dirección_ipv6> any
ROUTER(config-ipv6-acl)#permit ipv6 <dir_ipv6/máscara> any
ROUTER(config-ipv6-acl)#deny ipv6 any any
```

- Configurar los terminales virtuales

  En los terminales virtuales se deben configurar: el modo de acceso: SSH y/o *telnet* y las ACL IPv6 en caso de que hubiesen.

```
ROUTER(config)#line vty 0 15
ROUTER(config-line)#ipv6 access-class <nombre_ACL_IPv6> in
ROUTER(config-line)#transport input ssh
ROUTER(config-line)#transport output telnet ssh
```

REFERENCIAS BIBLIOGRÁFICAS
CAPÍTULO 1

LIBROS Y MANUALES

[1] VIVEK, Alwayn. “Advanced MPLS Design and Implementation”. Cisco-Press. Estados Unidos de América. Septiembre, 2001.

[2] HIDALGO LASCANO, Pablo William. Folleto “Redes de Área Extendida”. Escuela Politécnica Nacional. Quito, Ecuador. Marzo, 2011.

[3] ALMEIDA ARCOS, Andrés. “Arquitectura de Redes MPLS”. Academia de Certificaciones Internacionales en Redes y Tecnologías de Información ACIERTE-EPN. Quito, Ecuador. Junio, 2011.

[4] TANENBAUM, Andrew S. “Redes de Computadoras”. Cuarta Edición. PRETICE HALL. Vrije Universiteit. México. 2003.

[5] STALLINGS, William. “Comunicaciones y Redes de Computadores”. Séptima Edición. PRETICE HALL. Madrid, España. 2004.

[6] HIDALGO LASCANO, Pablo William. Folleto “Redes TCP/IP”. Escuela Politécnica Nacional. Quito, Ecuador. Marzo, 2009.

[7] MILES, David. MAGLIONE, Roberta. TOWNSLEY, Mark. “IPv6 for PPP Broadband Access TR-187”. Broadband Forum Technical Report. Mayo, 2010.

[8] ANÓNIMO. “Acceso a la WAN - CCNA 4”. Academia de red Cisco. Módulo cuatro. Cuarta edición. Capítulos 4 y 7. Madrid, España. 2007-2008.

[9] ANÓNIMO. “Aspectos Básicos de Networking - CCNA 1”. Academia de red Cisco. Módulo uno. Cuarta edición. Capítulo 8. Madrid, España. 2007-2008.

[10] CICILEO, Guillermo. ROQUE, Gagliano. O’FLAHERTY, Christian. “IPv6 para Todos - Guía de uso y aplicación para diversos entornos”. Internet Society. Buenos Aires, Argentina. 2009.

[11] PALET, Jordi. “Introducción a IPv6”. Consulintel. Cancún, México. Mayo, 2011.

[12] ANÓNIMO. “Nivel de Servicio Garantizado”. Telconet S.A. sucursal Quito, Ecuador. Agosto, 2011.

[13] VIVES, Álvaro. “Despliegue de IPv6”. 6Deploy. Santa Cruz, Bolivia. Octubre, 2010.

[14] ROMERO TERNERO, MariCarmen. “Seguridad en Redes y Protocolos Asociados”. Ingeniería de Protocolos. España, 2010.

[15] ALMEIDA ARCOS, Andrés. “BGP y Calidad de Servicio en Redes Convergentes”. Academia de Certificaciones Internacionales en Redes y Tecnologías de Información ACIERTE-EPN. Quito, Ecuador. Noviembre, 2011.

[16] GONT, Fernando. “Seminario IPv6”. Cisco Seminars: IPv6 Migration. Buenos Aires, Argentina. Julio, 2011.

[17] VALDIVIA GÓMEZ, Javier Rafael Ms.C. PEÑA MOLINER, Carmen DrC. “MPLS y su Aplicación en Redes Privadas Virtuales (L2VPN Y L3VPN)”. LACCET - Information Technology Track. Paper No. 83. Cartagena de Indias, Colombia, 2005.
Web: http://laccei.org/LACCEI2005-Cartagena/Papers/IT083_MolinerPena.pdf

[18] DE GHEIN, Luc CCIE. “MPLS Fundamentals”. Cisco Press. No. 1897. ISBN: 1-58705-197-4. Indianapolis, Estados Unidos de América. Noviembre, 2006.

[19] ANÓNIMO. “Conceptos y Protocolos de Enrutamiento - CCNA 2”. Academia de red Cisco. Módulo dos. Cuarta edición. Capítulos 4 y 5. Madrid, España. 2007-2008.

[20] ANÓNIMO, “Implementing Cisco Quality of Service”. *Student Guide* Cisco *Systems*, Inc. Versión 2.2. Volúmenes 1 y 2. 2006.

PROYECTOS DE TITULACIÓN

[21] NIETO PORRAS, Luisana Bertilda. “Diseño y Configuración de Calidad de Servicio en la Tecnología MPLS para un Proveedor de Servicios de Internet”. EPN. Mayo, 2010.

[22] MARCHÁN MERINO, Julia Soledad. YÁNEZ QUINTANA, Daniel Alfonso. “Estudio y Diseño para la Migración de una Red Gigabit Ethernet de datos de una Empresa Portadora de Servicios a la Tecnología MPLS (Multiprotocol Label Switching)”. Abril, 2008.

[23] HINOJOSA LÓPEZ, Mayra Alexandra. HERRERA MERCHÁN, Fabricio Fernando. “Diseño de una Red MPLS utilizando el Protocolo IPv6 para Proveedores de Servicios de Telecomunicaciones”. Julio, 2009.

DIRECCIONES ELECTRÓNICAS

[24] INTERNET ENGINEERING TASK FORCE. “Multiprotocol Label Switching Architecture”. Enero, 2001.
http://www.ietf.org/rfc/rfc3031.txt

[25] GARCÍA CAPEL, Daniel. “Comandos CISCO CCNA Exploration”. Cisco Systems, Inc. 13 de abril de 2011.
http://dani.albatalia.com/code/cisco/comandos_cisco_ccna_exploration.pdf

[26] VYNCKE, Eric. “IPv6 Security Best Practices”. Distinguished System Engineer. Estados Unidos de América. 2007.
http://www.cisco.com/web/SG/learning/ipv6_seminar/files/02Eric_Vyncke_Security_Best_Practices.pdf

[27] ANÓNIMO. “TACACS.net TH”. 2010. Web: http://www.tacacs.net/

[28] ANÓNIMO. “Internet Protocol Version Address Space”. Internet Assigned Numbers Authority.
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

[29] ANÓNIMO. “Implementing Traffic Filters and Firewalls for IPv6 Security”. Cisco Systems, Inc. Estados Unidos de América. 2010. http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-sec_trfltr_fw.html

[30] ANÓNIMO. “IPv6 Filtering”. ISP/IXP Workshops. Cisco Systems, Inc. Estados Unidos de América. 2006. http://support.udsm.ac.tz/ipv6/c6-1up.pdf

[31] CLAUBERG, Axel. “Deploying IPv6 Networks Cisco”. Session RST-231. Cisco IOS Software. 2002. http://www.ipv6-es.com/02/docs/patrick_grossetete_1.pdf

[32] VIVES, Álvaro. “Despliegue de IPv6”. WALC2011. Guayaquil, Ecuador. 10-14 de octubre de 2011. http://www.6deploy.eu/workshops2/20111010_guayaquil_ecuador/DIA5-1-2-Consulintel _Curso-IPv6_WALC2011.pdf

[33] LIAKOPOULOS, Athanassios. “IPv6 over IPv4/MPLS Networks: The 6PE Approach”. III Global IPv6 Summit. Greek Research & Technology Network (GRNET). Moscow, Rusia. 25 de noviembre de 2004. http://www.free.net/NTL/IP6/presentation/ALiakopoulos%20-%206PE%20-%203rd%20Global%20IPv6%20Summit.pdf

[34] ANÓNIMO. “Cisco IOS IPv6 Provider Edge Router (6PE) over MPLS”. Cisco IOS Software Releases 12.2 Mainline. http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_data_sheet09186a008052edd3.html

[35] GROSSETET, Patrick. “IPv6 over MPLS: Cisco IPv6 Provider, Edge Router (6PE), Cisco IPv6 VPN, Provider Edge y Router (6VPE)”. Cisco Systems, Inc. Estados Unidos de América. 2006. http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/prod_presentation0900aecd80311df4.pdf

[36] CONVERY, Sean. MILLER, Darrin. “IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)”. Cisco Systems, Inc. Estados Unidos de América. 2004. http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf

[37] ANÓNIMO. “IPv6 Security”. Cisco Networkers. Estados Unidos de América. 2006. http://www.cu.ipv6tf.org/pdf/cdccont_0900aecd8057a244.pdf

[38] ANÓNIMO. “Configuring IPv6 ACL”. Chapter 37. Cisco IOS Software Releases 12.2 Mainline. Estados Unidos de América. 2010. http://www.cisco.com/en/US/docs/switches/metro/me3400/software/release/12.2_50_se/configuration/guide/swv6acl.pdf

[39] STRETCH, Jeremy. “IPv6 Access Lists on IOS”, PacketLife. Virginia, Estados Unidos de América. 2010. http://packetlife.net/blog/2010/jun/30/ipv6-access-lists-acl-ios/

[40] ANÓNIMO. “Cisco Express Forwarding (CEF) Introduction”. Cisco IOS Software Releases 12.2 Mainline. http://www.cisco.com/en/US/tech/tk827/tk831/tk102/tsd_technology_support_sub-protocol_home.html

[41] ANÓNIMO. “MPLS Label Distribution Protocol”. Cisco IOS Software Releases 12.2 Mainline. http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/ftldp41.html

[42] ANÓNIMO. “LACNIC XVII - Quito, Ecuador”. Registro de Internet de América Latina y el Caribe. 29 de julio de 2011. http://lacnic.net/sp/anuncios/lacnicxvii.html

[43] REKHTER, Y. MOSKOWITZ, B. “Asignación de direcciones para Internet Privadas - RFC 1918”. Febrero, 1996. http://www.rfc-es.org/rfc/rfc1918-es.txt

[44] ANÓNIMO. “FREERADIUS The world's most popular RADIUS Server”. Network RADIUS Inc. 2012. Web: http://freeradius.org/

[45] LAKSHMI. “Secure Neighbor Discovery (SEND)”. IPv6.com Tech Spotlight. http://www.ipv6.com/articles/research/Secure-Neighbor-Discovery.htm

[46] PATTERSON, Michael. “What is VRF: Virtual Routing and Forwarding”. 10 de diciembre de 2009. http://www.plixer.com/blog/netflow/what-is-vrf-virtual-routing-and-forwarding/

[47] ANÓNIMO. “Virtual Private LAN Services (VPLS)”. Cisco Systems Inc. http://www.cisco.com/en/US/products/ps6648/products_ios_protocol_option_home.html

[48] ANÓNIMO. Internet Assigned Numbers Authority (IANA). Web: http://www.iana.org/

[49] ANÓNIMO. “Cisco Any Transport over MPLS”. Cisco Systems, Inc. Estados Unidos de América. 2002. http://www.cisco.com/warp/public/cc/so/neso/vpn/unVPNt/atomf_wp.pdf

[50] ANÓNIMO. “Protocol Registries”. Internet Assigned Numbers Authority (IANA). http://www.iana.org/protocols

[51] ANÓNIMO. “SSH Support Over IPv6”. Cisco Systems, Inc., 23 de julio de 2012. http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_nman/configuration/15-2mt/ip6-ssh.pdf

[52] ANÓNIMO. “Configuring IPv6 ACL”. Catalyst 3750 Software Configuration Guide, Release 12.2(55)SE. http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_55_se/configuration/guide/swv6acl.html

[53] ANÓNIMO. “Quality of Service on Cisco Catalyst 6500”. Cisco Catalyst 6500 Series Switches. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_white_paper0900aecd803e5269.html

CAPÍTULO 2

SITUACIÓN ACTUAL DEL PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES TELCONET S.A.

2.1. BREVE DESCRIPCIÓN DE LA RED DE TELCONET S.A.

2.1.1. INTRODUCCIÓN[1][22]

Telconet S.A. es una empresa ecuatoriana dedicada a brindar servicios de telecomunicaciones con 16 años de experiencia en el mercado nacional. Ofrece servicios de Internet, transmisión de voz, datos y vídeo, las 24 horas los 365 días del año. La matriz está ubicada en la ciudad de Guayaquil[19], con sucursales en cada una de las provincias y cobertura en más de 110 ciudades a nivel nacional, incluidas las Islas Galápagos.

Telconet S.A. pone a disposición de sus clientes el Centro de Operaciones y Monitoreo (NOC) para brindar soporte técnico las 24 horas del día. Además, se establecen Acuerdos de Nivel de Servicio (SLA) entre el proveedor y sus clientes, con el objetivo de definir por escrito los parámetros contratados y el servicio técnico ofrecido.

Telconet S.A. se enfoca en brindar servicios y cubrir los requerimientos de los clientes corporativos dentro del territorio nacional; es por ello, que la mayoría de universidades, bancos y empresas nacionales confían en Telconet S.A. por su compromiso y seriedad al ofrecer servicios de calidad, pronta respuesta a inconvenientes, una infraestructura de red propia y alta capacidad de crecimiento en nuevas tecnologías.

Telconet S.A. ha visto la necesidad de rediseñar su infraestructura de red, frente a la demanda de servicios en IPv6 por parte de sus clientes y a la implementación

[19] Las oficinas en Guayaquil están ubicadas en el parque Empresarial Colón. Edificio Coloncorp, primer piso.

de nuevas aplicaciones como el *Data Center* que incrementan significativamente el tráfico en la red, a fin de brindar servicios de calidad, lograr alta confiabilidad en los clientes y ser más competitivo en el mercado.

El presente proyecto tiene como objetivo rediseñar la red MPLS de Telconet S.A. para que tenga soporte para IPv6 y brinde las Mejores Prácticas de Seguridad en la ciudad de Quito[20], por lo que se realizará una breve descripción de la situación actual del *backbone* y se determinarán los requerimientos de tráfico para los cinco años posteriores.

Para fines exclusivos del presente proyecto, se obtuvo la información expuesta a continuación del departamento de *Networking* de Telconet S.A.; por motivos de seguridad y políticas de la empresa no se presentará el detalle de la misma.

2.1.2. SITUACIÓN ACTUAL DEL *BACKBONE* DE TELCONET S.A.[2][3][23]

Telconet S.A. se encuentra en el proceso de transición de su infraestructura de red a la tecnología MPLS/IPv4. En la sucursal de Quito, el 100% de los clientes que contrataron el servicio de transmisión de datos y apenas el 10% de los que contrataron Internet, trabajan con MPLS. El restante 90% trabaja solo con la tecnología *Ethernet.*

El *backbone* de Telconet S.A. está diseñado en base al modelo jerárquico de tres capas: núcleo, distribución y acceso, con dispositivos de red marca Cisco y enlaces de fibra óptica. Su topología física tiene forma de estrella en el núcleo con velocidades que van de 1 a 10 Gbps; y forma de anillo en las capas: distribución y acceso, con velocidades desde 1 Mbps hasta 1 Gbps.

La matriz Guayaquil es la puerta de salida de la red hacia los proveedores internacionales, por lo que tiene conexiones con el resto de nodos a nivel nacional. Para tener una mejor administración de la red, los nodos ubicados en el

[20] Las oficinas de la sucursal Quito se encuentran, desde los primeros días del año 2012, en la Av. 12 de Octubre N24-660 y Francisco Salazar. Edificio Concorde, pisos 1 y 2.

norte del país y especialmente los de la sierra, se conectan a la sucursal Quito para salir hacia Guayaquil, a través del enlace de alta velocidad GYE-UIO que atraviesa el país.

Quito es la sucursal más grande y robusta de Telconet S.A. después de la matriz. Tiene a cargo la administración, el monitoreo y el mantenimiento de los nodos de las ciudades de la Sierra más cercanas, como: Riobamba, Ambato, Santo Domingo de los Tsáchilas, Guaranda, Ibarra, Otavalo, entre otras; muchas de la Costa norte del país como: Esmeraldas; y muchas del Oriente como: Lago Agrio, Puyo, Tena, Lumbaqui y El Coca.

Actualmente, Condijua, El Coca y otros nodos lejanos del oriente utilizan radio enlaces para conectarse a la Sucursal Quito debido a las condiciones geográficas propias del Oriente, pero pronto serán reemplazados por fibra óptica según se incremente la acogida de los servicios de Telconet S.A. en estos sectores del país.

Guayaquil administra los nodos de la Costa, la región Insular y el sur del país, como las ciudades de: Machala, Salinas Huaquillas, Manta, Cuenca, Loja, Catamayo y las Islas Galápagos, entre otras.

El enlace GYE-UIO es un anillo robusto de fibra óptica monomodo con tecnología *Ethernet* sobre DWDM[21], que conecta el país desde Quito hacia Guayaquil a una capacidad de 10 Gbps con balanceo de carga y redundancia automática. Atraviesa las ciudades de: Tandapi y Santo Domingo por el oeste; y Cuenca y Ambato por el este.

En la Figura 2.1 se detalla la interconexión de la red de Telconet S.A. de los principales nodos a nivel nacional.

[21] La Multiplexación por División en Longitudes de Onda Densas (DWDM) es un mecanismo que permite transmitir varias señales en distintas longitudes de onda a través de una única fibra óptica. Trabaja en la banda de frecuencia C (de 4 a 8 Gbps) en la tercera ventana: 1550nm.

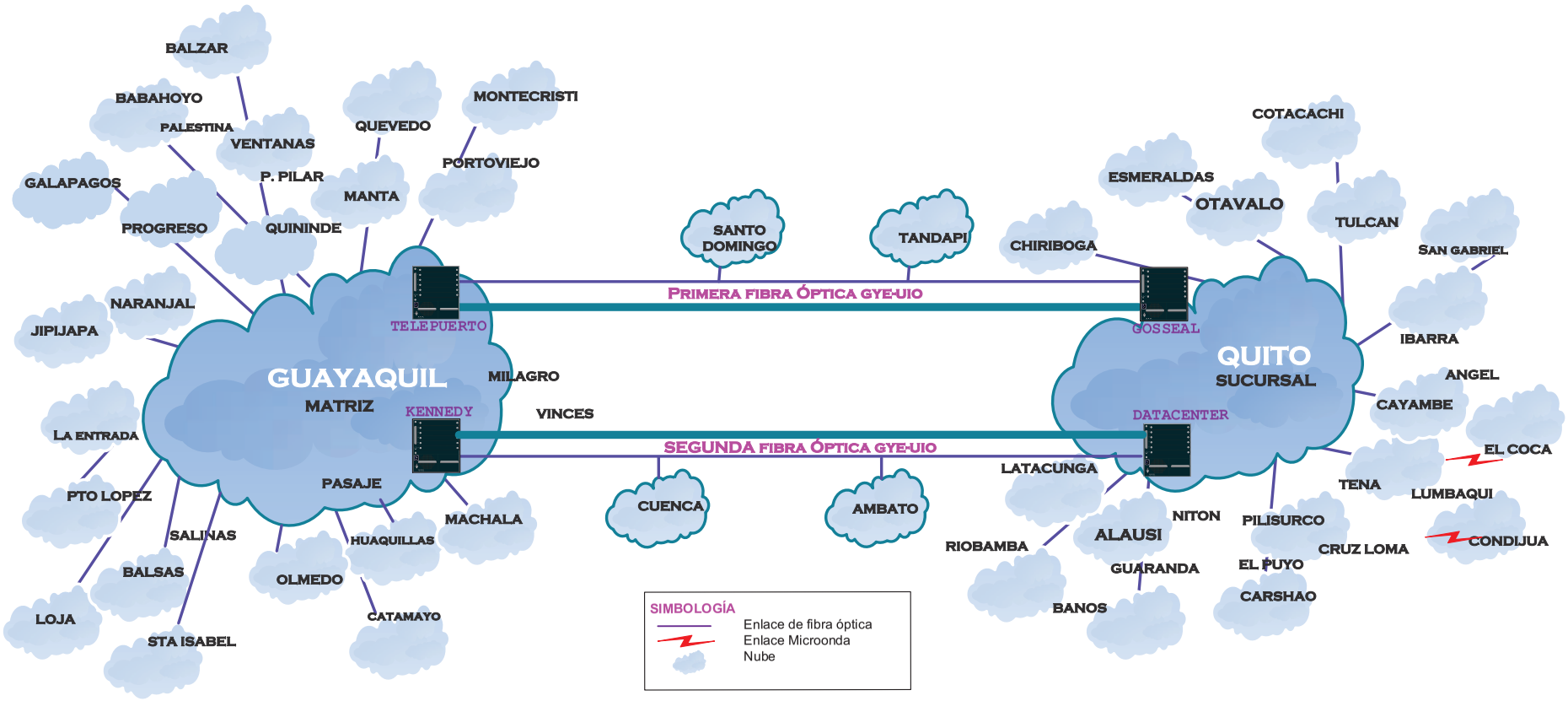


Figura 2.1 Interconexión nacional de la red de Telconet S.A.

Fuente: [2]

2.1.2.1. Interconexión del *backbone* hacia las Salidas Internacionales[14]

El principal proveedor internacional de Telconet S.A. es TIWS mediante los cables submarinos: SAM-1 y PANAM. Para garantizar la disponibilidad de la red, se tienen salidas internacionales redundantes con otros proveedores, como: SPRINT, TINET y Transnexa.

Las salidas internacionales de Telconet S.A. se ubican en el nodo Telepuerto de la ciudad de Salinas, a excepción de Transnexa que se encuentra en la sucursal de Quito. En la Tabla 2.1, se detallan las capacidades contratadas con cada proveedor internacional con un total de 8,266 Gbps.

CABLE SUBMARINO	PROVEEDOR	CAPACIDAD
SAM-1	TIWS	1STM-16
SAM-1	TIWS	3STM-1
PANAM	SPRINT	1STM-16
SAM-1	TINET	1STM-4
PANAM	TIWS	7STM-1
PANAM	TIWS	7STM-1
ARCOS-1	Transnexa	24Mbps
	TOTAL	8,266 Gbps

Tabla 2.1 Proveedores internacionales de Telconet S.A.
Fuente: [14]

2.1.2.2. Descripción de los componentes de la red de Quito de Telconet S.A.[2][3]

Telconet S.A. adoptó implementar su red MPLS/IPv4 según el modelo jerárquico de tres capas: núcleo, distribución y acceso, a fin de garantizar la escalabilidad y facilitar la administración de sus componentes ya que presenta funciones y características específicas en cada una de ellas.

En las secciones 2.1.2.2.1, 2.1.2.2.3 y 2.1.2.2.4, se detalla el hardware y el software que dispone la red de la ciudad de Quito, según la capa del modelo jerárquico al que pertenecen.

2.1.2.2.1. Componentes de la capa núcleo[6][9][10][12][24][32][33]

La capa núcleo es el *backbone* de la red y la capa más importante del modelo. Está formada por los equipos más robustos de la sucursal ya que soportan el tráfico proveniente de las capas: distribución y acceso. La redundancia en esta parte de la red es vital, ya que una falla en estos equipos afectaría seriamente el desempeño de la red.

La sucursal de Quito de Telconet S.A. dispone de dos equipos redundantes en calidad de LSR de la red MPLS y seis en calidad de LER. Los LSR son dispositivos marca Cisco y modelo WS-C6509-E que soportan la tecnología MPLS. Se interconectan entre sí y a la matriz Guayaquil con los P: Telepuerto y Kennedy, como se indica en la Figura 2.2.

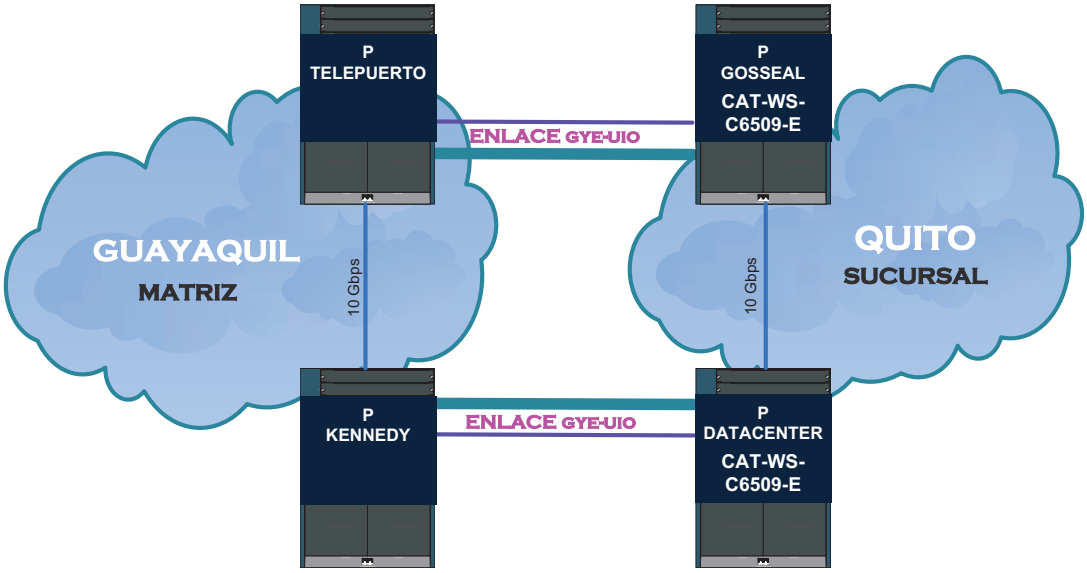


Figura 2.2 Equipos P de la capa núcleo

Fuente: [3]

Los LSR de la red MPLS/IPv4 de Telconet S.A se denominan[22]: PGOSSEAL y PDATACENTER. Se interconectan entre sí mediante enlaces de 10 Gbps para

[22] Por motivos de confidencialidad, los nombres de los dispositivos de red y las direcciones IP mostradas en este proyecto han sido cambiados.

garantizar redundancia en esta parte de la red, y manejan enlaces de 1 y 10 Gbps con los LER.

En la Tabla 2.2 se detallan las características técnicas de los equipos LSR: PGOSSEAL y PDATACENTER.

CARACTERÍSTICAS TÉCNICAS		
Descripción	**PGOSSEAL**	**PDATACENTER**
Marca	Cisco	Cisco
Modelo	CAT-WS-C6509-E	CAT-WS-C6509-E
Versión IOS	12.2(33)SXI6	12.2(33)SXI6
Memoria no volátil NVRAM	1.917K bytes	1.917K bytes
Memoria del búfer de paquetes	8.192K bytes	8.192K bytes
Memoria *flash*	65.536K bytes	65.536K bytes

Tabla 2.2 Características técnicas de los P

Los módulos de las interfaces de los routers LSR de la red se detallan en la Tabla 2.3.

MÓDULOS DE INTERFACES		
DESCRIPCIÓN	**PGOSSEAL**	**PDATACENTER**
Número de ranuras	9	9
Performance	400Mpps/720Gbps	400Mpps/720Gbps
Interfaces *Ten Gigabit Ethernet*	12	8
Interfaces *Gigabit Ethernet*	46	28
Interfaces *Virtual* Ethernet	1/255	1/255

Tabla 2.3 Módulos de las interfaces de los P

En la capa núcleo, también se encuentran los LER. Estos equipos son routers marca Cisco de la serie 7000 que manejan dos tecnologías: MPLS, en las interfaces conectadas a los LSR; y *Ethernet,* en las interfaces conectadas con los dispositivos de la capa distribución.

En la red de Telconet S.A. se tienen 6 equipos LER denominados:

- PE1GOSSEAL
- PE1DATACENTER
- PE1SUR2
- PE1ARMENIA
- PE1BORROMONI
- PE1MUROS

Como se puede observar en la Figura 2.3, los equipos LER pertenecen a la serie 7000 y presentan redundancia de enlaces hacia los LSR. En caso de que uno de los dos LSR falle, los LER tendrán una ruta alternativa para comunicarse con otro punto de la red.

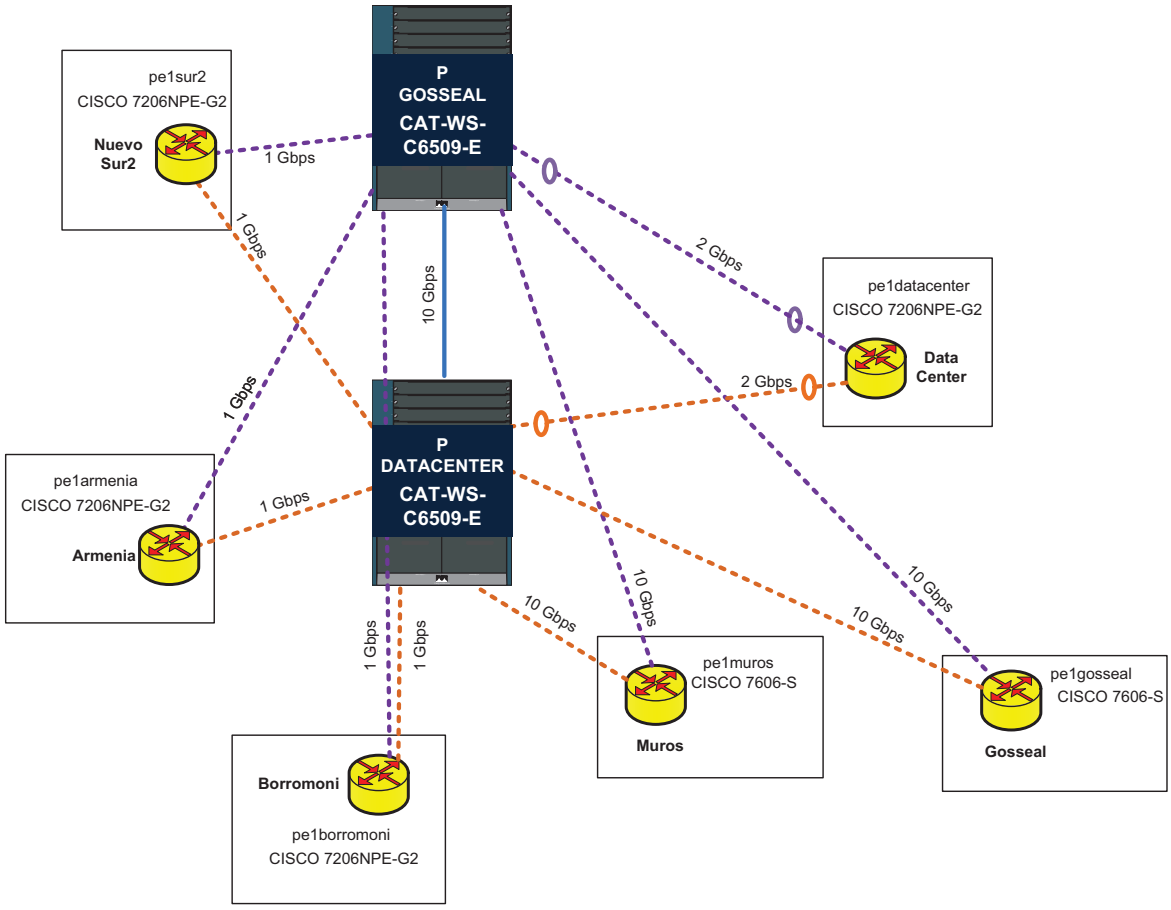


Figura 2.3 Equipos PE de la capa núcleo

Fuente: [3]

En la Tabla 2.4 se resumen las características técnicas de los LER.

CARACTERÍSTICAS TÉCNICAS			
DESCRIPCIÓN	**PE1SUR2 PE1DATACENTER**	**PE1ARMENIA PE1BORROMONI**	**PE1GOSSEAL PE1MUROS**
Marca	Cisco	Cisco	Cisco
Modelo	7206VXR (NPE-G2)	7206VXR (NPE-G2)	7609-S
Versión IOS	15.0(1)M7	12.2(33)SRD5	15.0(1)S4
Memoria no volátil NVRAM	2.045K bytes	2.045K bytes	3.964K bytes
Memoria Interna ATA PCMCIA card	255.744K bytes	255.744K bytes	507.024K bytes
Memoria *flash*	65.536K bytes	65.536K bytes	131.072K bytes

Tabla 2.4 Características técnicas de los PE

Los módulos de las interfaces de los LER se detallan en la Tabla 2.3.

MÓDULOS DE INTERFACES				
DESCRIPCIÓN	**PE1SUR2 PE1ARMENIA PE1BORROMONI**	**PE1DATACENTER**	**PE1GOSSEAL**	**PE1MUROS**
Número de ranuras	6	6	9	9
Performance	2Mpps/1024Mbps	2Mpps/1024Mbps	400Mpps/720Gbps	400Mpps/720Gbps
Interfaces *Ten Gigabit Ethernet*	-	-	8	8
Interfaces *Gigabit Ethernet*	3	6	4	4
Interfaces *Virtual Ethernet*	-	-	167/255	142/255

Tabla 2.5 Módulos de las interfaces de los PE

2.1.2.2.2. Componentes de la capa distribución[2][3][10][25]

La capa distribución es la capa intermedia de la red. Tiene la función de reenviar todo el tráfico proveniente de la capa de acceso hacia la capa núcleo, y viceversa. Aquí se aplican políticas de acceso, VLAN y es de suma importancia brindar rápida respuesta a los requerimientos de tráfico.

Esta capa está compuesta por equipos denominados agregadores; aunque por las funciones de distribución, los PE también pueden pertenecer a ella. Sin embargo, para el presente proyecto se los incluyó solo en la capa núcleo por facilidad de estudio.

Los agregadores son switches Cisco que se conectan a cada LER con el objetivo de conmutar el tráfico proveniente de la capa de acceso. Por motivos de redundancia, se tienen dos agregadores por cada PE ubicados en los terminales de los anillos de la capa de acceso. Según la capacidad del LER al que se conectan, estos dispositivos pueden tener interfaces de 1 o 10 Gbps hacia el PE y su agregador de respaldo. Además, tienen enlaces de 1 Gbps con los equipos de la capa de acceso.

La sucursal de Quito de Telconet S.A. dispone de 12 switches agregadores, y son:

Para PE1GOSSEAL
- SW1AGGOSSEAL
- SW2AGGOSSEAL

Para PE1ARMENIA
- SW1AGARMENIA
- SW2AGARMENIA

Para PE1DATACENTER
- SW1AGDATACENTER
- SW2AGDATACENTER

Para PE1BORROMONI
- SW1AGBORROMONI
- SW2AGBORROMONI

Para PE1SUR2
- SW1AGSUR2
- SW2AGSUR2

Para PE1MUROS
- SW1AGMUROS
- SW2AGMUROS

En la Figura 2.4 se detallan los dispositivos de las capas núcleo y distribución, con los modelos y las capacidades de los enlaces que manejan en la red en dirección al núcleo.

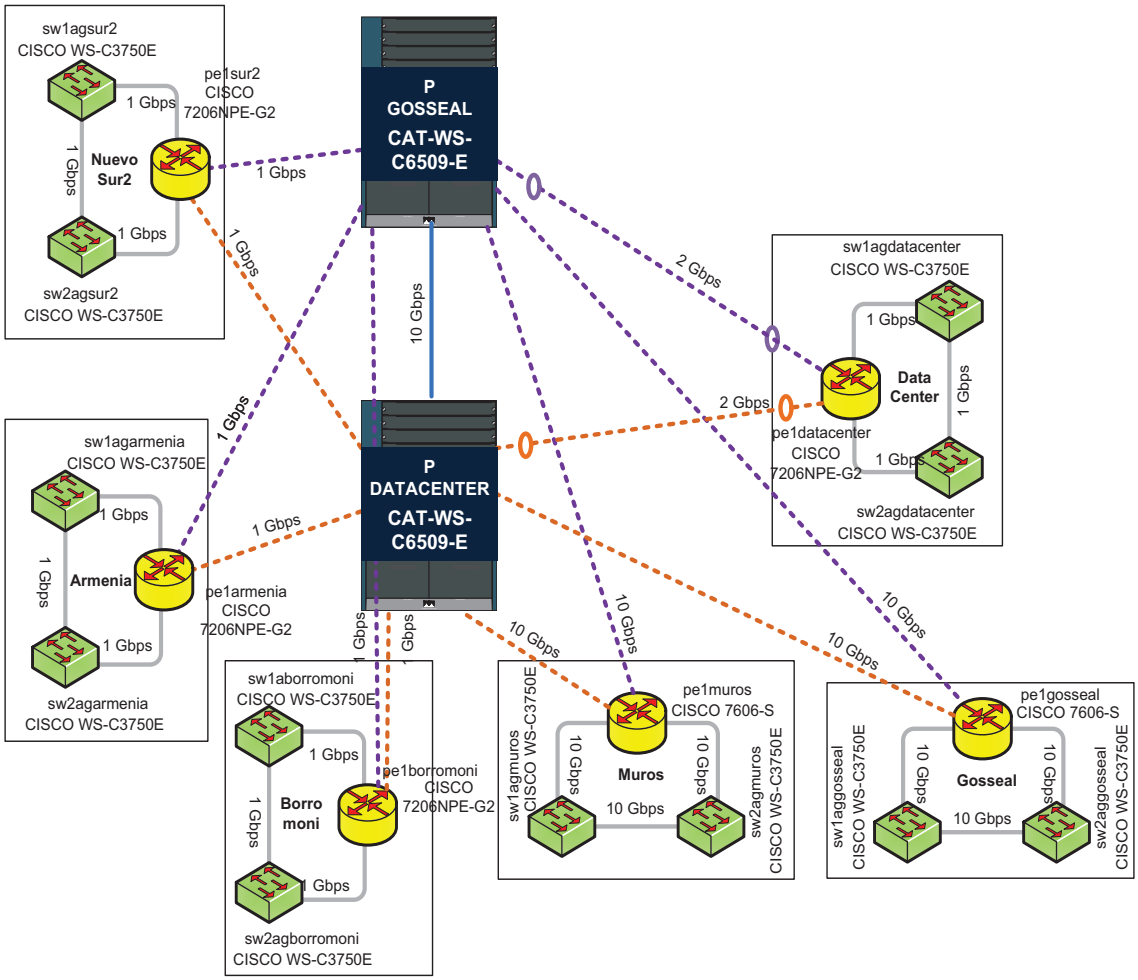


Figura 2.4 Equipos de las capas: núcleo y distribución

Fuente: [3]

En la Tabla 2.6 se detallan las características técnicas de los switches agregadores.

CARACTERÍSTICAS TÉCNICAS	
DESCRIPCIÓN	**AGREGADORES**
Marca	Cisco
Modelo	WS-C3750E-24TD-S
Versión IOS	12.2(50)SE
Memoria no volátil NVRAM	512K bytes

Tabla 2.6 Características técnicas de los agregadores

En la Tabla 2.7 se detallan los módulos de las interfaces de los agregadores.

MÓDULOS DE INTERFACES	
DESCRIPCIÓN	**AGREGADORES**
Performance	38.7Mpps/32Gbps
Interfaces *Ten Gigabit Ethernet*	2
Interfaces *Gigabit Ethernet*	28
Interfaces *Fast Ethernet*	1
Interfaces *Virtual Ethernet*	1/255

Tabla 2.7 Módulos de las interfaces de los agregadores

2.1.2.2.3. Componentes de la capa acceso[2][3][10][26]

La capa acceso es la más cercana al usuario y sirve para conectar los equipos de los clientes con la red de Telconet S.A. En esta capa se tiene una topología física en anillo, donde cada anillo se conecta a un LER mediante dos agregadores redundantes. Si un equipo o enlace del anillo falla, el resto de dispositivos seguirán funcionando porque tienen un camino adicional para conectarse con el LER; pero si falla el LER, todos los pétalos de ese nodo se verán afectados mientras el resto de la red seguirá funcionando sin inconvenientes.

Para aumentar la disponibilidad de la red y garantizar redundancia sin lazos en capa 2, se configuran diferentes instancias, una en cada anillo, del protocolo *Multi-Spanning Tree* (MSTP)[23]. En esta capa se tienen dispositivos marca Cisco y modelo WS-C3550 de 24 y 48 puertos, con velocidades en sus enlaces de hasta 1 Gbps.

En la Figura 2.5 se detalla la red actual de la sucursal de Quito del proveedor Telconet S.A. con un total de 106 nodos de acceso.

[23] Para mayor información del protocolo MSTP se recomienda revisar [5].

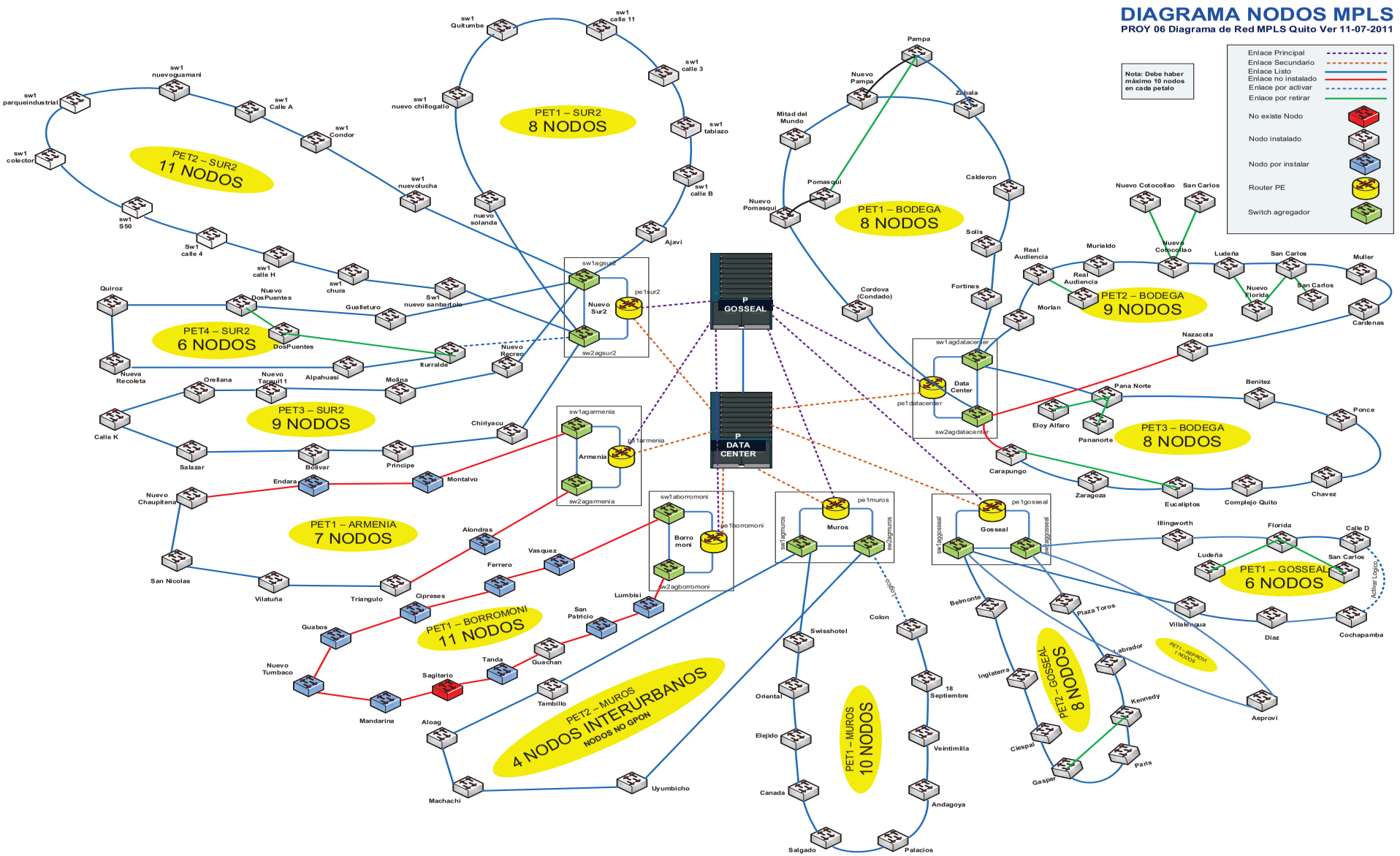


Figura 2.5 Dispositivos de la red de la sucursal Quito de Telconet S.A.

Fuente: [3]

En la Tabla 2.8 se detallan las características técnicas de los dispositivos de la capa de acceso.

CARACTERÍSTICAS TÉCNICAS			
DESCRIPCIÓN	**SWITCHES DE ACCESO**		**AEPROVI**
Marca	Cisco	Cisco	Cisco
Modelo	WS-C3550-24	WS-C3550-48	WS-C4900M
Versión IOS	12.2(25)SEB4	12.2(25)SEB4	12.2(53)SG1
Memoria no volátil NVRAM	348K bytes	384K bytes	511K bytes

Tabla 2.8 Características técnicas de los switches de acceso

En la Tabla 2.9 se detallan los módulos de las interfaces de los switches de la capa acceso.

MÓDULOS DE INTERFACES			
DESCRIPCIÓN	**SWITCHES DE ACCESO**		**AEPROVI**
Número de ranuras	-	-	3
Performance	6.6Mpps/8.8 Gbps	10.1Mpps/13.6 Gbps	11Mpps/22 Gbps
Interfaces 10 *Gigabit Ethernet*	-	-	24
Interfaces *Gigabit Ethernet*	2	2	32
Interfaces *Fast Ethernet*	24	48	-

Tabla 2.9 Módulos de las interfaces de los switches de acceso

En el ANEXO A se presentan: los nombres, los modelos y el número de los dispositivos de cada nodo de la sucursal de Quito del proveedor Telconet S.A.

2.1.2.3. Componentes de los nodos[7][8]

Los nodos de la red de Telconet S.A. están ubicados estratégicamente alrededor de la ciudad de Quito y disponen de una serie de elementos adicionales que permiten el funcionamiento adecuado de los dispositivos.

Los componentes de los nodos más representativos son:

- Sistema de Alimentación Ininterrumpida (UPS)
- Banco de baterías
- Aires acondicionados
- *Racks*

Sistema de Alimentación Ininterrumpida (UPS)[19]

Un UPS es un equipo de seguridad que frente a una emergencia eléctrica, proporciona energía a los dispositivos de red evitando que se apaguen. Todos los nodos cuentan con uno o más UPS dependiendo de la cantidad de dispositivos que tengan a su cargo.

Los UPS disponen de bancos de baterías para proporcionar energía por un periodo determinado de tiempo. Por ejemplo, en la Figura 2.6 se puede ver un UPS marca APC 10kVA[27].

Figura 2.6 APC *Smart*-UPS

Bancos de baterías[19]

Son un conjunto de baterías en serie que permiten aumentar la intensidad de corriente. Se utilizan en lugares donde se frecuentan cortes energéticos, o donde se necesita garantizar la disponibilidad de los equipos evitando que se apaguen.

En la Figura 2.7 se puede ver el banco de baterías del nodo Gosseal.

Figura 2.7 Banco de baterías del nodo Gosseal

Aires acondicionados[19]

Son sistemas de acondicionamiento de la temperatura y la humedad de un espacio físico. Se utilizan en los grandes nodos para evitar que los dispositivos de red se sobrecalienten y dejen de funcionar. En la Figura 2.8 se indica el sistema de enfriamiento del nodo Gosseal.

Figura 2.8 Aire acondicionado del nodo Gosseal

***Racks*[19]**

Los *racks* son estructuras metálicas utilizadas para alojar los dispositivos de red y equipos electrónicos en general. Tienen medidas de ancho normalizadas (19 pulgadas) mientras la altura se ajusta a las necesidades de la empresa.

En la Figura 2.9 se muestra un *rack* del nodo Gosseal.

Figura 2.9 *Racks* de Gosseal

2.1.2.4. Descripción de la fibra óptica de Telconet S.A.[4][7][8][9]

La fibra óptica ha permitido dar grandes saltos en las telecomunicaciones motivo por el cual, los ISP a nivel nacional han empezado a adaptarla. Telconet S.A. utiliza en su red, fibra óptima monomodo y multimodo tendida en los postes de alumbrado público de las principales ciudades del país. Para la sucursal de Quito, se arriendan los postes a la Empresa Eléctrica Quito (EEQ), mientras en los sectores que tenga soterramiento de cables, se solicita el permiso al Municipio del Distrito Metropolitano de Quito.

Telconet S.A. tiene en su infraestructura fibra óptica de: 2, 12, 48, 96 y 144 hilos alrededor de toda su red, distribuida según su ubicación en: fibra óptica urbana y fibra óptica interurbana.

Fibra Óptica Urbana[8]

Este tipo de fibra óptica es tendida en el sector urbano de las ciudades del país. Tiene en su interior dos cables de acero de 1,5 milímetros de espesor para brindar mayor resistencia al ser fijada en los postes de alumbrado público.

Fibra Óptica Interurbana[8]

Este tipo de fibra óptica tiene una guía metálica en su interior para brindar rigidez durante el tendido y alcanzar mayores distancias entre los postes. En la actualidad, Telconet S.A. está migrando su infraestructura a fibra óptica de 144 hilos en el sector urbano y de 96 hilos en el sector interurbano, frente al incremento de clientes en las principales ciudades y a las regulaciones municipales de ubicar el menor número de cables en los postes.

La fibra óptica de 12 y 48 hilos está siendo desplazada a ciudades donde el número de clientes no es muy grande. Mientras, la fibra óptica de 2 hilos se utiliza en la acometida de los clientes, un hilo para la conexión al *backbone* de Telconet S.A. y el otro, hacia la red del cliente.

La fibra óptica viene en bobinas de 2 y 4 Km de longitud. En la Figura 2.10 se indica una bobina de fibra óptica de 2 Km.

Figura 2.10 Bobina de FO

2.1.3. TIPOS DE CLIENTES DE TELCONET S.A.[1]

A nivel general, un ISP clasifica sus clientes en: corporativos y residenciales. Telconet S.A. se orienta a brindar servicios a empresas corporativas antes que al sector residencial, por lo que tiene dos tipos de clientes:

- Clientes corporativos VIP
- Clientes corporativos

2.1.3.1. Clientes corporativos VIP

Un cliente corporativo VIP es aquel que al contratar uno o más servicios con Telconet S.A., factura montos superiores a 5.000 dólares. No tiene tratos preferenciales en la red porque no se tiene implementada Calidad de Servicio ni Ingeniería de Tráfico, pero si distinciones a nivel del soporte técnico.

Telconet S.A. asigna un ingeniero a cada cliente corporativo VIP, con el fin de que este resuelva las dudas, sea el responsable de informar al cliente la existencia de un problema y lo mantenga informado hasta que se resuelva el mismo. El cliente corporativo VIP no tiene que llamar al departamento de soporte NOC y esperar que alguien del personal lo atienda, porque dispone del teléfono móvil del ingeniero asignado.

2.1.3.2. Clientes corporativos

Los clientes corporativos son todos los clientes de Telconet S.A. que no pertenecen a la clase VIP. Tienen el mismo trato en la red que los clientes corporativos VIP pero a diferencia de ellos, no tienen soporte personalizado.

2.1.4. DESCRIPCIÓN DE LOS ACUERDOS DE NIVEL DE SERVICIOS (SLA) DE TELCONET S.A.[11]

Telconet S.A. ofrece una disponibilidad comprometida mensual mínima de 99,6% para el servicio de transmisión de datos y 99,9% para Internet. La disponibilidad

se calcula restando el tiempo total fuera de servicio (TFS) del tiempo total (TS) en un mes transcurrido y dividiendo para el tiempo TS, como se indica en la Ecuación 2.1.

$$\text{Disponibilidad} = \frac{TS - TFS}{TS}$$

Ecuación 2.1 Disponibilidad de Telconet S.A.

El tiempo total fuera de servicio (TFS) se considera la suma de todos los tiempos en los cuales el cliente se ha quedado sin servicio y ha informado al departamento NOC[24] con la apertura de un *trouble ticket.* El TFS es contabilizado hasta que el personal de soporte devuelve la llamada al cliente, notifica que el problema ha sido superado y cierra el *trouble ticket*.

Las consideraciones para el TFS son solo fallas de la red de Telconet S.A. No se incluyen las horas de mantenimiento porque serán oportunamente anticipadas al cliente con 48 horas y realizadas durante las 4 horas posteriores a la media noche. Telconet S.A. no se responsabiliza por servicios tercerizados ni problemas causados en los equipos bajo el dominio del cliente.

Además, se especifican porcentajes detallados en la Tabla 2.10 que disminuyen el monto de la factura del cliente. Las notas de crédito son notificaciones escritas que se establecen cuando el proveedor no ha cumplido con la disponibilidad mínima garantizada.

Por ejemplo, si un cliente se ha quedado sin servicio durante 20 horas en un mes de 30 días, tendrá el 5% descuento en su factura porque recibió una disponibilidad del 97,2%, inferior a la disponibilidad comprometida por Telconet S.A. de 99,6%.

[24] El departamento NOC de la ciudad de Quito atiende las llamadas de sus clientes las 24 horas del día al: +593 2 3963100 ext 254 y responde al correo: noc@telconet.ec

CRÉDITOS MENSUALES DE TELCONET S.A.		
DISPONIBILIDAD	**HORAS FUERA DE SERVICIO[25]**	**CRÉDITO MENSUAL**
100% a 99,60%	0 h a 2,88 h	0
99,60% a 98,00 %	2,88 h. a 14,4 h	2%
98,00 % a 95,00%	14,4 h a 36,0 h	5%
95,00% a 90,00%	36,0 h a 72,0 h	10%
90,00% a 80,00%	36,0 h a 144,0 h	20%
Menos del 80,00%	Más de 144,0 h	50%

Tabla 2.10 Crédito Mensual de Telconet S.A.

Fuente: [11]

Un cliente pueda dar por terminado el contrato si se llega a presentar uno de los tres puntos indicados a continuación:

- Más de 15 horas de interrupción total del servicio durante un mes.
- Más de 45 horas de interrupción total del servicio en un período de 3 meses consecutivos.
- Interrupción continua superior a 72 horas consecutivas.

2.1.5. PROTOCOLOS UTILIZADOS EN LA RED DE TELCONET S.A.[6][7]

Los protocolos que se manejan en el *backbone* de Telconet S.A. son:

- Para brindar redundancia de capa 2 en la red, se dispone del protocolo *Multi-Spanning Tree* (MSTP), el cual ofrece un enlace activo y la posibilidad de levantar automáticamente otro en caso de fallos, brindando un camino alterno a los paquetes durante la conmutación.
- Para el enrutamiento dinámico de la red, Telconet S.A. utiliza el protocolo estado de enlace OSPF, el cual brinda alta convergencia al enviar actualizaciones por eventos y recrear la topología de la red en cada dispositivo.

[25] Se basan en un mes de 30 días, 720 horas.

- En la red MPLS, se utiliza el protocolo LDP para la distribución de la información de las etiquetas y generar los LSP.
- Se emplea el protocolo BGP versión 4 para establecer sesiones e intercambiar información de enrutamiento entre el proveedor y los sistemas autónomos de los clientes.
- El protocolo VLAN *Trunking Protocol* (VTP) se utiliza para distribuir la información de las VLAN durante la configuración de los switches.
- Se utilizan los protocolos: *telnet* y SSH para la administración remota de los dispositivos de red, siendo SSH el más utilizado al ofrecer encriptación en los datos.
- Para la administración y gestión de la red, se utiliza la versión 2c del protocolo *Simple Network Management Protocol* (SNMPv2c).

2.2. DIMENSIONAMIENTO DE TRÁFICO DE TELCONET S.A.

El tráfico que circula por la red de Telconet S.A. en la ciudad de Quito será dimensionado mediante la estimación de uso de las aplicaciones, las capacidades contratadas por los clientes y la proyección del crecimiento de la red. El objetivo de este dimensionamiento se centra en obtener los requerimientos necesarios para poder rediseñar la red MPLS de Telconet S.A. con soporte a IPv6.

Los requerimientos se obtendrán en base a los servicios que brinda la empresa actualmente y aquellos que se ofrecerán en los próximos meses. Se analizarán las capacidades que tienen contratadas los clientes de la ciudad de Quito y el crecimiento esperado.

Los servicios que ofrece Telconet S.A. en la actualidad son:

- Internet dedicado 1:1 y tránsito al *backbone* de Internet
- Internet 2
- Transmisión de datos y canal de vídeo
- IP PBX gestionado

En la Tabla 2.11 se muestran: el número de clientes registrados y las velocidades de subida y bajada contratadas por cada servicio ofertado por Telconet S.A. entre el 31 de marzo de 2011 al 31 de marzo de 2012.

SERVICIO OFERTADOS	NÚMERO DE CLIENTES	VELOCIDADES DE SUBIDA (Mbps)	VELOCIDADES DE BAJADA (Mbps)
Internet dedicado 1:1 y tránsito al backbone de Internet	721	2.763,84	2.763,84
Internet 2	1	5,120	5,120
Transmisión de datos y canal de vídeo	1.615	5.486,020	5.486,020
IP PBX Gestionado	3	11,264	11,264
TOTAL	**2.340**	**8.266,239**	**8.266,239**

Tabla 2.11 Número de clientes actuales y velocidades contratadas por servicio

Fuente: [17]

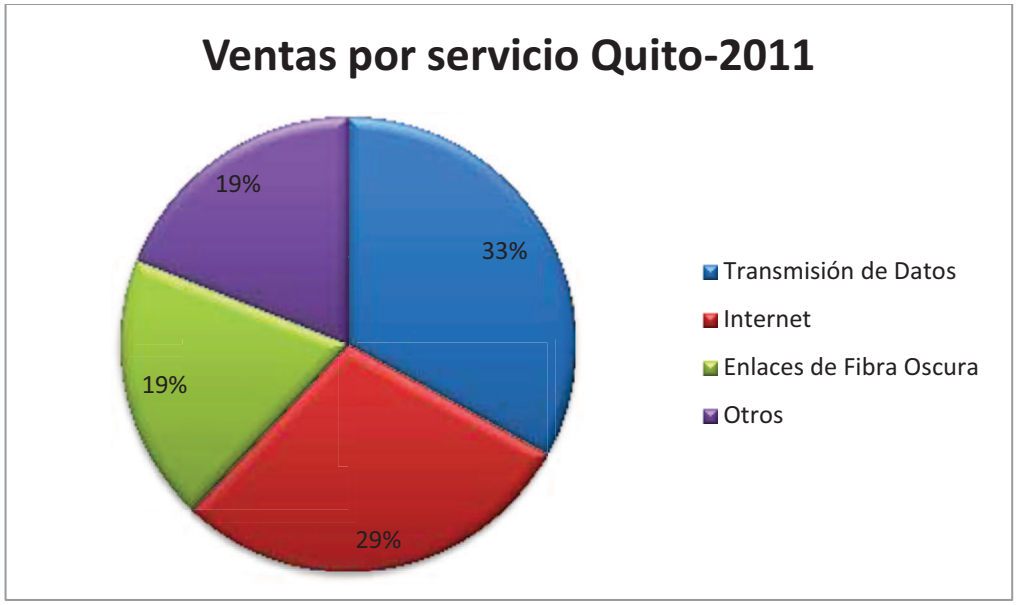


Figura 2.11 Ventas por producto Quito-2011

Fuente: [1]

Aunque los servicios de mayor acogida en la sucursal de Quito son: Internet dedicado 1:1 y trasmisión de datos. Por ejemplo, en el año 2011 las ventas fueron de: 33% de transmisión de datos, 29% de Internet, 19% de enlaces de fibra oscura[26] y 19% de otros servicios, como se indica en la Figura 2.11.

Telconet S.A. espera integrar nuevas aplicaciones como:

- *Virtual Data Centers*
- *E-billing*
- Videoconferencia en *High Definition* (HD) y Web
- Seguridad perimetral gestionada y consultorías de seguridad
- Comunicaciones unificadas

Las aplicaciones internas de la empresa no serán consideradas como los requerimientos en el presente diseño, porque se pretende orientar el proyecto a la parte WAN mas no a la restructuración del área local.

2.2.1. NÚMERO DE CLIENTES

Para el dimensionamiento de tráfico, el número actual de clientes es la cantidad de usuarios de la ciudad de Quito que tienen contratado uno varios servicios con Telconet S.A. al 31 de marzo de 2012.

La información fue facilitada por el departamento *Internet Access Control* (IAC) de la sucursal de Quito, y obtenida del Sistema Integrado de Telconet (SIT) que contiene el registro actualizado de las capacidades contratadas por cliente y las configuraciones de los dispositivos de red.

En la Tabla 2.12, se muestra el número de los clientes actuales de la sucursal de Quito y las velocidades contratadas en cada uno de los 6 routers LER de la red MPLS.

[26] Los enlaces de fibra oscura son enlaces dedicados demandados por el cliente para interconectar dos puntos determinados. El tráfico no atraviesa la red del ISP ni se registra en el SIT.

NÚMERO DE CLIENTES ACTUALES[27]			
Nodo PE	**Núm. clientes**	**Velocidad de subida (Mbps)**	**Velocidad de bajada (Mbps)**
ARMENIA	100	224,264	224,264
BORROMONI	118	327,488	327,488
DATACENTER	398	1.144,458	1.144,458
GOSSEAL	1.197	4.982,769	4.982,769
MUROS	238	738,520	738,520
SUR 2	289	848,740	848,740
TOTAL	**2.340**	**8.266,239**	**8.266,239**

Tabla 2.12 Número de clientes actuales y velocidades contratadas por PE
Fuente: [17]

En los datos presentados en la Tabla 2.12, se puede notar que el nodo GOSSEAL tiene el mayor número de clientes y por lo tanto, mayores capacidades en las velocidades registradas; seguido por los nodos: DATACENTER y SUR2. Para un mejor análisis se presenta la información en una gráfica de barras en la Figura 2.12.

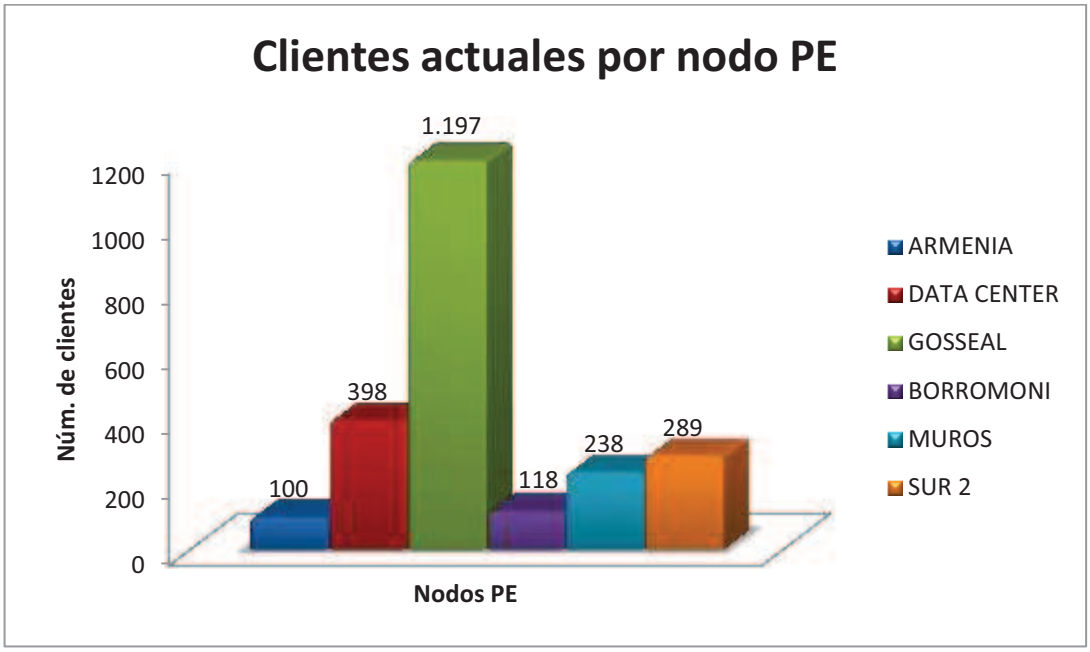


Figura 2.12 Clientes actuales por nodo PE

[27] Datos obtenidos el 31 de marzo del 2012.

2.2.1.1. Porcentaje de crecimiento[17][29][31]

Para determinar el porcentaje de crecimiento de Telconet S.A., se analiza el número de clientes de la ciudad de Quito que contrataron por primera vez los servicios del ISP en los últimos cinco años: desde el 31 de marzo de 2007 hasta el 31 de marzo de 2012.

En la Tabla 2.13 se detalla el número de clientes totales y nuevos de la sucursal de Quito en los últimos 5 años.

NÚMERO DE CLIENTES POR AÑO		
Año	Totales	Nuevos
31 de marzo 2007 - 31 de marzo 2008	411	236
31 de marzo 2008 - 31 de marzo 2009	841	430
31 de marzo 2009 - 31 de marzo 2010	1.356	515
31 de marzo 2010 - 31 de marzo 2011	1.806	450
31 de marzo 2011 - 31 de marzo 2012	2.340	534

Tabla 2.13 Número de clientes 2007-2012
Fuente: [17]

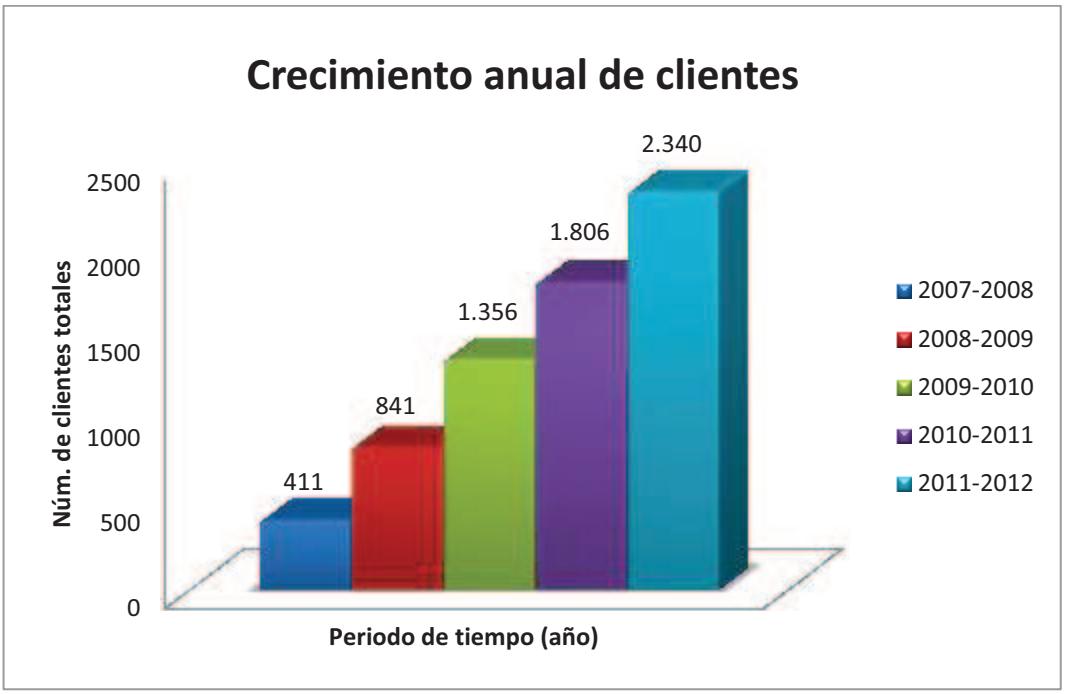


Figura 2.13 Crecimiento anual de clientes de Quito 2007-2012

El crecimiento de los clientes durante los últimos cinco años ha sido positivo, como se puede observar en la Figura 2.13, de 411 clientes registrados en el año 2007-2008 a 2.340 en el 2011-2012.

Para un mejor análisis se presenta el crecimiento de los clientes nuevos en una gráfica de barras en la Figura 2.14. Para los tres primeros años: 2007, 2008 y 2009, este crecimiento ha sido positivo. En el 2010, aunque se tienen nuevos clientes, la cantidad es menor que en el 2009; mientras para el 2011, el crecimiento supera los años anteriores y se estabiliza.

Las razones del incremento reducido en el número de clientes durante el año 2010 son dos: primero, Telconet S.A. no estuvo ofertaron nuevos servicios durante este periodo; y segundo, no tenía tanta cobertura como en el 2011, cuando empezó a migrar su infraestructura de red a fibra óptica, y a la tecnología MPLS en su *backbone.*

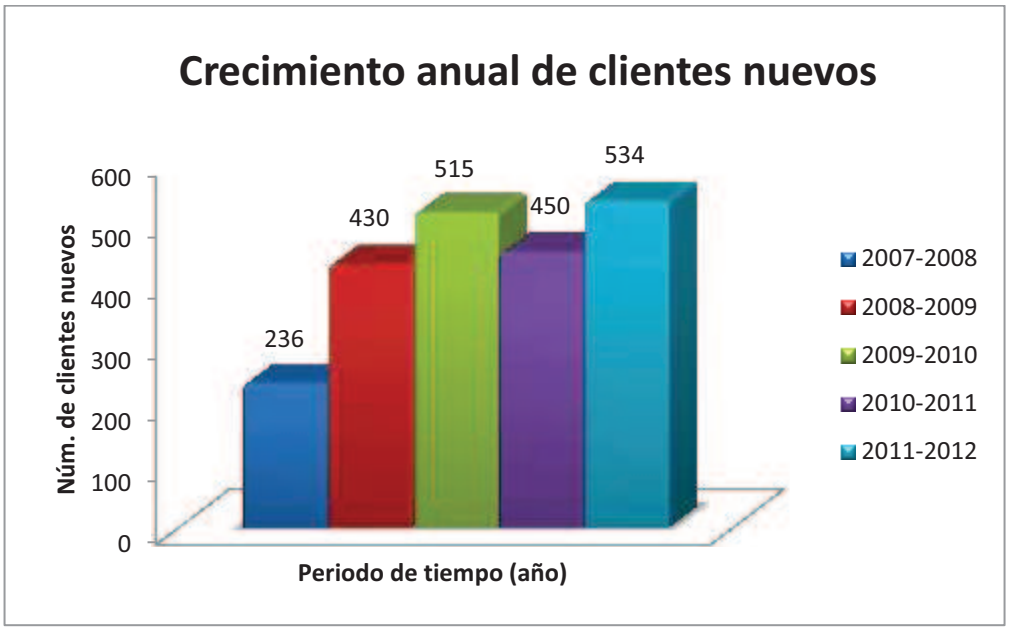


Figura 2.14 Clientes anual de clientes nuevos de Quito 2007-2012

En la Figura 2.15, se obtiene la gráfica de tendencia lineal del crecimiento de los clientes nuevos, con el objetivo de encontrar la dependencia funcional de los puntos y poder extrapolar la información a cinco años.

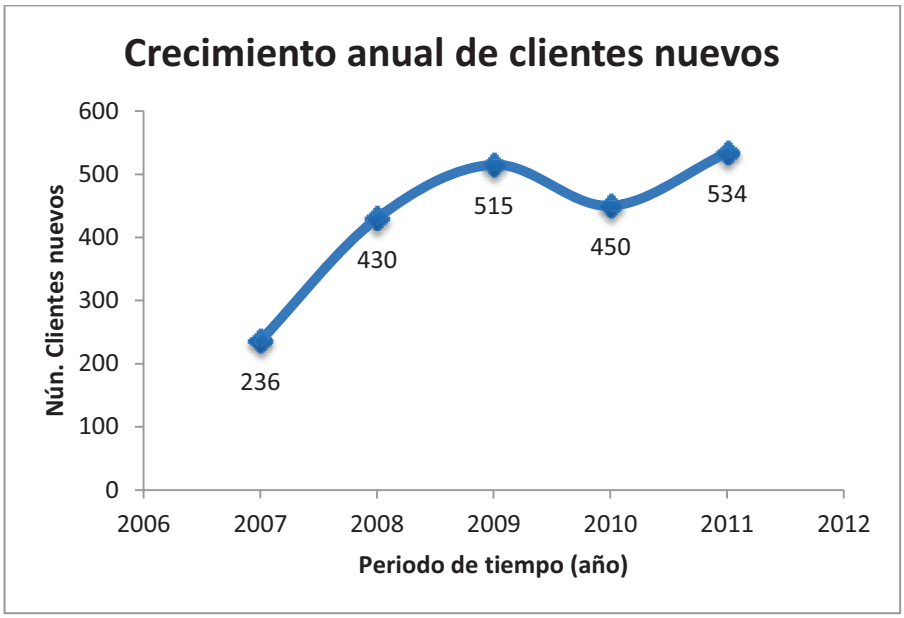


Figura 2.15 Crecimiento de clientes nuevos 2007-2012

Los datos mostrados en la Figura 2.15, no tienen una dependencia funcional perfecta pero se puede realizar una, empleando tres funciones: lineal, cuadrática y logarítmica. Si se aproximan los datos a una función lineal, se espera que el crecimiento de los clientes en los próximos cinco años sea significativo; pero desde el punto de vista corporativo, los clientes nuevos en la ciudad de Quito no serán masivos, sino aquellos que se cambien de proveedor o que contraten las nuevas aplicaciones que ofrece Telconet S.A.; por lo que esta regresión no es viable.

Por el contrario, la regresión cuadrática se acopla perfectamente a los datos analizados pero no es objetiva; porque como toda empresa, Telconet S.A. espera crecer en número de clientes y ventas en los próximos años. La función cuadrática negativa mostrada en la Figura 2.15, indica que en un determinado año el número de clientes alcanzará su valor máximo y empezará a disminuir hasta llegar a cero; por lo cual, este comportamiento no se acopla a los objetivos de Telconet S.A.

La regresión logarítmica es la tendencia más acertada. En los años 2007, 2008 y 2009, el crecimiento del número de clientes ha sido considerable; pero en los últimos tres años se ha mantenido casi constante, lo que refleja un

comportamiento logarítmico. Además, Telconet S.A. espera crecer en ventas facturadas por las nuevas aplicaciones, como el *Data Center*, antes que en número de clientes debido a que todas las empresas de Quito ya se encuentran asociadas a un proveedor.

2.2.1.2. Regresión y extrapolación logarítmica[29][31]

Para poder extrapolar el crecimiento de los clientes a cinco años, se procederá a obtener la función que represente este comportamiento mediante regresión logarítmica.

La nube de puntos se analiza en base a las variables $\boldsymbol{ln(x)}$ y $\boldsymbol{y}$, pretendiendo obtener una función de la forma: $\boldsymbol{y = a\, ln(x) + b}$. En vista de que se tienen dos constantes: $\boldsymbol{a\ y\ b}$ en la ecuación, se encontrarán dos ecuaciones sumatorias a partir de la primera para poder hallar los valores. En la Ecuación 2.2 se presentan las ecuaciones a usar.

$$(\boldsymbol{a}) \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{y} = \boldsymbol{a} \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{ln(x)} + \boldsymbol{b\, n}$$

$$(\boldsymbol{b}) \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{y\, ln(x)} = \boldsymbol{a} \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{ln^2\,(x)} + \boldsymbol{b} \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{ln(x)}$$

Ecuación 2.2 Regresión logarítmica, sumatoria de (a) 1er grado (b) 2do grado
Fuente: [29]

Siendo,
$\boldsymbol{x}$ = la variable dependiente
$\boldsymbol{y}$ = la variable independiente
$\boldsymbol{n}$ = el número de muestras $(\boldsymbol{x_i, y_i})(\boldsymbol{i = 1, 2, 3, \ldots n})$
$\boldsymbol{a\ y\ b}$ = constantes

Si se despeja $\boldsymbol{b}$ de Ecuación 2.2 parte (a) y se reemplaza en la parte (b), se obtiene la Ecuación 2.3.

$$a = \frac{\sum_{i=1}^{n} y\, ln(x) - \bar{y} \sum_{i=1}^{n} ln(x)}{\sum_{i=1}^{n} ln^2(x) - \overline{ln(x)} \sum_{i=1}^{n} ln(x)}$$

Ecuación 2.3 Constante a

Entonces se encuentra la Ecuación 2.4 para obtener $\boldsymbol{b}$.

$$b = \bar{y} - \frac{a}{n} \sum_{i=1}^{n} ln(x)$$

Ecuación 2.4 Constante b

Considerando las ecuaciones 2.2, 2.3 y 2.4 se obtienen los valores indicados en la Tabla 2.14 para el crecimiento de clientes nuevos del proveedor Telconet S.A. en particular. Los datos analizados representan el comportamiento de los últimos cinco años por lo que el valor de $\boldsymbol{n}$ es 5.

CÁLCULOS DE LA REGRESIÓN LOGARÍTMICA						
Año	x	y	$ln(x)$	$ln^2(x)$	$y.ln(x)$	y^2
2007-2008	1	236	0	0	0	55.696
2008-2009	2	430	0,693	0,480	298,053	184.900
2009-2010	3	515	1,099	1,207	565,785	265.225
2010-2011	4	450	1,386	1,922	623,832	202.500
2011-2012	5	534	1,609	2,590	859,440	285.156
Total	**15**	**2.165**	**4,787**	**6,200**	**2.347,111**	**993.477**
Total/n	**3**	**433**	**0,957**	**1,240**	**469,422**	**198.695**

Tabla 2.14 Cálculos de la regresión logarítmica

Con los valores obtenidos en la Tabla 2.13, se puede calcular la constante $\boldsymbol{a}$ mostrada en la Ecuación 2.5.

$$a = \frac{2347 - 433\ x\ 4,787}{6,200 - 0,957\ x\ 4,787} = 169,687$$

Ecuación 2.5 Obtención de la constante a

Con el valor de $\boldsymbol{a}$, se puede obtener la constantes $\boldsymbol{b}$ mostrada en la Ecuación 2.6.

$$b = 433 - \frac{169,687}{5} \; x \; 4,787 = 279,53$$

Ecuación 2.6 Obtención de la constante b

De esta manera se obtiene la función logarítmica estimada en la Ecuación 2.7.

$$Y = 169,687 * ln(x) + 279,53$$

Ecuación 2.7 Función logarítmica estimada

Teniendo la función logarítmica estimada, se puede extrapolar la información de los clientes nuevos a los cinco años posteriores: 2012-2017. Los valores calculados se indican en la Tabla 2.15 con los porcentajes de crecimiento.

REGRESIÓN Y EXTRAPOLACIÓN LOGARÍTMICA						
Año	x	y	**% *Crec.***	***Y***	**% *Crec.***	$e = y\text{-}Y$
2007-2008	1	236	-	271	-	-34,525
2008-2009	2	430	82,20%	388	43,48%	41,857
2009-2010	3	515	19,77%	457	17,73%	58,055
2010-2011	4	450	-12,62%	506	10,68%	-55,761
2011-2012	5	534	18,67%	544	7,49%	-9,625
2012-2013	6	-	-	575	5,69%	-
2013-2014	7	-	-	601	4,55%	-
2014-2015	8	-	-	623	3,77%	-
2015-2016	9	-	-	643	3,21%	-
2016-2017	10	-	-	661	2,78%	-
PROMEDIO (2012-2017)				**5269**	**4,00%**	

Tabla 2.15 Regresión y extrapolación logarítmica

Considerando los resultados de la Tabla 2.15 se puede determinar que durante los primeros años, el crecimiento de los clientes fue significativo; pero en los años posteriores el número de clientes se mantiene casi constante. Con ello, para el 2016-2017 el porcentaje de crecimiento esperado será de 2,78% llegando a 661 clientes, y para los años 2012-2017 de 4% en promedio.

En la Figura 2.16 se grafican las funciones: original con los datos obtenidos de Telconet S.A. y logarítmica estimada con la proyección a cinco años.

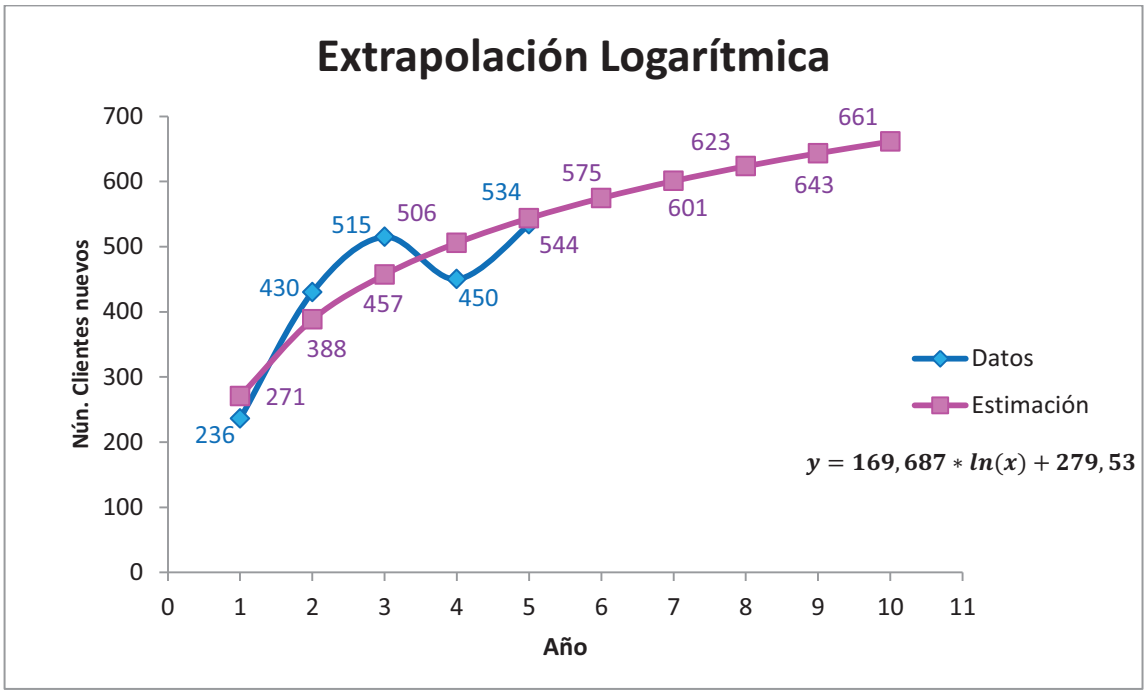


Figura 2.16 Extrapolación logarítmica

2.2.2. VENTAS FACTURADAS[15][29][31]

El número de clientes no refleja el crecimiento real de una empresa. Se pueden tener pocos clientes que facturen grandes cantidades de dinero, o cientos de ellos con facturas pequeñas. Por lo cual además del número de clientes, se analizarán las ventas facturas durante los últimos cinco años (marzo de 2007 a marzo de 2012), y se proyectará la información a marzo de 2017. Los datos presentados en la Tabla 2.16 fueron obtenidos del departamento de Facturación de Telconet S.A.

VENTAS FACTURADAS POR AÑO		
Año	**Ventas facturadas[28]**	**% Crec.**
31 de marzo 2007- 31 de marzo 2008	11,967	-
31 de marzo 2008- 31 de marzo 2009	15,745	31,57%
31 de marzo 2009- 31 de marzo 2010	21,697	37,80%
31 de marzo 2010- 31 de marzo 2011	27,271	25,69%
31 de marzo 2011- 31 de marzo 2012	36,921	35,38%

Tabla 2.16 Ventas facturadas 2007- 2012

[28] En millones de dólares

Para un mejor análisis se presenta la información en una gráfica de barras en la Figura 2.17.

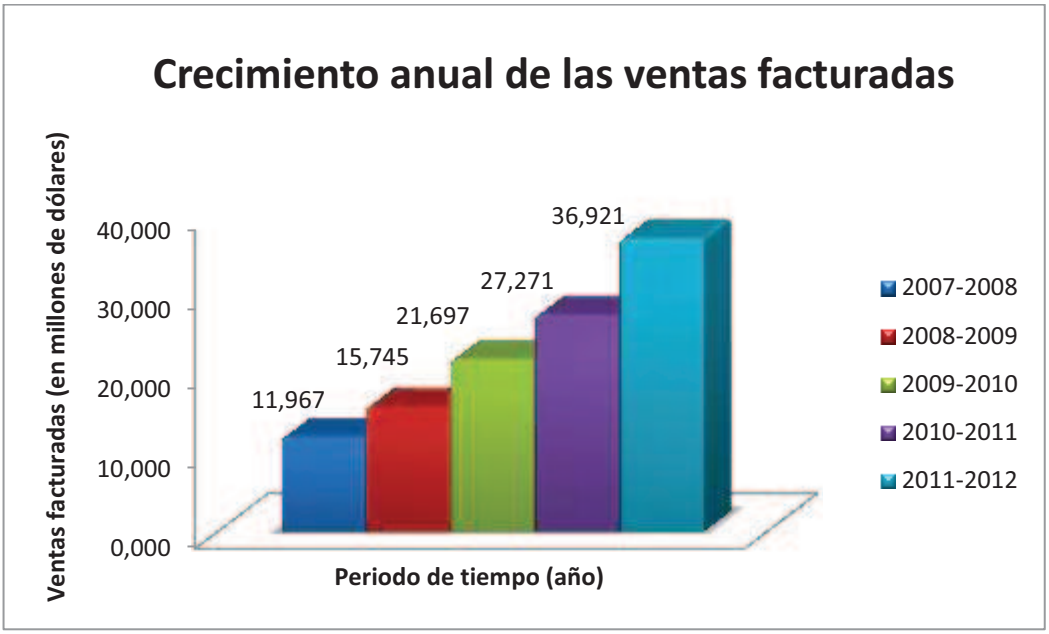


Figura 2.17 Ventas facturadas 2007- 2012

El crecimiento de las ventas ha sido positivo y progresivo, de 11 millones facturados en el 2007-2008 se ha llegado a casi 37 millones de dólares en el 2012.

2.2.2.1. Porcentaje de crecimiento

En la Figura 2.18 se obtiene la gráfica lineal del crecimiento de las ventas facturadas durante los últimos cinco años, con el objetivo de encontrar la dependencia funcional de los puntos y poder extrapolar la información.

La gráfica presentada en la Figura 2.18 tiene una dependencia funcional casi perfecta a dos funciones: exponencial y polinomial de segundo orden. Si se aproximan los datos a una función exponencial, se esperaría que en los próximos años las ventas se incrementen drásticamente lo cual es incierto pero optimista. Por el contrario, si se analiza una función polinomial de segundo orden, el crecimiento será significativo y más realista, acoplándose a los objetivos de Telconet S.A.

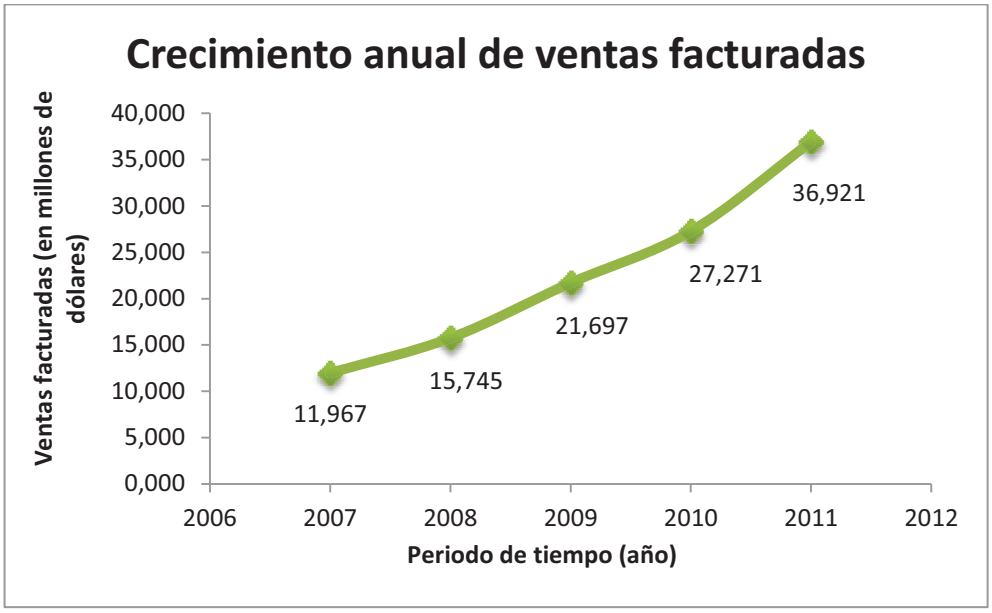


Figura 2.18 Crecimiento de las ventas facturadas 2007-2012
Fuente: [15]

2.2.2.2. Regresión y extrapolación polinomial de segundo orden[15][29][31]

Para poder extrapolar el crecimiento de las ventas facturas, se procederá a obtener la función que represente este comportamiento mediante regresión polinomial de segundo orden, pretendiendo obtener una función de la forma: $\boldsymbol{y = ax^2 + bx + c}$. Se tienen tres constantes: $\boldsymbol{a, b\ y\ c}$ en la ecuación, por lo que se encontrarán tres ecuaciones sumatorias a partir de la primera, para poder hallar los valores.

En las Ecuaciones 2.8 se presentan las ecuaciones a reemplazar.

$$(\boldsymbol{a}) \sum_{i=1}^{n} \boldsymbol{y} = \boldsymbol{c} * \boldsymbol{n} + \boldsymbol{b} \sum_{i=1}^{n} \boldsymbol{x} + \boldsymbol{a} \sum_{i=1}^{n} \boldsymbol{x^2}$$

$$(\boldsymbol{b}) \sum_{i=1}^{n} \boldsymbol{xy} = \boldsymbol{c} \sum_{i=1}^{n} \boldsymbol{x} + \boldsymbol{b} \sum_{i=1}^{n} \boldsymbol{x^2} + \boldsymbol{a} \sum_{i=1}^{n} \boldsymbol{x^3}$$

$$(\boldsymbol{c}) \sum_{i=1}^{n} \boldsymbol{x^2 y} = \boldsymbol{c} \sum_{i=1}^{n} \boldsymbol{x^2} + \boldsymbol{b} \sum_{i=1}^{n} \boldsymbol{x^3} + \boldsymbol{a} \sum_{i=1}^{n} \boldsymbol{x^4}$$

Ecuación 2.8 Regresión polinomial, sumatoria de (a) 1er grado (b) 2do grado (c) 3er grado
Fuente: [29]

Siendo,

$\boldsymbol{x}$ = la variable dependiente

$\boldsymbol{y}$ = la variable independiente

$\boldsymbol{n}$ = el número de muestras $(\boldsymbol{x_i}, \boldsymbol{y_i})(\boldsymbol{i = 1, 2, 3, \ldots n})$

$\boldsymbol{a, b\ y\ c}$ = constantes

Considerando las Ecuaciones 2.8 se obtienen los valores indicados en la Tabla 2.17 para el crecimiento en ventas de Telconet S.A. Los datos analizados representan el comportamiento de los últimos cinco años por lo que el valor de $\boldsymbol{n}$ es 5.

CÁLCULOS DE LA REGRESIÓN POLINOMIAL[29]							
Año	$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{x^2}$	$\boldsymbol{x^3}$	$\boldsymbol{x^4}$	$\boldsymbol{xy}$	$\boldsymbol{x^2y}$
2007-2008	1	11,967	1,000	1,000	1,000	11,967	11,967
2008-2009	2	15,745	4,000	8,000	16,000	31,490	62,981
2009-2010	3	21,697	9,000	27,000	81,000	65,091	195,272
2010-2011	4	27,271	16,000	64,000	256,000	109,086	436,342
2011-2012	5	36,921	25,000	125,000	625,000	184,607	923,033
TOTAL	**15**	**113,602**	**55,000**	**225,000**	**979,000**	**402,240**	**1629,595**
TOTAL/n	**3**	**22,720**	**11,000**	**45,000**	**195,800**	**80,448**	**325,919**

Tabla 2.17 Cálculos de la regresión polinomial

Con los valores obtenidos en la Tabla 2.17 se obtienen las tres ecuaciones para hallar las constantes $\boldsymbol{a, b\ y\ c}$, mostradas en las Ecuaciones 2.9.

$$(\boldsymbol{a})\ \boldsymbol{113602144,93\ = 5c + \ 15b + 55a}$$

$$(\boldsymbol{b})\boldsymbol{402240477,74 = 15c + \ 55b + 225a}$$

$$(\boldsymbol{c})\boldsymbol{1629594968,46\ = 55c + 225b + 979a}$$

Ecuación 2.9 Reemplazo de las sumatorias de (a) 1er grado (b) 2do grado (c) 3er grado

[29] En millones de dólares

Resolviendo las Ecuaciones 2.9, se obtiene la función polinomial estimada de segundo orden en la Ecuación 2.10.

$$Y = 811936,39x^2 + 1271786,22x + 9973769,11$$

Ecuación 2.10 Función polinomial estimada

Con la función polinomial estimada, se puede extrapolar la información de las ventas facturadas de la sucursal de Quito a los años: 2012-2017. Los valores calculados se indican en la Tabla 2.18, además de los porcentajes de crecimiento y los errores.

REGRESIÓN Y EXTRAPOLACIÓN LOGARÍTMICA[30]						
Año	x	y	*% Crec.*	*Y*	*% Crec.*	$e = y - Y$
2007-2008	1	11,967	-	12,057	-	-0,090
2008-2009	2	15,745	31,57%	15,765	30,75%	-0,020
2009-2010	3	21,697	37,80%	21,097	33,82%	0,600
2010-2011	4	27,271	25,69%	28,052	32,97%	-0,781
2011-2012	5	36,921	35,38%	36,631	30,58%	0,290
2012-2013	6	-	-	46,834	27,85%	-
2013-2014	7	-	-	58,661	25,25%	-
2014-2015	8	-	-	72,112	22,93%	-
2015-2016	9	-	-	87,187	20,90%	-
2016-2017	10	-	-	103,885	19,15%	-
PROMEDIO (2007-2017)			32,61%		27,13%	

Tabla 2.18 Regresión Polinomial

El valor de las ventas esperadas en el 2016-2017 es de 103 millones de dólares con un porcentaje de crecimiento de 19,15%, y en promedio de 27,13% para los años 2007-2017. En la Figura 2.19 se grafican las funciones: original con los datos obtenidos de Telconet S.A. y polinomial estimada de segundo orden con proyección a cinco años.

[30] En millones de dólares.

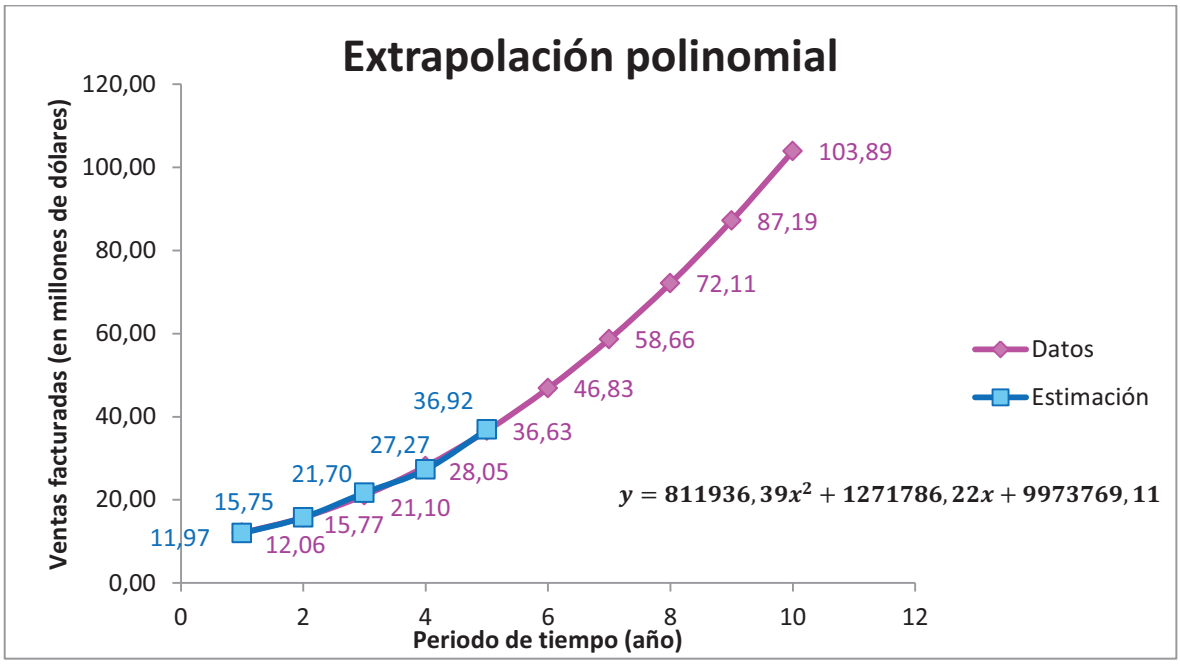


Figura 2.19 Extrapolación polinomial de segundo orden

2.2.3. PORCENTAJE DE CRECIMIENTO DE TELCONET S.A.-QUITO

Después del análisis de los clientes nuevos y de las ventas facturadas en los últimos años, se determina que para los requerimientos del rediseño se considerará el porcentaje de las ventas, como el porcentaje de crecimiento de la sucursal de Quito de Telconet S.A.

Se estima tener un ligero incremento en el número de clientes nuevos en el proveedor, pero un crecimiento substancial en las ventas facturas por las nuevas aplicaciones que se empiezan a ofrecer.

PORCENTAJE DE CRECIMIENTO	27,13%

2.2.4. REQUERIMIENTOS Y ANÁLISIS DE TRÁFICO PARA EL REDISEÑO DE LA RED MPLS DE TELCONET S.A.-QUITO

La sucursal de Quito del proveedor Telconet S.A. requiere rediseñar su red MPLS con el objetivo de:

- Brindar diferenciación de Clases de Servicios y QoS
- Tener mecanismos de control y evasión de la congestión
- Manejar Ingeniería de Tráfico
- Ofrecer VPN en MPLS
- Tener soporte para IPv6
- Brindar seguridad en IPv6

En las secciones 2.2.4.1 y 2.2.4.2 se realizará el análisis de tráfico a fin de determinar: el tipo y la cantidad de información que circula por la red, los requerimientos de tráfico y las capacidades de los enlaces requeridas para el rediseño.

Para este análisis se establecerán dos mecanismos y son:

- Mecanismo 1

  Se obtendrán las capacidades contratadas por los clientes y se analizará el tráfico de los servicios ofertados por el ISP para los próximos cinco años.
- Mecanismo 2

  Se utilizará la herramienta Cacti para graficar la tendencia del tráfico y conseguir los valores máximos y promedios de las velocidades registradas en los principales equipos.

La idea de analizar la red mediante estos dos mecanismos, permitirá obtener resultados más cercanos a la realidad del proveedor.

2.2.4.1. Mecanismo 1: Análisis de tráfico mediante las capacidades contratadas

Para obtener los requerimientos del diseño se determinarán las velocidades contratadas por los clientes y diferenciadas por servicios, como: Internet 1:1, transmisión de datos, transmisión de vídeo, etc; más la proyección de crecimiento esperada en cinco años que fue analizada en la sección 2.2.3.

Toda la información mostrada fue obtenida del departamento de *Networking* de la sucursal de Quito de Telconet S.A.

1. Requerimientos de Internet dedicado y tránsito al *backbone* de Internet[1]

El tráfico de Internet es tolerante a retardos, *jitter* y pérdida de paquetes por lo tanto no requiere un trato preferencial en la red y sus requerimientos no tienen grandes exigencias. Pero de manera particular, Telconet S.A. ofrece los siguientes parámetros en los SLA:

- Disponibilidad: 99,9%[1]
- Pérdida de paquetes: cercanos al 0%
- Latencias al *backbone* en E.E.U.U.: 100 ms
- *Mean Time To Repair* (MTTR): 2 horas

Con el fin de definir los requerimientos de las velocidades de subida y bajada de este servicio ya que el retardo, el *jitter* y la pérdida de paquetes no demandan grandes exigencias en la red, se obtuvieron las capacidades contratadas en cada PE: desde el 31 de marzo del 2011 hasta el 31 de marzo de 2012; y se extrapoló la información al 2017 con el porcentaje de crecimiento obtenido en la sección 2.2.3.

La Tabla 2.19 presenta la velocidad requerida según la estimación realizada. La velocidad de bajada contratada tiene los mismos valores que la Tabla 2.19.

VELOCIDAD DE SUBIDA (Mbps)							
NODOS PE	**2011-2012**	**% Crec.**	**2012-2013**	**2013-2014**	**2014-2015**	**2015-2016**	**2016-2017**
SUR2	331,488	27,13%	421,421	535,752	681,102	865,885	1.100,799
ARMENIA	120,296	27,13%	152,932	194,423	247,170	314,227	399,477
BORROMONI	176,704	27,13%	224,644	285,590	363,070	461,571	586,795
DATACENTER	432,84	27,13%	550,269	699,558	889,348	1.130,628	1.437,367
GOSSEAL	1.403,771	27,13%	1.784,614	2268,780	2.884,300	3.666,810	4.661,616
MUROS	303,856	27,13%	386,292	491,093	624,327	793,707	1.009,039
TOTAL	**2.768,955**	**27,13%**	**3.520,172**	**4.475,195**	**5.689,316**	**7.232,827**	**9.195,093**

Tabla 2.19 Requerimientos de Internet dedicado

Según la información presentada en la Tabla 2.19, los requerimientos de las velocidades serán de 9 Gbps.

2. Requerimientos de transmisión de datos[1][22]

Los requerimientos para este servicio son: la disponibilidad del 99,6% y la velocidad proyectada a marzo de 2017.

Para los requerimientos de las velocidades, se obtuvieron las capacidades contratadas por los clientes durante el año 2011-2012, y se las proyectó a cinco años, utilizando el porcentaje de crecimiento analizado en la sección 2.2.3.

En la Tabla 2.20 se detallan las velocidades estimadas, con un total de 18 Gbps para el año 2017. Las velocidades de subida y bajada contratadas en Telconet S.A. tienen los mismos valores.

VELOCIDAD DE SUBIDA (Mbps)							
NODOS PE	**2011-2012**	**% Crec.**	**2012-2013**	**2013-2014**	**2014-2015**	**2015-2016**	**2016-2017**
SUR2	517,252	27,13%	657,582	835,985	1.062,787	1.351,121	1.717,681
ARMENIA	103,968	27,13%	132,175	168,033	213,621	271,576	345,255
BORROMONI	149,76	27,13%	190,390	242,043	307,709	391,190	497,320
DATACENTER	711,618	27,13%	904,680	1.150,120	1.462,147	1.858,828	2.363,128
GOSSEAL	3.568,758	27,13%	4.536,962	5.767,840	7.332,655	9.322,004	11.851,064
MUROS	434,664	27,13%	552,588	702,506	893,095	1.135,392	1.443,424
TOTAL	**5.486,02**	**27,13%**	**6.974,377**	**8.866,526**	**11.272,014**	**14.330,112**	**18.217,871**

Tabla 2.20 Requerimientos de trasmisión de datos

3. Requerimientos de Internet 2[1][28][30]

Telconet S.A. tiene implementado IPv6 solo en los equipos del proyecto del Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (CEDIA)[31] y no en el resto de la ciudad de Quito. El servicio que se brinda es enrutamiento *unicast* de Internet en IPv6 y no se tiene soporte para aplicaciones *multicast*.

[31] CEDIA es el consorcio que impulsa el desarrollo científico y educativo de las tecnologías de la información, las redes de telecomunicaciones y las redes informáticas del país.

La red Avanzada de Ecuador (RED CEDIA) interconecta las principales universidades, escuelas politécnicas e instituciones de investigación y desarrollo del país como se indica en la Figura 2.20. Tiene capacidades exclusivas de hasta 1 Gbps; pero por seguridad del proyecto y confidencialidad de la empresa con el Gobierno de Ecuador, no se puede mostrar a detalle la red.

Para los requerimientos del rediseño, no se pueden detallar las capacidades contratadas por el proyecto CEDIA y proyectarlas al 2017 como se hizo con los dos servicios anteriores, ya que esta información es sumamente confidencial para la empresa por ser de un consorcio del Gobierno. El tráfico de este proyecto no se detallará por separado, sino dentro de las capacidades de los servicios de: Internet y transmisión de datos, especificados en las secciones 1 y 2 respectivamente.

Figura 2.20 Instituciones del proyecto CEDIA

Fuente: [1]

Por otro lado, la Secretaría Nacional de Telecomunicaciones (SENATEL) envió una circular el 10 de mayo de 2012 sobre las exigencias establecidas a los ISP para la implementación de IPv6, y se centra en dos puntos[32]:

- Admitir en sus redes, plataformas y sistemas el curso normal de tráfico de IPv6 en coexistencia con IPv4.
- Establecer planes de direccionamiento, y en función de los mismos, iniciar los trámites necesarios para la solicitud de recursos de direccionamiento IPv6.

Tras esta circular, Telconet S.A. espera que la demanda de IPv6 se incremente, no solo para las instituciones del Consorcio CEDIA sino a nivel nacional. Por el momento, la medida acatada por el proveedor para los ISP medianos, es que soliciten sus propias direcciones IPv6 a LACNIC, aunque Telconet S.A. les puede facilitar temporalmente un rango de direcciones (subred máscara 48) de la red que actualmente dispone.

La circular fue facilitada por el departamento de *Networking* de Telconet S.A.-Quito y se muestra en el ANEXO B.

Para el presente rediseño de red, los requerimientos de Internet 2 se incluyen en la sección 2.2.4.1.1, debido a que el tráfico en IPv6 no se incrementará drásticamente en los próximos cinco años. Los ISP pequeños y los clientes contratarán los servicios de Internet en IPv4 e IPv6 simultáneamente; y aumentarán su capacidad en IPv6 conforme la disminuyan en IPv4 hasta que la desplacen por completo, lo cual sucederá después de algunos años. Por lo que, el tráfico de Internet en IPv6 estará asociado con el tráfico de Internet en IPv4.

4. Requerimientos de transmisión de canal de vídeo, videoconferencia en HD y Web[1][16][21][22]

La transmisión de canal de vídeo y las videoconferencias en HD y Web son servicios que no han tenido gran acogida en la sucursal de Quito, a excepción de algunas radiodifusoras y canales de televisión abierta y por cable.

[32] Esta información fue tomada textualmente del ANEXO B.

De los tres, el servicio que más se brinda es la transmisión de canal de vídeo. Sus requerimientos no son de vídeo en sí, sino de transmisión de datos debido a que se levanta un túnel entre los dos puntos, desde y hacia donde el cliente desea transmitir el vídeo. No es un servicio que requiere mucho tráfico ni se implementa todo el tiempo. Por ejemplo, Ecuavisa, un canal de televisión abierta, tiene contratado este servicio para las transmisiones de los partidos de fútbol en vivo desde los estadios solo cuando hay un partido.

En la Figura 2.21, se detalla el proceso y los dispositivos para realizar una transmisión de vídeo. Se establece un túnel de datos por donde se trasmite el vídeo, teniendo en los puntos terminales del túnel los de/codificadores (*StreamBox* SBT3[33]) que se encargan de convertir la señal de vídeo analógico a vídeo digital y viceversa.

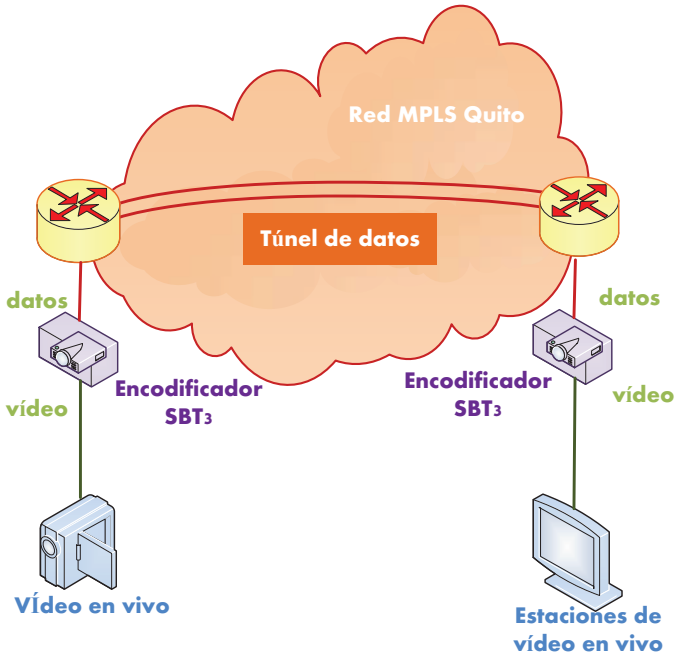


Figura 2.21 Transmisión de vídeo

Fuente: [1]

Los requerimientos para este servicio se incluirán en la sección 2.2.4.1.2 debido a que a través de la red, se transmiten como datos.

[33] El de/codificador que utiliza Telconet S.A. es el SBT3-5300 SD *Enconder* que maneja velocidades de compresión desde 64 kbps hasta 15 Mbps. Para mayor información del funcionamiento de los *streambox* se recomienda revisar [21].

Además, frente a la demanda de ciertas empresas por realizar videoconferencias, se ofrecen los servicios de videoconferencias: en *High Definition* (HD) y Web; aunque más acogida se ha tenido en la venta de los equipos de videoconferencia. Para este servicio, se ofrece un canal de transmisión de datos dedicado de 4 Mbps, full dúplex, con garantía de vídeo en HD si la videoconferencia es en alta definición.

Los requerimientos de tráfico para las videoconferencias HD y Web no son muy significativos, así que se los incluye dentro del servicio de Internet dedicado en la sección 2.2.1, que ya considera el crecimiento para el 2017. No se espera gran acogida de este servicio.

5. Requerimientos de IP PBX gestionado[22]

Telconet S.A. brinda también comunicaciones de voz mediante sus enlaces de datos instalados. El ISP será el proveedor de los servicios de datos y de voz, representando mayores beneficios económicos y de administración para el cliente. Se minimiza el costo de las llamadas nacionales y regionales al aprovechar los enlaces instalados para la transmisión de datos, en vez de pagar un costo adicional a la Corporación Nacional de Telecomunicaciones (CNT).

La garantía de hardware es ilimitada y sin costo, porque Telconet S.A. es el responsable de la administración de los equipos a excepción de los teléfonos IP. Los clientes no deben comprar los equipos del IP PBX, ni necesitan personal altamente capacitado para administrarlo.

Para los requerimientos de velocidad de este servicio, se obtienen las capacidades contratadas de los clientes en el año 2011-2012, y se las estima a cinco años utilizando el porcentaje de crecimiento analizado en la sección 2.2.3.

En la Tabla 2.21 se detallan las velocidades estimadas, con un total de 37 Mbps para el año 2017. Las velocidades de subida y bajada contratadas en Telconet S.A. tienen los mismos valores.

VELOCIDAD DE SUBIDA (Mbps)							
NODOS PE	**2011-2012**	**% Crec.**	**2012-2013**	**2013-2014**	**2014-2015**	**2015-2016**	**2016-2017**
SUR2	0	27,13%	0,000	0,000	0,000	0,000	0,000
ARMENIA	0	27,13%	0,000	0,000	0,000	0,000	0,000
BORROMONI	1,024	27,13%	1,302	1,655	2,104	2,675	3,400
DATACENTER	0	27,13%	0,000	0,000	0,000	0,000	0,000
GOSSEAL	10,24	27,13%	13,018	16,550	21,040	26,748	34,005
MUROS	0	27,13%	0,000	0,000	0,000	0,000	0,000
TOTAL	**11,264**	**27,13%**	**14,320**	**18,205**	**23,144**	**29,423**	**37,405**

Tabla 2.21 Requerimientos de la IP PBX Gestionado

6. Requerimientos de comunicaciones unificadas[22]

Telconet S.A. ofrece muchos de sus servicios dentro de un solo ambiente, como las principales comunicaciones de una empresa: telefonía, correo electrónico, vídeo, mensajería instantánea, entre otras. Las comunicaciones unificadas aumentan la productividad, a través de la simplicidad del acceso a la información y a los recursos, disminuyendo los costos operativos.

El crecimiento para este servicio en los próximos cinco años, no se espera que sea tan significativo porque para empezar, la telefonía no ha tenido gran aceptación y peor lo harán el resto de aplicaciones. Los requerimientos de tráfico para las comunicaciones unificadas no son significativos, por lo que se incluyen en los requerimientos del IP PBX analizado en la sección 2.2.4.1.5.

7. Requerimientos de seguridad perimetral gestionada y consultorías de seguridad[22]

Telconet S.A. pretende ofrecer a sus clientes seguridad avanzada de la información, a través del uso eficiente de las herramientas. El proceso es transparente al usuario, con excelente equipamiento de hardware y software y sobre todo, recurso humano altamente calificado; asegurando la disponibilidad, la integridad y la confidencialidad de la información.

La inversión de los clientes no se deprecia en el tiempo porque tendrán un sistema actualizado en tecnología y protegido frente a ataques informáticos. Además, se ofrecen consultorías de seguridad relacionadas a proyectos de diseño, implementación, seguimiento y certificación de seguridad de la información de una entidad.

Los requerimientos de tráfico para la seguridad perimetral gestionada es despreciable, al igual que para las consultorías de seguridad, debido a que estos servicios representan asesoría técnica e implementación de hardware y software para el análisis de las vulnerabilidades, y no generación de tráfico por parte del cliente.

8. Requerimientos del Centro de Datos[1][13][22]

Ecuador presenta una demanda insatisfecha de sitios de alta disponibilidad, por lo que Telconet S.A. está construyendo dos Centros de Datos con más de 1.500 m², en las ciudades de Quito y Guayaquil.

Para la sucursal Quito, se esperan brindar los servicios de *Data Center: housing* y *hosting,* a partir del mes de abril del 2013.

- Alquiler de espacios para gabinetes cerrados (*housing*)
  Este servicio implica alojamiento compartido de la información en suites dedicadas llamadas jaulas (*cage*), y/o alquiler de espacios cerrados (*colocation*) que ofrecen total privacidad y seguridad.
- Suites dedicadas dentro del *Data Center* (*hosting*)
  Brinda servidores virtualizados y servicios en la nube con los últimos avances tecnológicos en seguridad, como: vigilancia, seguridad biométrica, protección anti-incendios, alimentación eléctrica, climatización controlada y atención profesional 24x7.

Además, se ofrecerán más servicios conforme sean requeridos como: seguridad lógica, mantenimiento de sistemas, soporte de manos remotas, monitoreo

dedicado, *backups cold/hot,* administración de bases de datos y consultorías, entre otras como se indican la Figura 2.22.

Figura 2.22 Esquema de servicios del *Data Center* de Telconet S.A.-Quito
Fuente: [1]

Para determinar los requerimientos del Centro de Datos, se recurre al estudio de mercado realizado por Telconet S.A. que impulsó a desarrollar esta infraestructura. La información no se podrá mostrar a detalle debido a que es confidencial, sobre todo porque este servicio se implementará en los próximos meses.

El resultado del estudio de mercado establece[13]: "se construye el Centro de Datos en la ciudad de Quito con una capacidad de 180 racks y enlaces de 20 Gbps, para soportar el tráfico de cinco carriers que se incluyen en este proyecto a nivel nacional: Telefónica, Claro, CNT, *Global Crossing* y Telconet S.A."

Para los requerimientos de tráfico del Centro de Datos, se considera la capacidad obtenida del estudio de mercado de 20 Gbps como el tráfico estimado que circulará por la infraestructura de red del proveedor para el año 2017.

9. Requerimientos de E-*Billing*[22]

Telconet S.A. pretende brindar como nuevo servicio la facturación electrónica (*e-billing*), ya que el costo de emisión y envío de una factura impresa tradicionalmente, resulta elevado. *E-billing* permite: la búsqueda ordenada y eficiente de los archivos, la simplicidad en la administración y el mantenimiento adecuado del servicio.

Para el presente diseño, los requerimientos de *e-billing* se incluyen en el análisis de la sección 2.2.4.1.1, debido a que el tráfico generado por este servicio es prácticamente despreciable.

REQUERIMIENTOS TOTALES DE TRÁFICO DEL MECANISMO 1

Considerando cada uno de los servicios detallados en las secciones 1 a 9, en la Tabla 2.22 se presentan de manera resumida, los requerimientos de tráfico para la red de Telconet S.A.-Quito con un total de 47,5 Gbps aproximadamente para el año 2017.

VELOCIDAD DE SUBIDA (Mbps)					
NODOS PE	**INTERNET DEDICADO**	**TRANSMISIÓN DE DATOS**	**IP PBX GESTIONADO**	**DATACENTER**	**TOTAL 2017**
SUR 2	1.100,799	1.717,681	0,000	20.000,000	2.818,480
ARMENIA	399,477	345,255	0,000		744,732
BORROMONI	586,795	497,320	3,400		1.087,516
DATACENTER	1.437,367	2.363,128	0,000		23.800,494
GOSSEAL	4.661,616	11.851,064	34,005		16.546,685
MUROS	1.009,039	1.443,424	0,000		2.452,463
TOTAL	**9.195,093**	**18.217,871**	**37,405**	**20.000,000**	**47.450,369**

Tabla 2.22 Requerimientos de totales de tráfico del mecanismo 1

Los requerimientos de las velocidades de bajada tienen los mismos valores que los mostrados en la Tabla 2.22.

2.2.4.2. Mecanismo 2: Análisis de tráfico mediante la herramienta Cacti

En este mecanismo se utiliza la herramienta Cacti para obtener las estadísticas de tráfico de los principales equipos de la red, así como los valores máximos, mínimos y promedios del tráfico entrante y saliente. La información fue graficada a la salida de las interfaces del PGOSSEAL en dirección a cada PE debido a que en el proceso de migración, todavía no se han levantado los enlaces entre el PDATACENTER y los PE.

La información expuesta a continuación fue obtenida del departamento de *Networking* de Telconet S.A. durante la última semana del mes de mayo de 2012. Por exigencias de seguridad del proveedor, se han modificado los nombres reales de los dispositivos y las interfaces a las que se encuentran conectadas.

Telconet S.A. implementó la herramienta Cacti en el año 2010 por lo que no se tienen registros de las estadísticas de tráfico de los años anteriores. Las gráficas de tráfico mostradas en esta sección tienen los siguientes parámetros:

- Inbound: Tráfico entrante.
- Outbound: Tráfico saliente.
- Current: Es el valor registrado en el momento que se tomó la muestra. Puede pertenecer al tráfico entrante o saliente.
- Average: Es el promedio entre el máximo y mínimo valor de la gráfica.
- Maximum: Es el pico más alto registrado en la gráfica.

1. PE1SUR2[18][20]

En la Figura 2.22 se muestra el tráfico registrado en el PE1SUR2 desde el 2007 hasta el 2012. En los tres primeros años no se tiene información para graficar

debido a que Telconet S.A. implementó la herramienta Cacti a partir del mes de abril del 2010. Mientras, en los dos últimos años el tráfico ha sido progresivo a excepción del mes de abril de 2011 en que el Cacti no tiene datos completos de los registros debido a las migraciones realizadas.

Según los datos de la migración a MPLS de Telconet S.A.[18], el nodo PE1SUR2 fue migrado durante el mes de abril de 2011 por lo que el Cacti no tiene registros de tráfico durante este tiempo; pero después crece considerablemente porque se activan las interfaces de los clientes.

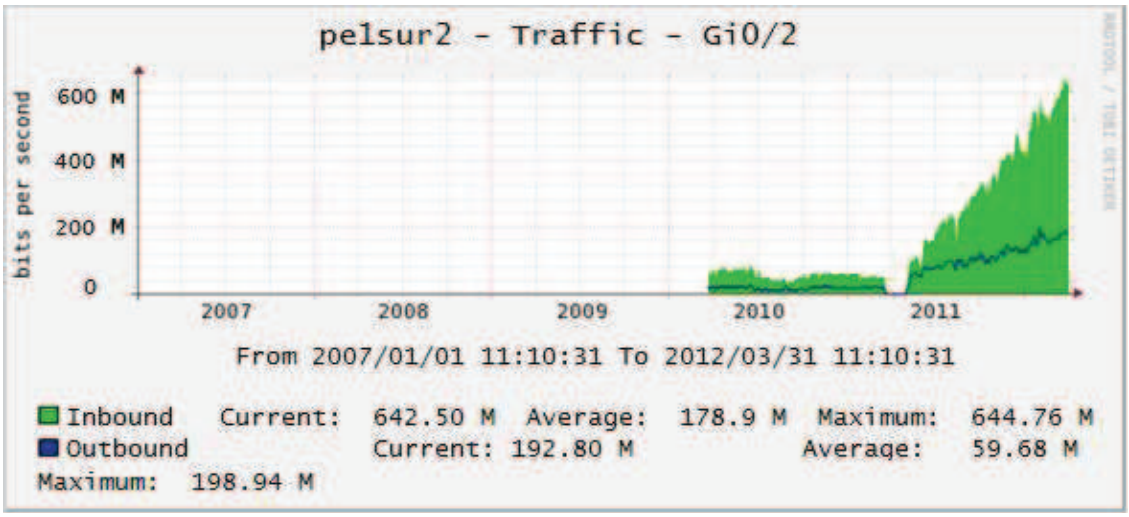


Figura 2.22 Tráfico PE1SUR2, 2007-2012

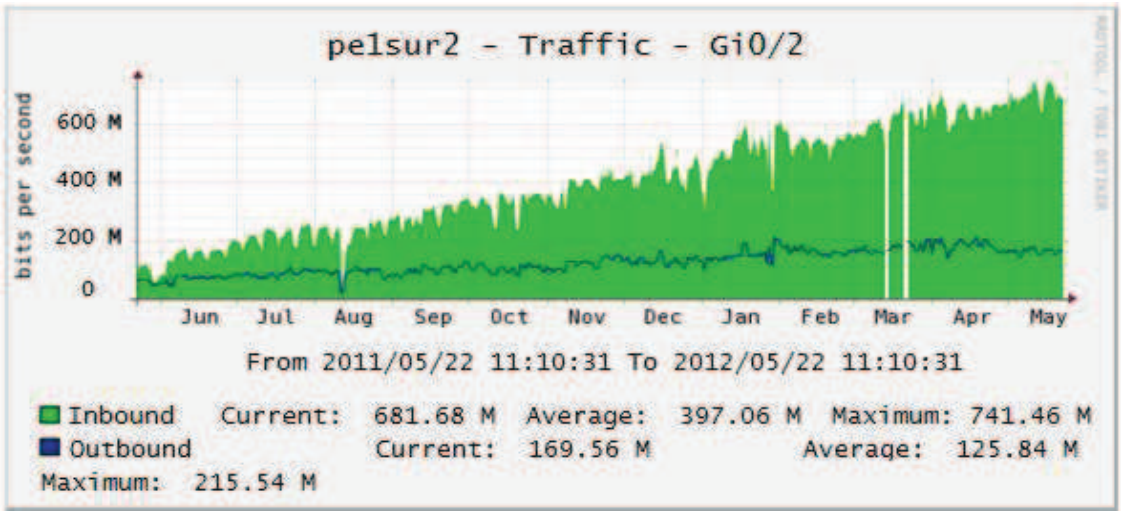


Figura 2.23 Tráfico PE1SUR2, mayo 2011- mayo 2012

Para mejor análisis del tráfico en los últimos años, se hace un acercamiento de la gráfica desde junio de 2011 hasta junio de 2012 en la Figura 2.23. Los primeros meses se tienen registros de tráfico bajos debido a la migración a MPLS, por lo que esta información no es de mucha ayuda para obtener los requerimientos del diseño.

En la Figura 2.24, se recurre a analizar el tráfico durante los primeros meses del año 2012, debido a que este presenta un comportamiento progresivo y sin cambios drásticos con valores que se acercan más a la realidad que la información presentada en las Figuras 2.22 y 2.23.

Según los registros de las emergencias de Cacti[20], durante las semanas: 11 (jueves 15 de marzo) y 12 (jueves 21 y viernes 22 de marzo de 2012) se tuvieron inconvenientes con la herramienta y se perdió información del tráfico de esos días.

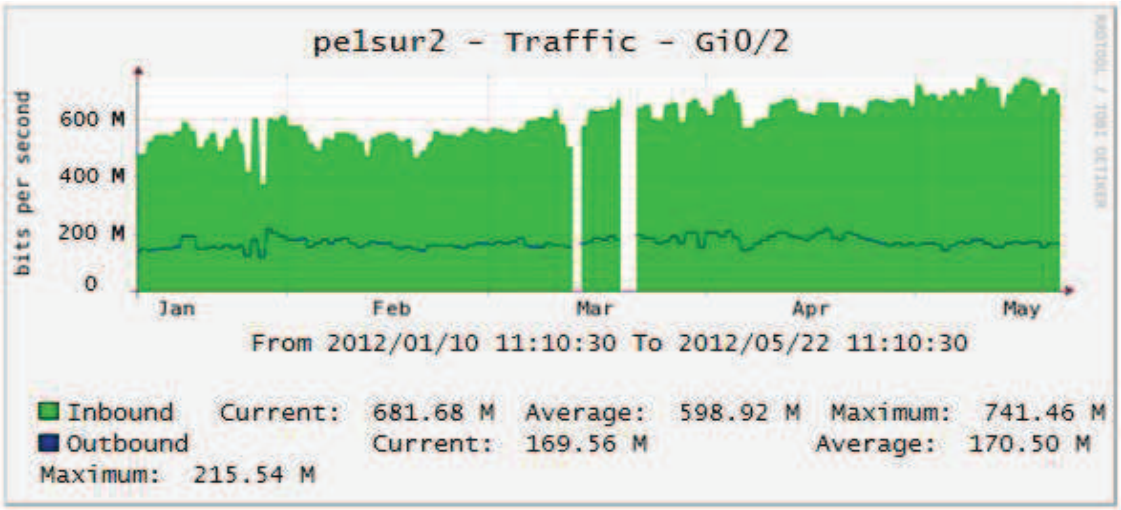


Figura 2.24 Tráfico PE1SUR2, enero - mayo 2012

2. PE1ARMENIA[18][20]

De la misma manera que en el PE1SUR2, para el PE1ARMENIA no se tienen registros de tráfico durante los años: 2007, 2008 ni 2009. Mientras, en el 2010 los valores son muy bajos y por lo tanto, no de gran ayuda para obtener los requerimientos del diseño.

En la Figura 2.25 se presenta el tráfico durante el último año correspondiente a mayo de 2011 y mayo de 2012, con el objetivo de analizar las estadísticas de tráfico que más se acerquen al comportamiento real de la red.

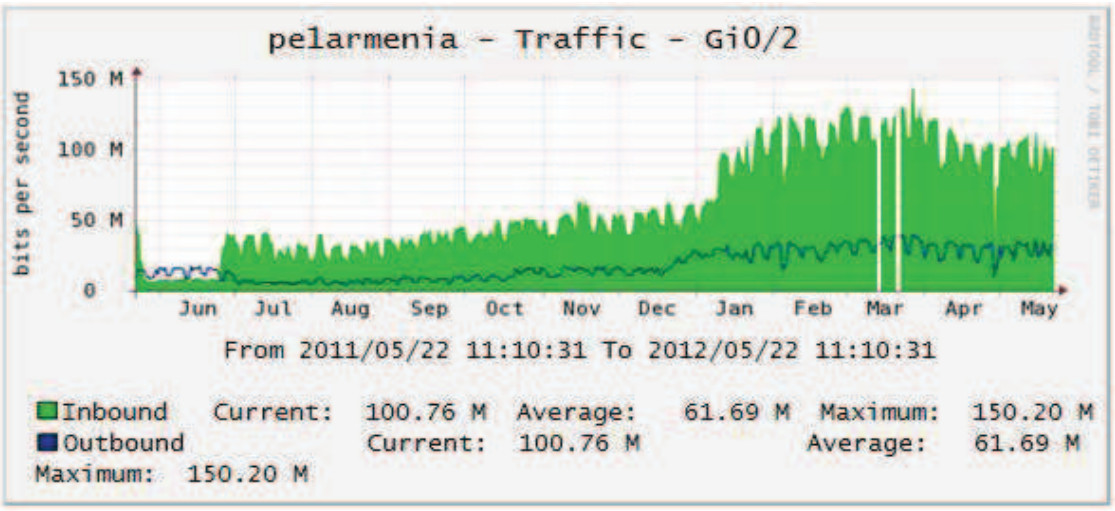


Figura 2.25 Tráfico PE1ARMENIA, mayo 2011 - mayo 2012

Según la información mostrada en la Figura 2.25, el tráfico ha variado considerablemente durante el año 2011, por lo que para el rediseño, se utilizan los registros de tráfico de los primeros meses del año 2012, como se presenta en la Figura 2.26.

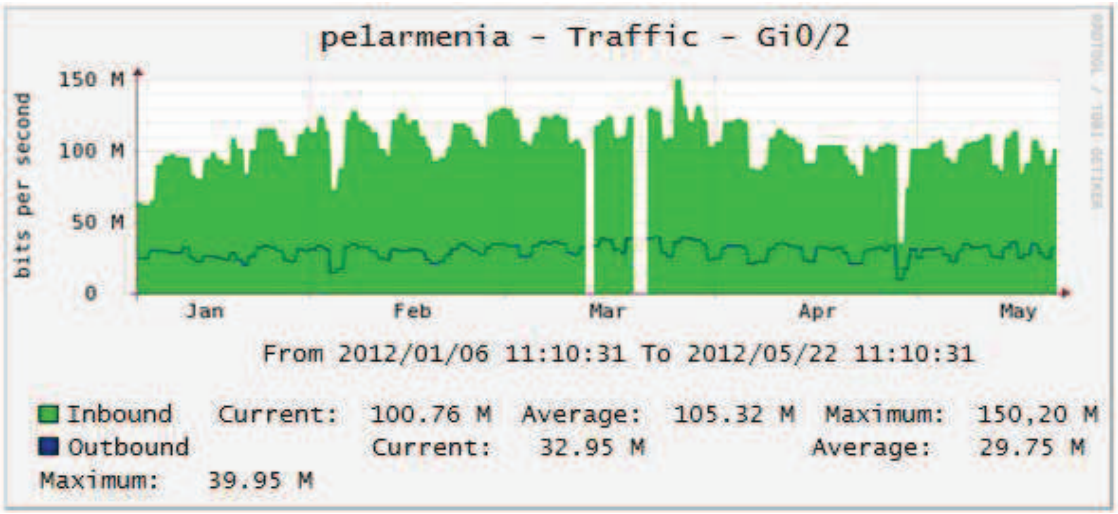


Figura 2.26 Tráfico PE1ARMENIA, enero - mayo 2012

3. PE1BORROMONI[18][20]

En la Figura 2.27 se presentan los registros de tráfico desde el 22 de mayo de 2011 hasta el mismo día del 2012. Los valores han tenido un comportamiento de crecimiento progresivo, con excepción de tres picos en los meses de agosto y octubre de 2011 y febrero de 2012 que según los registros[18], fueron producto de las migraciones temporales de los clientes al PE1BORROMONI.

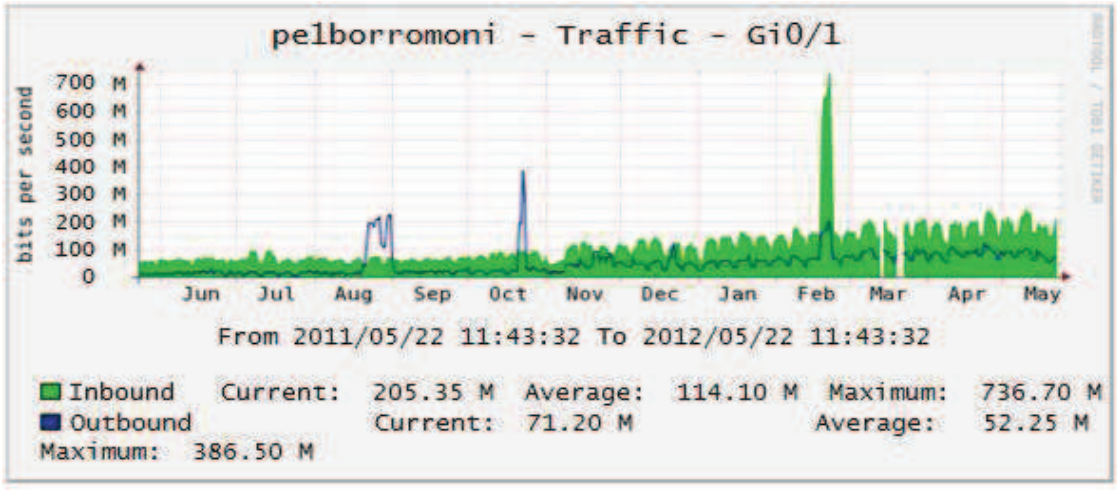


Figura 2.27 Tráfico PE1BORROMONI, mayo 2011 – mayo 2012

Para el análisis de tráfico solo se considera la información desde el 22 de febrero hasta el 22 de mayo del 2012, donde se tiene un comportamiento similar entre un mes y otro como se aprecia en la Figura 2.28.

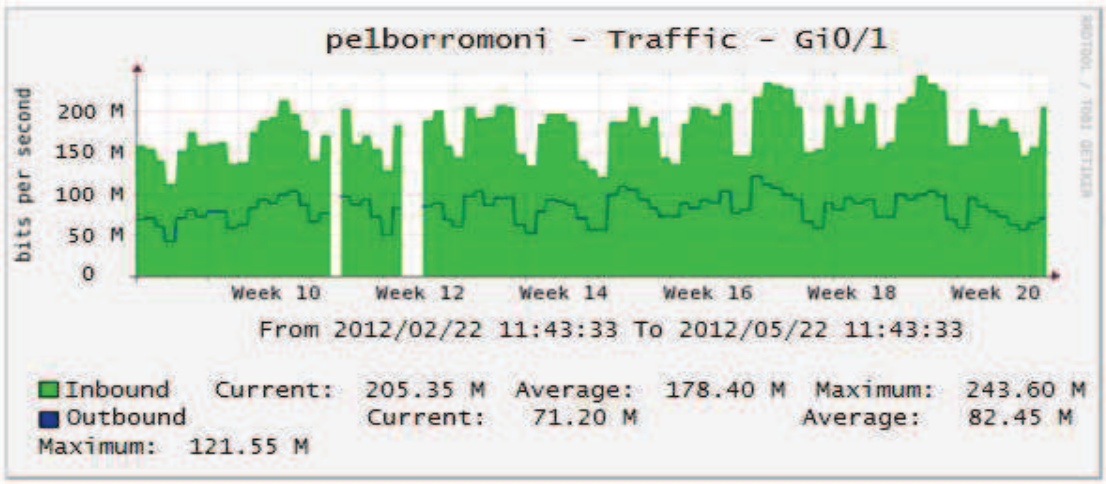


Figura 2.28 Tráfico PE1BORROMONI, febrero - mayo 2012

4. PE1DATACENTER[18][20]

En la Figura 2.29 se presenta el tráfico que ha circulado por el PE1DATACENTER durante el último año. Para los meses de junio, julio y agosto de 2011, el tráfico es bajo debido a que, según los registros de la migración a MPLS, este nodo era nuevo y no se tenían muchos clientes. Pero a partir de agosto, el tráfico empieza a crecer significativamente gracias a la acogida de los clientes en el sector.

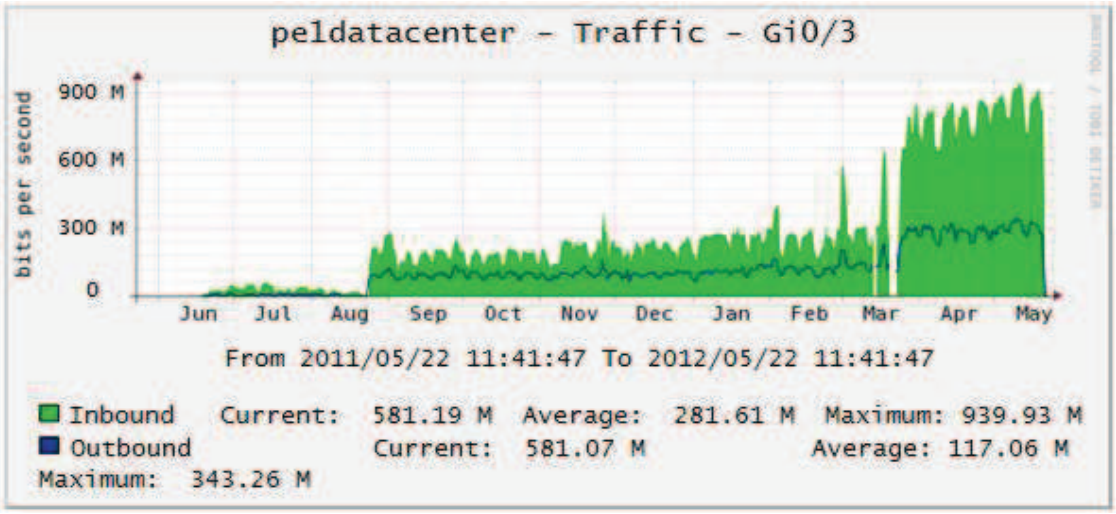


Figura 2.29 Tráfico PE1DATACENTER, mayo 2011 - mayo 2012

Con el objetivo de tener un comportamiento de tráfico más real en los requerimientos del diseño, se utilizan la información desde el mes de febrero hasta mayo de 2012 como se indica en la Figura 2.30.

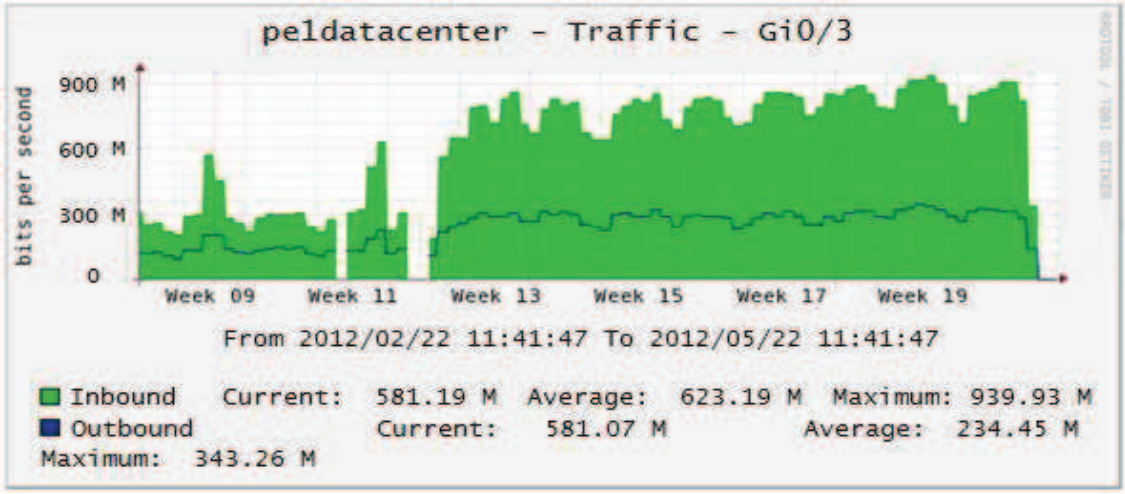


Figura 2.30 Tráfico PE1DATACENTER, febrero - mayo 2012

5. PE1GOSSEAL[18][20]

En la Figura 2.31 se presenta el tráfico que circula por el nodo PE1GOSSEAL durante los meses desde mayo de 2011 a junio de 2012, con un comportamiento de crecimiento progresivo hasta estabilizarse para los primeros meses del año 2012.

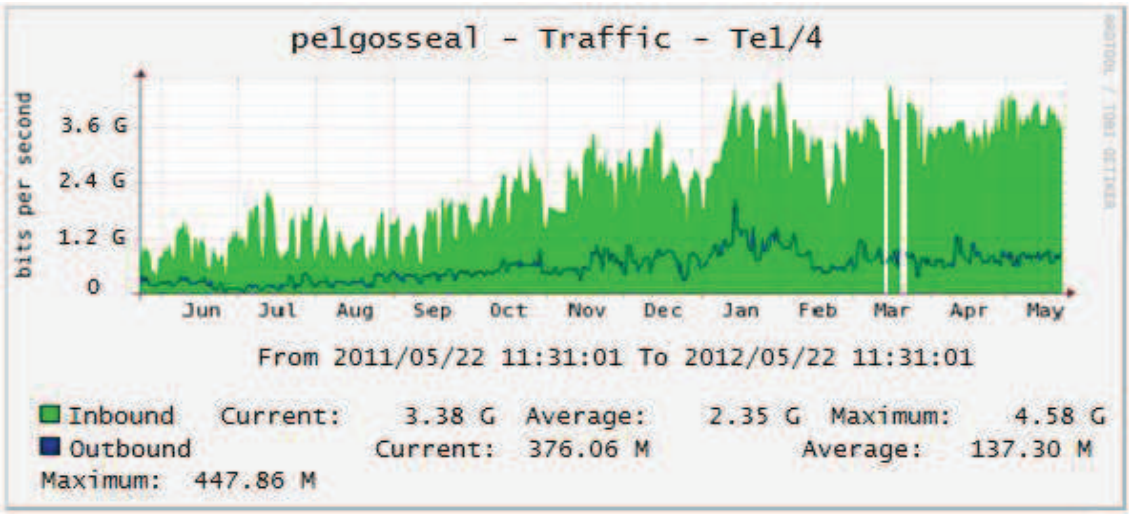


Figura 2.31 Tráfico PE1GOSSEAL, junio 2011- mayo 2012

La información útil para el rediseño implicará el comportamiento de tráfico durante los meses de enero hasta mayo de 2012, como se indica en la Figura 2.32.

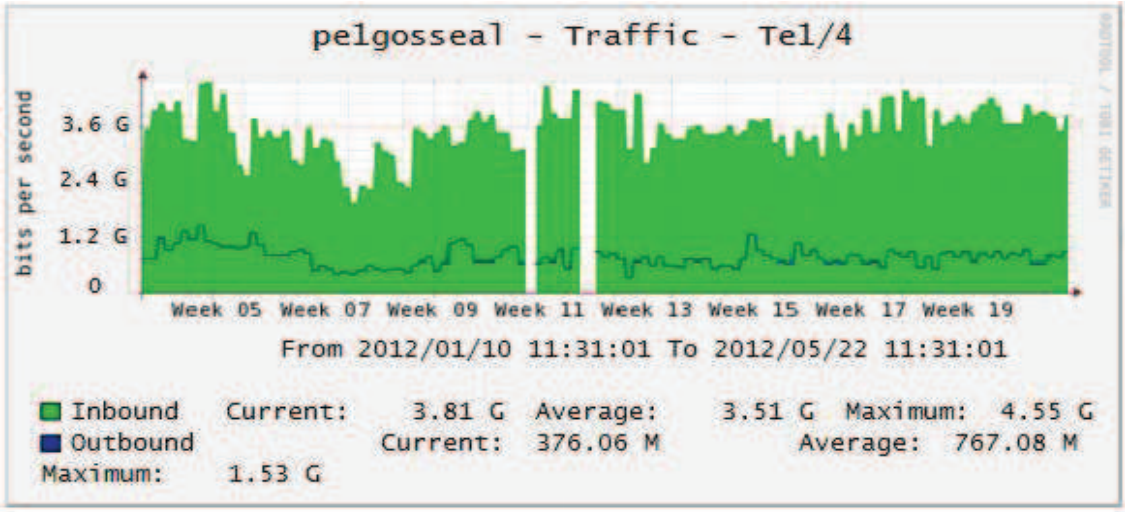


Figura 2.32 Tráfico PE1GOSSEAL, enero - mayo 2012

6. PE1MUROS[18][20]

En la Figura 2.33 se tiene el comportamiento de tráfico del nodo PE1MUROS durante el último año. La información ha tenido crecimiento progresivo a excepción de los picos del mes de enero de 2012 que, según los registros del proveedor para la migración de la red a MPLS, durante este mes el PE1MUROS soportó el tráfico de los clientes de otros nodos para poder migrarlos a MPLS.

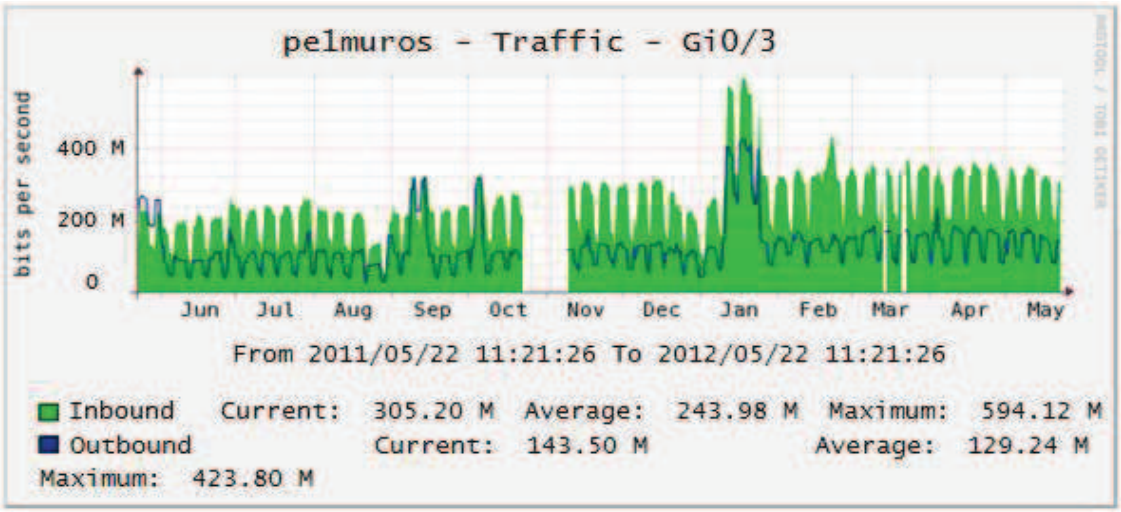


Figura 2.33 Tráfico PE1MUROS, mayo 2011- mayo 2012

Para tener un acercamiento mayor del patrón de tráfico, se utilizará la información de la Figura 2.34 para analizar los requerimientos del diseño.

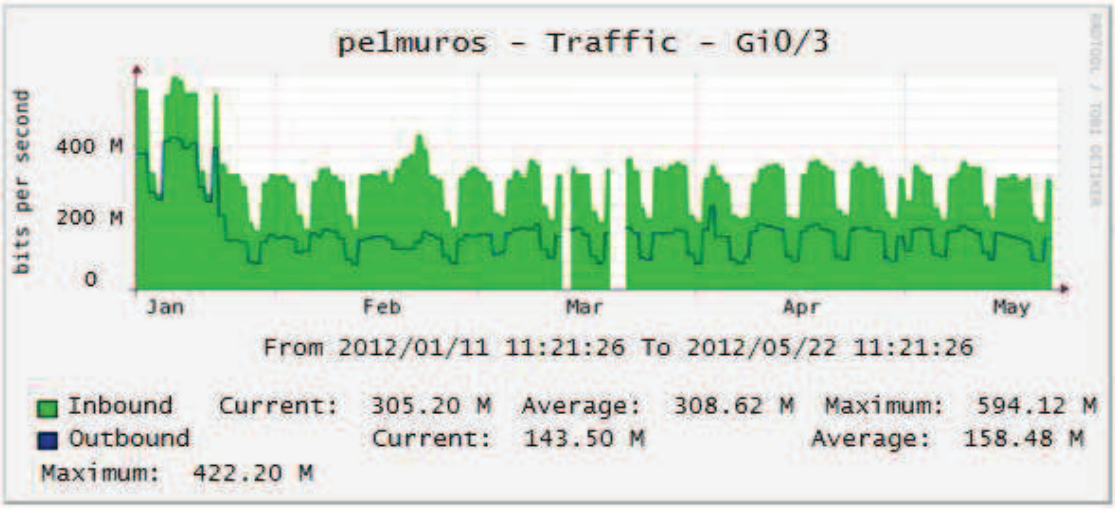


Figura 2.34 Tráfico PE1MUROS, enero - mayo 2012

REQUERIMIENTOS TOTALES DE TRÁFICO DEL MECANISMO 2

Para el rediseño de la infraestructura de red de Telconet S.A. es importante analizar la peor situación y trabajar en base a esta. En las Figuras 2.22 a 2.34 se diferencian tres valores de tráfico: el actual, el promedio y el máximo. El primero refleja el valor de tráfico registrado durante la toma de la muestra; mientras el segundo permite analizar el tráfico promedio que circula por el nodo; pero ninguno de los dos es la peor situación registrada. A diferencia del tercero que indica el máximo pico de tráfico registrado en el tiempo de análisis.

En las Tablas 2.23 y 2.24 se indican los valores máximos de velocidad registrados en las Figuras 2.22 a 2.34, y la proyección de crecimiento al año 2017.

VELOCIDAD DE SUBIDA (Mbps)							
NODOS PE	**2011-2012**	**% Crec.**	**2012-2013**	**2013-2014**	**2014-2015**	**2015-2016**	**2016-2017**
SUR2	741,46	27,13%	942,62	1.198,35	1.523,46	1.936,78	2.462,23
ARMENIA	150,20	27,13%	190,95	242,75	308,61	392,34	498,78
BORROMONI	243,60	27,13%	309,69	393,71	500,52	636,31	808,94
DATACENTER	939,93	27,13%	1.194,93	1.519,12	1.931,26	2.455,20	3.121,30
GOSSEAL	4.550,40	27,13%	5.784,92	7.354,37	9.349,61	11.886,17	15.110,88
MUROS	594,12	27,13%	755,30	960,22	1.220,73	1.551,91	1.972,94
TOTAL	**7.219,71**	**27,13%**	**9.178,42**	**11.668,52**	**14.834,19**	**18.858,71**	**23.975,08**

Tabla 2.23 Valores máximos de las velocidades de subida

VELOCIDAD DE BAJADA (Mbps)							
NODOS PE	**2011-2012**	**% Crec.**	**2012-2013**	**2013-2014**	**2014-2015**	**2015-2016**	**2016-2017**
SUR2	215,54	27,13%	274,02	348,36	442,87	563,02	715,76
ARMENIA	39,95	27,13%	50,79	64,57	82,08	104,35	132,67
BORROMONI	121,55	27,13%	154,53	196,45	249,75	317,50	403,64
DATACENTER	343,26	27,13%	436,39	554,78	705,29	896,63	1.139,89
GOSSEAL	1.536,00	27,13%	1.952,72	2.482,49	3.155,99	4.012,21	5.100,72
MUROS	422,20	27,13%	536,74	682,36	867,49	1.102,83	1.402,03
TOTAL	**2.678,50**	**27,13%**	**3.405,18**	**4.329,00**	**5.503,46**	**6.996,55**	**8.894,71**

Tabla 2.24 Valores máximos de las velocidades de bajada

Considerando que el *Data Center* es un nuevo servicio, el tráfico requerido no está incluido en los requerimientos de las Tablas 2.23 y 2.24. Es por ello que en la

Tabla 2.25, se adicionan 20 Gbps como la capacidad de tráfico estimada del *Data Center.* Obteniendo, según el análisis del mecanismo 2, un total de 44 Gbps para los requerimientos de las velocidades de subida y 25 Gbps para las velocidades de bajada.

	VELOCIDAD DE SUBIDA (Mbps)			VELOCIDAD DE BAJADA (Mbps)		
NODOS PE	**TOTAL 2017**	***DATA CENTER***	**TOTAL**	**TOTAL 2017**	***DATA CENTER***	**TOTAL**
SUR2	2.462,226	20.000,000	2.462,226	715,761	20.000,000	715,761
ARMENIA	498,781		498,781	132,665		132,665
BORROMONI	808,942		808,942	403,641		403,641
DATACENTER	3.121,302		26.891,252	1.139,891		21.139,891
GOSSEAL	15.110,882		15.110,882	5.100,720		5.100,720
MUROS	1.972,942		1.972,942	1.402,034		1.402,034
TOTAL	**23.975,076**	**20.000,000**	**43.975,076**	**5.503,460**	**20.000,000**	**25.503,460**

Tabla 2.25 Requerimiento totales de tráfico del mecanismo 2

2.2.4.3. Resultado del análisis de los mecanismos 1 y 2

En la Tabla 2.26 se presentan los requerimientos de tráfico totales entre los mecanismos 1 y 2. En el primero se analizaron los valores contratados por los clientes y se obtuvieron capacidades mayores que en el mecanismo 2 ya que los clientes no siempre están trabajando a la capacidad que contratan. Mientras el análisis del segundo mecanismo, presenta el uso real de los enlaces y los dispositivos de red.

Para el rediseño se utilizarán los requerimientos obtenidos en el mecanismo 2, debido a que indican las capacidades de tráfico reales que circulan por la red de Telconet S.A.- Quito. Aunque la peor situación se presenta cuando todos los clientes trabajen a su máxima capacidad contratada, como en el mecanismo 1; no se rediseña en base a este análisis porque los costos de cada Mbps serán mayores, al requerir enlaces y equipos más robustos que en definitiva, estarán sobre estimados. Dentro del segundo mecanismo, ya se trabaja con la peor situación de la red cuando se analizan los valores máximos y no los promedios de cada gráfica, obteniendo mejores costos acorde el uso real de la infraestructura de red del proveedor.

	VELOCIDAD DE SUBIDA (Mbps)		VELOCIDAD DE BAJADA (Mbps)	
NODOS PE	**MECANISMO 1**	**MECANISMO 2**	**MECANISMO 1**	**MECANISMO 2**
SUR2	2.818,480	2.462,226	2.818,480	715,761
ARMENIA	744,732	498,781	744,732	132,665
BORROMONI	1.087,516	808,942	1.087,516	403,641
DATACENTER	23.800,494	26.891,252	23.800,494	21.139,891
GOSSEAL	16.546,685	15.110,882	16.546,685	5.100,720
MUROS	2.452,463	1.972,942	2.452,463	1.402,034
TOTAL	**47.450,369**	**43.975,076**	**47.450,369**	**25.503,460**

Tabla 2.26 Requerimientos totales de tráfico

2.2.5. ANÁLISIS DEL USO DEL CPU DE LOS EQUIPOS[19]

Un dispositivo de red debe tener el rendimiento promedio de su CPU en valores menores o iguales al 75%[19] para considerar un estado de funcionamiento óptimo. Si se sobrepasa este valor, es necesario reevaluar el tráfico que circula por el equipo y realizar los cambios necesarios para que evitar que se sobrecargue y presente problemas posteriormente.

En la Tabla 2.27 se detallan de forma resumida, los valores de uso del CPU: actuales, promedios y máximos de los equipos del *backbone* de la ciudad de Quito.

USO DEL CPU			
DISPOSITIVO	**Actual (%)**	**Promedio (%)**	**Máximo (%)**
PGOSSEAL	12	17	42
PDATACENTER	12	14	38
PE1SUR2	12	15	20
PE1ARMENIA	12	12	22
PE1BORROMONI	11	12	17
PE1DATACENTER	24	24	29
PE1GOSSEAL	24	28	32
PE1MUROS	17	18	30
PROMEDIO	**15,5**	**17,5**	**28,75**

Tabla 2.27 Uso del CPU de los equipos del *backbone* de la ciudad de Quito

Los routers LSR son equipos robustos que en promedio tienen 15.5% del uso de su CPU, mientras que los LER varían: con el 28% para el PE1GOSSEAL, el 18% para los PE1MUROS y PE1DATACENTER y el 15% y 12% para los equipos restantes; por lo que, no se deben realizar cambios ni tomar medidas urgentes sobre el funcionamiento de estos dispositivos.

Las gráficas del uso del CPU de los routers LER y LSR de la red de Telconet S.A. Quito, se presentan en el ANEXO C.

REFERENCIAS BIBLIOGRÁFICAS
CAPÍTULO 2

LIBROS Y MANUALES

[1] ANÓNIMO. “Portafolio 2011”. Departamento de Ventas de Telconet S.A.-Quito. Ecuador. 2011.

[2] ALVARADO, Alexandra. “Diagrama Capa 3”. ESP PROY 06 Versión Jul 11. Guayaquil, Ecuador. Julio, 2011.

[3] TIPÁN, Milton. “Diagrama de Red MPLS Quito-Telconet S.A.”. PROY 06 Ver 17-02-2012. Quito, Ecuador. Febrero, 2011.

[4] ANÓNIMO. “Aspectos Básicos de Networking – CCNA 1”. Academia de red Cisco. Módulo cuatro. Cuarta edición. Capítulo 8. Madrid, España. 2007-2008.

[5] ANÓNIMO. “Conmutación y Conexión Inalámbrica de LAN – CCNA 3”. Academia de red Cisco. Módulo cuatro. Cuarta edición. Capítulo 1. Madrid, España. 2007-2008.

[6] ANÓNIMO. “Acceso a la WAN - CCNA 4”. Academia de red Cisco. Módulo cuatro. Cuarta edición. Capítulos 7. Madrid, España. 2007-2008.

[7] JIMÉNEZ, María Soledad MSc. “Comunicación Digital.” Escuela Politécnica Nacional. Quito, Ecuador. Marzo, 2005.

[8] CERVANTES, Javier. “Manual para el tendido de la fibra óptica de Telconet S.A. – parte A”. Quito, Ecuador. Enero 2011.

[9] STALLINGS, William. “Comunicaciones y Redes de Computadores”. Séptima Edición. PRETICE HALL. Madrid, España. 2004.

[10] ANÓNIMO, “Portable Product Sheet – Switch Perf”. *Catalyst Switching Performance.* Cisco *Systems* Inc. 25 de agosto de 2005.

[11] ANÓNIMO. “Nivel de Servicio Garantizado”. Departamento de Ventas de Telconet S.A. sucursal Quito. Ecuador. Agosto, 2011.

[12] ANÓNIMO, “Portable Product Sheet – Router Perf”. *Router Switching Performance in Packets Per Second (PPS).* Cisco *Systems* Inc. 15 de diciembre de 2006.

[13] ANÓNIMO. “Estudio de Mercado de Telconet S.A.”. Departamento de Proyectos de Telconet S.A. Guayaquil, Ecuador. Diciembre, 2010.

[14] ANÓNIMO, “Salidas Internacionales de Telconet Dic-2011”, Departamento de Networking de Telconet S.A. Quito, Ecuador. Diciembre, 2011.

[15] ANÓNIMO. “Ventas Facturadas Telconet S.A. Quito 2007-2011”, Departamento de Facturación de Telconet S.A. Quito, Ecuador. Mayo, 2012.

[16] ANÓNIMO, “Manual de configuración de equipos Streambox”. Departamento IAC de Telconet S.A. Quito, Ecuador. Enero, 2011.

[17] ANÓNIMO. “Documento de Resultados de Búsquedas en SIT - Clientes Activos de Quito”. Departamento IAC de Telconet S.A. Quito, Ecuador. 31 de marzo de 2012.

[18] ANÓNIMO. “Registros de la migración de MPLS de Telconet S.A.- Documento de Resultados de Búsquedas en SIT”. Departamento IAC de Telconet S.A. Quito, Ecuador. 23 de mayo de 2012.

[19] PARNELL, Teré. “Guía de redes de alta velocidad”. Mc Graw Hill. 2da edición. Madrid, España. 2001.

[20] ANÓNIMO. “Registros de las emergencias del Cacti - Documento de Resultados de Búsquedas en SIT”. Departamento NOC de Telconet S.A. Quito, Ecuador. 2010-2012.

DIRECCIONES ELECTRÓNICAS

[21] ANÓNIMO. “StreamBox Rackmount Encoders/Decoders”. 2012. http://www.streambox.com/products/rackmount-encoder-decoder.html

[22] ANÓNIMO. “Telconet S.A. la fibra del Ecuador”. Telconet S.A. Ecuador. 2011.

http://www.telconet.net/?section=home

[23] ANÓNIMO. “Fundamentals of DWDM Technology”. Cisco Systems. http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm_ovr.htm

[24] ANÓNIMO. “Cisco 7609 Chassis”. Cisco Systems, Inc. 1992-2006. http://www.cisco.com/en/US/prod/collateral/routers/ps368/ps367/product_data_sheet09186a0080169ead_ps368_Products_Data_Sheet.html

[25] ANÓNIMO. “Cisco Catalyst 3750 Series Switches”. Cisco Systems, Inc. 1992-2008. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/product_data_sheet0900aecd80371991.pdf

[26] ANÓNIMO. “Cisco Catalyst 3550 Series Intelligent Ethernet Switches”. Cisco Systems, Inc. 1992-2008. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps646/product_data_sheet09186a00800913d7.html

[27] ANÓNIMO. “APC Smart-UPS RT 10000VA 208V”. ErickProtect. Ecuador. http://www.upsecuador.com/equipos-proteccion-electrica-venta-importador-distribuidor-quito-ecuador.php?recordID=123

[28] PALET, Jordi. “Taller de IPv6- Despliegue de IPv6 en Ecuador”. Consulintel Quito- Ecuador, 2 de diciembre de 2011. http://www.6deploy.eu/workshops2/20111202_quito_ecuador/evento_IPv6_SENATEL_v2.pptx.pdf

[29] ANÓNIMO. “Regresión No Lineal”. SEQC. http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CFMQFjAA&url=http%3A%2F%2Fwww.seqc.es%2Fdl.asp%3F175.145.205.255.15.30.27.21.118.133.24.113.255.173.47.5.166.145.65.153.249.7.59.180.219.25.233.119.115.80.195.223.111.197.213.82.70.131.125.124.232.86.165.216.192.188&ei=-

xS4T_KtDYGo8QTGrvycCg&usg=AFQjCNEgnspoWKlfHtUgBlmtjArYu1q5FA&sig2=kPpI3d_iNJQlNUL8JZeA8A

[30] ANÓNIMO. “CEDIA ¿Qué es Cedia?”. http://www.cedia.ec/index.php?option=com_content&view=article&id=1&Itemid=8

[31] MITTAL, Kunal. “Internet Traffic Growth-Analysis of Trends and Predictions”. Paper del Departamento de Administración de la Universidad de Nebraska. Estados Unidos de América. Septiembre, 2011. http://www.kunalmittal.com/includes/Papers/PredictingInternetTrafficGrowth.pdf

[32] ANÓNIMO. “Cisco Catalyst 6500 and 6500-E Series Datasheet”. Cisco Systems, Inc. 2009. http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a00800ff916_ps708_Products_Data_Sheet.html

[33] ANÓNIMO. “Cisco 7200 VXR Series Routers Overview”. Cisco Systems, Inc. 1992-2008. http://www.cisco.com/en/US/prod/collateral/routers/ps341/data_sheet_c78_339749.pdf

CAPÍTULO 3

REDISEÑO DE LA RED MPLS CON SOPORTE PARA IPv6

3.1. INTRODUCCIÓN

MPLS es la tecnología de transporte con mayor aceptación en los proveedores de servicios de telecomunicaciones, gracias a la eficiente conmutación de etiquetas que ofrece; pero tener implementada una red MPLS sin sus principales aplicaciones, es limitarse a explotar sus ventajas.

Telconet S.A. requiere rediseñar su red MPLS ante la implementación del Data Center que incrementará drásticamente su tráfico, así como la demanda de servicios en IPv6 por parte de los clientes, con el fin de brindar servicios de calidad y ser más competitivos en el mercado.

En el presente capítulo se realizará el rediseño de la red MPLS para soportar IPv6 empleando las mejores prácticas de seguridad. En lo referente a las aplicaciones de Calidad de Servicio, se trabajará con la arquitectura Servicios Diferenciados y se determinarán las diferentes CoS en base a los SLA firmados entre el proveedor y sus clientes, se hará uso de Ingeniería de Tráfico para optimizar el uso de los recursos, y las VPN de MPLS en capa 2 y capa 3 entre las sucursales de los clientes, con el fin de mantener garantías de QoS extremo a extremo.

Se seleccionará el mecanismo de transición IPv4/v6 sobre MPLS que mejor cumpla con los requerimientos del diseño y se aplicarán las Mejores Prácticas de Seguridad en IPv6. Se realizarán las recomendaciones de hardware y software, y para los equipos que no soportan IPv6, se analizará la posibilidad de cambiar su hardware y/o software a través de una matriz de decisión comparando tres marcas del mercado, seleccionando aquel equipo o IOS que cumpla con los requerimientos del diseño. Finalmente, se llevará a cabo la estimación de costos de la solución.

3.2. IPv6 SOBRE LA TECNOLOGÍA MPLS[21][22][23][25]

Aun cuando los protocolos IPv4 e IPv6 son incompatibles, las redes IPv4 seguirán coexistiendo con las redes IPv6 gracias a los mecanismos de transición IPv4/IPv6. El objetivo final será desplazar por completo a IPv4, y progresivamente, desplegar a IPv6 en todas las redes empezando por los proveedores de Internet.

Un cambio por completo a IPv6 no es viable en la actualidad debido a que representa altos costos económicos al implicar cambios de hardware y software en todos los dispositivos de la red, por lo cual, se recurre a seleccionar el mecanismo de transición que mejor se acople a los requerimientos de la sucursal Quito de Telconet S.A.

En las secciones 1.3.1, 1.3.2, y 1.1.3 se detallan los fundamentos básicos de los tres principales mecanismos de transición IPv4/IPv6, y son:

- IPv6 sobre Circuitos de Transporte en MPLS
- IPv6 con Túneles en los routers CE
- IPv6 en routers PE (6PE/6VPE)

Además, en la sección 1.3.4 se describen las redes MPLS migradas por completo a IPv6, donde tanto los routers de la nube MPLS como los CE están configurados en IPv6 y no existe ningún otro nodo en IPv4.

Con el objetivo de analizar las ventajas y desventajas de los mecanismos de transición IPv4/IPv6, se presentan las principales características de cada uno de ellos en un cuadro comparativo, a fin de seleccionar aquel que mejor se acople a la red de Telconet S.A.

En la Tabla 3.1 se presentan las características de los mecanismos de transición IPv4/IPv6 como: la escalabilidad, los cambios requeridos, la transparencia al usuario, etc; que fueron detallados en la sección 1.3.

MECANISMOS DE TRANSICIÓN IPv4/IPv6							
Mecanismo	**Descripción**	**Cambios en la red**	**Conexiones *full mesh***	**Dispositivos de doble pila**	**Transparente al usuario**	**IPv6 nativo**	**Escalable**
IPv6 sobre Circuitos de Transporte en MPLS	Uso de circuitos de transporte estáticos. La comunicación entre los CE se realiza sobre enlaces dedicados mediante túneles de capa 2	No modifica las configuraciones de los LSR de la red, pero si de los LER	Si, en los LER	LER	Si	Si	No
IPv6 con Túneles en los routers CE	Implementa túneles de capa 3 configurados en los routers CE IPv6. Es el mecanismo más simple para implementar IPv6 en redes MPLS	No modifica las configuraciones de los LER ni de los LSR. La comunicación se establece entre los CE	Si, entre todos los CE	CE	No	No	No
IPv6 en routers PE (6PE/6VPE)	Utiliza el protocolo MP-BGP para el transporte de paquetes IPv6. Brinda seguridad al implementar VPN de capa 3	No modifica las configuraciones de los LSR de la red MPLS, pero si de los LER	No, utiliza MP-BGP para la comunicación	LER	Si	No, en 6PE Si, en 6VPE	Si
IPv6 sobre una red MPLS/IPv6	Utiliza configuraciones IPv6 en toda la red. En la actualidad es muy costoso.	Si, en toda la red	No	No, a menos que se requiera dar soporte a IPv4	No	Si	Si

Tabla 3.1 Cuadro comparativo de los mecanismos de transición IPv4/IPv6

3.2.1. SELECCIÓN DEL MECANISMO DE TRANSICIÓN IPv4/IPv6[24]

La sucursal de Quito de Telconet S.A. dispone de una red MPLS/IPv4 robusta y se espera que la migración a IPv6, no la debilite. El mecanismo seleccionado debe implicar el menor número de cambios en las configuraciones, los dispositivos y los enlaces, a fin de ahorrar en costos y brindar transparencia a los usuarios de la red. La escalabilidad es otro factor importante porque se espera que el proveedor siga creciendo al ofrecer nuevos servicios.

Un análisis de los mecanismos presentados en la Tabla 3.1 permitió seleccionar a IPv6 en routers PE (6PE/6VPE) como el mecanismo de transición más adecuado para el presente rediseño ya que ofrece: escalabilidad, seguridad con la implementación de las VPN de capa 3, transparencia para el usuario e incluye configuraciones solo en los LER y no en los LSR.

Los mecanismos IPv6 sobre Circuitos de Transporte en MPLS e IPv6 con Túneles en los routers CE no se adaptan a los requerimientos de Telconet S.A. principalmente porque no ofrecen escalabilidad en la red, la cual es crítica para un proveedor de servicios.

3.2.2. MECANISMO: IPv6 EN ROUTERS PE (6PE/6VPE)[21][22][24][25]

6PE y 6VPE son mecanismos escalables que requieren configuraciones solo en los routers LER de la red MPLS. Manejan el protocolo MP-BGP para brindar soporte a IPv4 e IPv6.

6PE permite que los dominios IPv6 se comuniquen a través de la nube MPLS/IPv4, manejando una tabla de enrutamiento común para todos los dispositivos. Sin embargo, si se transporta la información a través de una VPN de capa 3, este mecanismo se conoce como 6VPE.

6VPE permite que los dominios IPv6 se comuniquen usando tablas de enrutamiento separadas lógicamente para cada VPN de capa 3, ofrece mayor seguridad de la información y transporte de paquetes con IPv6 nativo.

En el presente diseño se utiliza 6PE para establecer la comunicación y poder monitorear los dispositivos de la red de Telconet S.A. que manejen IPv6; y 6VPE para la comunicación entre las sucursales de los clientes IPv6, a fin de brindar seguridad en el transporte de la información.

3.3. REDES PRIVADAS VIRTUALES (VPN) EN LA TECNOLOGÍA MPLS[16][41]

La comunicación entre dos sucursales de un cliente resulta costosa si este la realiza a través de una infraestructura propia. Por el contrario, las VPN en una red MPLS son soluciones mucho más eficientes y económicas que permiten comunicar dos o más localidades remotas de un cliente.

El presente diseño de la red MPLS de Telconet S.A.-Quito tiene por objetivo implementar un esquema que disponga de las VPN de capa 2 punto a punto (VPWS) y las VPN de capa 3, para comunicar las redes de los clientes entre puntos distantes.

3.3.1. LAS VPN DE MPLS DE CAPA 2 (VPWS)

Las VPWS se configuran para transportar tramas *Ethernet* entre dos puntos distantes de las redes de los clientes, dejando el direccionamiento a cargo de los routers CE.

En el presente diseño no se define ningún protocolo adicional a LDP que se encargue de la distribución de las etiquetas en la red, debido a que Telconet S.A. solo brinda el transporte de la información y no es responsable del enrutamiento.

Se utilizará la encapsulación MPLS para el establecimiento de los *pseudowires* y un valor de circuito virtual (VC) que lo defina. En la Tabla 3.2 se presentan la numeración de los VC de acuerdo al tipo de cliente que lo contrate.

NUMERACIÓN DE LAS VPN DE CAPA 2	
Tipos de Clientes	**Circuitos Virtuales**
corporativos VIP	1-500
corporativos	501-1.000

Tabla 3.2 Numeración de las VPN de capa 2

El número de las VPWS a configurar en la red depende de la demanda que tenga este servicio por parte de los clientes de Telconet S.A. En la Figura 3.1 se presenta un esquema modelo para su implementación entre dos LER de la red MPLS.

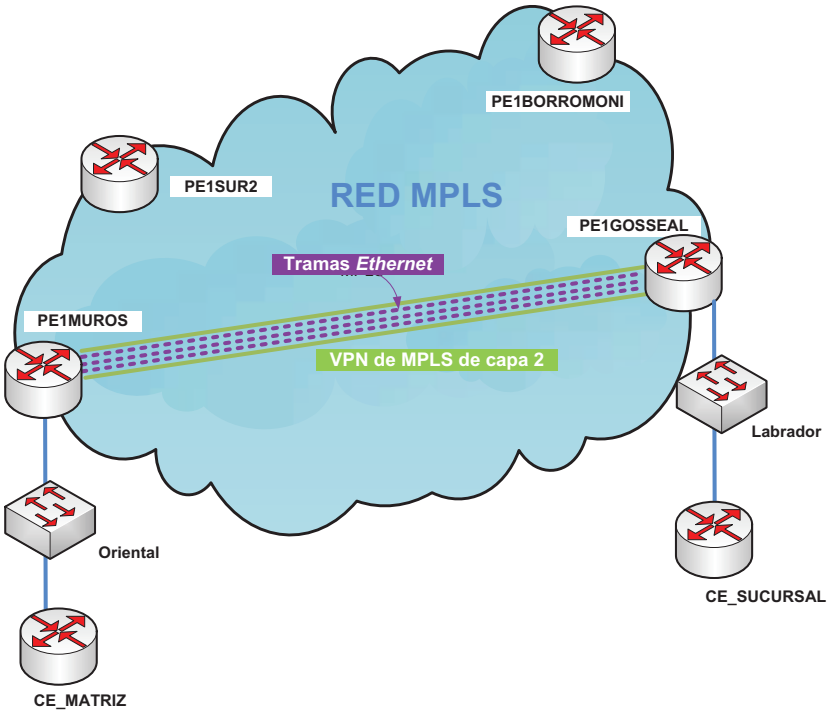


Figura 3.1 VPN de capa 2 punto a punto

Durante el transporte de la información, los routers LER tendrán conocimiento de las direcciones físicas de los routers utilizados por los clientes. Mientras para los

CEs, la VPN es transparente porque solo conocen las direcciones físicas y lógicas del CE remoto.

3.3.2. LAS VPN DE MPLS DE CAPA 3

El presente diseño tiene por objetivo implementar un esquema que disponga de las VPN de capa 3 para comunicar redes en las dos versiones de IP: IPv4 e IPv6. Estas VPN manejan tablas de enrutamiento independientes de la tabla de enrutamiento general, por lo cual permiten brindar mayor seguridad.

Para la distribución de la información de enrutamiento, las VPN de capa 3 trabajan con el protocolo BGP que mediante la creación de las comunidades de destino de ruta (RT), permite definir las sucursales de los clientes que pueden importar y/o exportar esta información.

BGP establece un prefijo de 64 bits llamado *Route Distinguisher* (RD) como el identificador de la tabla VRF, que se agrega a cada dirección IP para hacerla única en la red. En IPv4, la dirección única se conoce como VPNv4 y estará formada por 96 bits; mientras en IPv6, la dirección se conoce como VPNv6 y tendrá 192 bits.

En el rediseño de la red MPLS, se utilizará la versión más reciente del protocolo BGP: BGPv4. Se definirán los valores RD y RT según el formato $AS{:}\,nn$, donde AS es el sistema autónomo de Telconet S.A. registrado con el valor 27947, y nn es un número decimal de hasta 32 bits que seguirá el orden mostrado en la Tabla 3.3.

NUMERACIÓN DE LAS VPN DE CAPA 3		
Tipo de Clientes	**Rango Normal**	**Rango Extendido**
corporativos VIP	1-500	1.001 - 2’000.000
Corporativos	501-1.000	2’000.001 - 4.294’967.296

Tabla 3.3 Numeración de las VPN de capa 3

Las VPN de capa 3 estarán definidas en mayúsculas con el nombre del cliente al que representan. Si se emplean más de una palabra, se utilizarán guiones bajos (_) para separarlas. Por ejemplo, BANCO_DE_GUAYAQUIL.

De la misma manera que las VPWS, la configuración de las VPN de capa 3 dependerá de la demanda de servicio por parte de los clientes de Telconet S.A. En la Figura 3.2 se presenta un esquema modelo para su implementación.

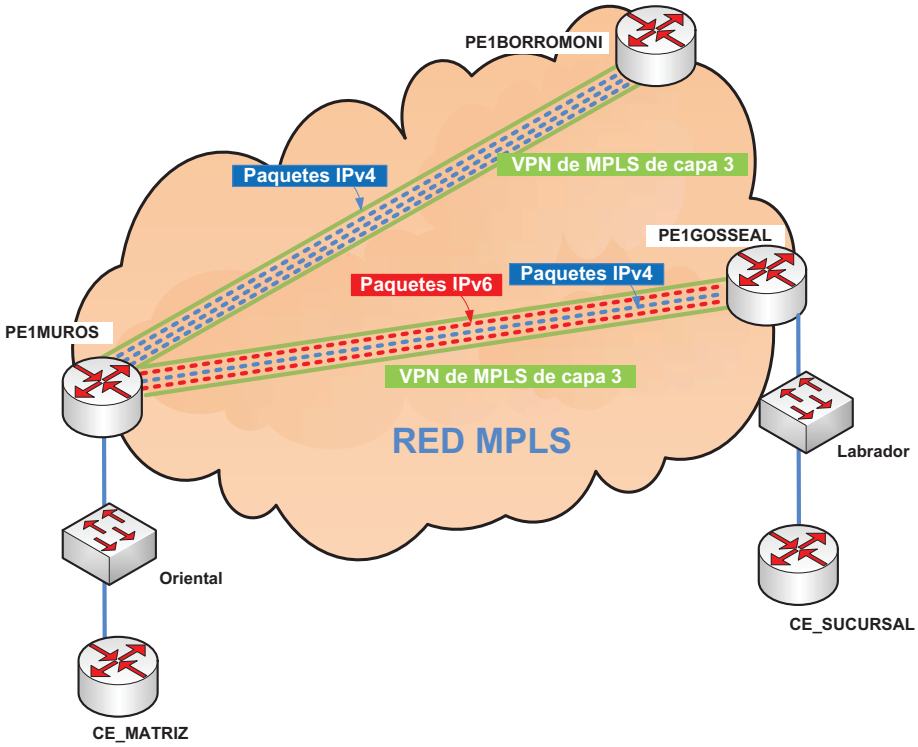


Figura 3.2 VPN de capa 3 en IPv4 e IPv6

Como se observa en la Figura 3.2, las VPN pueden transportar solo paquetes en IPv4, o en IPv4 e IPv6 simultáneamente. Cada cliente del servicio de transmisión de datos, tendrá su propia VPN de capa 3, sea en IPv4 o en IPv6. Mientras, para el servicio de Internet, se tendrá una VRF llamada INTERNET que soportará el tráfico en IPv4 e IPv6 simultáneamente.

3.4. CALIDAD DE SERVICIO (QoS) EN LA TECNOLOGÍA MPLS

Telconet S.A. requiere un diseño de Calidad de Servicio a fin de poner brindar tratamiento diferencial a las clases de tráfico, y en caso de congestión, garantizar prioridad a las aplicaciones más críticas como la voz y el vídeo.

Telconet S.A.-Quito maneja la tecnología MPLS en la capa núcleo de su red, y *Ethernet* en las capas distribución y acceso, por lo que se debe trabajar con un esquema de Calidad de Servicio que integre estas dos tecnologías.

Las diferentes Clases de Servicios (CoS) se especificarán de acuerdo a los parámetros establecidos en los Acuerdos de Nivel de Servicio (SLA) otorgados por Telconet S.A. con el objetivo de determinar el tratamiento que recibirán los paquetes durante su transmisión por la red. Las funciones de QoS son diferentes para los routers MPLS: los LER se encargan de la clasificación y el marcaje de los paquetes; mientras, los LSR trabajan en la gestión y la evasión de la congestión mediante la definición de políticas.

3.4.1. REQUERIMIENTOS DE QOS Y PARÁMETROS DE LOS SLA DE TELCONET S.A.[3][10]

En la red de Telconet S.A. se tienen aplicaciones que necesitan un trato preferencial. El departamento Networking solicita que el tráfico crítico, como la voz sobre IP y el vídeo, reciba un nivel de prioridad mayor que el resto de aplicaciones; y, en caso de congestión, el tráfico de los clientes corporativos VIP tengan prioridad sobre el de los clientes Corporativos. A continuación, se detallan los requerimientos de Calidad de Servicio:

- Se espera que la red de Telconet S.A. pueda transportar los paquetes de tráfico diferenciados, y en caso de congestión, dar prioridad al tráfico más crítico como la voz y el vídeo.
- Brindar, mientras sea posible, Calidad de Servicio de extremo a extremo.

- Garantizar alta prioridad al tráfico de voz, cumpliendo con los parámetros que se muestran en la Tabla 3.4.
- Brindar alta prioridad al tráfico de vídeo cumpliendo los parámetros mostrados en la Tabla 3.4.
- Garantizar que el tráfico de los clientes corporativos VIP tenga prioridad sobre el tráfico de los clientes Corporativos.

PARÁMETROS COMPROMETIDOS		
Parámetros	**Voz**	**Vídeo**
Retardo	≤150 ms	=150 ms
Jitter	≤30 ms	=30 ms
Paquetes perdidos	≤1%	=1%

3.4.1.1.

Tabla 3.4 Parámetros comprometidos de la voz y el vídeo

Fuente: [1], páginas 43 y 44

El estudio de los parámetros comprometidos en los SLA de Telconet S.A. sale del alcance de este proyecto, porque amerita un análisis profundo de las aplicaciones que circulan por la red y un estudio de mercado que determine el porcentaje de uso de cada una de ellas. El objetivo de este proyecto es dar a conocer las configuraciones de la Calidad de Servicio en redes MPLS que permitan transportar paquetes IPv4 e IPv6 con diferentes tratamientos, por lo que se recurrirá al estudio de las aplicaciones presentado en [10].

Las Clases de Servicios para Telconet S.A.-Quito serán designadas de la siguiente manera:

1. La clase *Routing* incluye los protocolos de enrutamiento usados en la red, a fin de garantizar que las sesiones que estos protocolos establecen se mantengan activas aun cuando exista congestión.
2. La clase *Platinum* se orienta a la aplicación más crítica: la voz; a fin de cumplir con los parámetros establecidos en la Tabla 3.4. No se requiere un gran ancho de banda porque los paquetes de voz son pequeños.

3. La clase *Gold* incluye las aplicaciones de vídeo a fin de garantizar las exigencias establecidas en la Tabla 3.4.
4. La clase *Silver* se orienta al tráfico de los clientes corporativos VIP con altas prestaciones de acceso.
5. La clase *Bronze* se orienta al tráfico de los clientes corporativos para que tengan prioridad frente al tráfico *Best-Effort.*
6. La clase *Best-Effort* no recibe ningún trato preferencial e incluye todas las aplicaciones que no han sido marcadas en las clases anteriores.

3.4.2. DESIGNACIÓN DE LOS PHB

Una vez definidas las Clases de Servicios y las aplicaciones que pertenecen a cada una de ellas, es necesario asociar las CoS a uno o varios *Per-Hop Behaviors* (PHB), a fin de determinar el tratamiento que recibirán los paquetes durante su retransmisión en la red.

En la Tabla 3.5 se presenta los PHB designados a cada CoS, las aplicaciones y los porcentajes de anchos de banda requeridos por el departamento *Networking* de Telconet S.A.

***PER-HOP BEHAVIORS* (PHB)**			
CoS	**PHB**	**APLICACIONES**	**ANCHO DE BANDA**
Routing	CS7, CS6	Protocolos de enrutamiento: OSPF, BGP y LDP	5% prioritario
Platinum	EF	Voz	10% prioritario
Gold	AF41	Videoconferencia	15%
Silver	AF31	Datos de los clientes corporativos VIP	35%
Bronze	AF21	Datos de los clientes Corporativos	30%
Best-Effort	0	Protocolos: SMTP, ICMP, HTTP, DNS, etc.	-

Tabla 3.5 *Per-Hop Behaviors*

3.4.3. MAPA DE CORRESPONDENCIAS DSCP - EXP

Cuando un paquete ingresa a la red MPLS, el router LER debe asociar el campo Tipo de Servicio en IPv4, o Clase de Tráfico en IPv6 con el campo EXP de la cabecera MPLS mediante el mapa de correspondencias DSCP - EXP; a fin de enviar la información de Calidad de Servicio que requieren los paquetes durante su retransmisión en la red.

En la Tabla 3.6 se presentan el mapa de correspondencias DSCP – EXP definido para las clases del presente diseño.

MAPAS DE CORRESPONDENCIAS				
CoS	**PHB**	**Valor DSCP**	**Valor ToS**	**Valor EXP**
Routing	CS7	56	224	6
	CS6	48	192	
Platinum	EF	46	184	5
Gold	AF41	34	136	4
Silver	AF31	26	104	3
Bronze	AF21	18	72	2
Best-Effort	0	0	0	0

Tabla 3.6 Mapas de correspondencias

3.4.4. DEFINICIÓN DE LA POLÍTICA PARA LIMITAR LA CAPACIDAD DE TRÁFICO

Cuando un cliente contrata una cierta capacidad de tráfico, el proveedor debe controlar las velocidades de envío y recepción máximas con el fin de cumplir con los parámetros firmados en el SLA. En el presente diseño, se utilizará el mecanismo traffic policing para limitar el tráfico de los clientes.

Las políticas serán configuradas para cada cliente en particular, debido a que las capacidades contratadas son diferentes entre un cliente y otro. Se hará referencia a la clase por defecto con el fin de abarcar todo el tráfico que atraviese la interfaz, se configurará el valor CIR contratado y se establecerán las acciones de descarte.

Finalmente, se asociarán las políticas a las interfaces y/o subinterfaces de salida de los routers CE hacia los LER.

3.4.5. DEFINICIÓN DE LA POLÍTICA PARA DEFINIR EL MAPA DE CORRESPONDENCIAS ENTRE LOS CAMPOS DSCP Y EXP DEL PAQUETE

Para poder clasificar un paquete y asignarlo a una clase en especial, se debe marcar el campo de EXP de la cabecera MPLS con el PHB respectivo, a fin de que cada dispositivo en la red pueda identificarlo y asociarlo a una clase.

La clasificación de los paquetes IP es responsabilidad exclusiva de los LER ya que están ubicados entre las dos tecnologías: MPLS e IP. Cada router debe tener configuradas las clases de la Tabla 3.5 con los valores DSCP respectivos, para que cuando un paquete ingrese a la red MPLS, se pueda asociar su campo Tipo de Servicio en IPv4, o Clase de Tráfico en IPv6, con uno de los valores DSCP configurados e identificar la clase a la que pertenece. Por ejemplo, si un paquete IPv4 tiene marcado el valor DSCP 34, pertenecerá a la clase Gold.

Posteriormente, se crea una política que marque el campo EXP de cada paquete clasificado, en una de las seis CoS configuradas en base a los criterios de correspondencia presentados en la Tabla 3.6. Por ejemplo, los paquetes de la clase Gold, tendrán el valor 4 en su campo EXP. Finalmente, se asigna la política de marcaje a la entrada de la interfaz o subinterfaz del router, para que la clasificación se realice durante el ingreso de los paquetes a la red MPLS.

3.4.6. DEFINICIÓN DE LAS POLÍTICAS PARA EL MANEJO DE LA CONGESTIÓN DE LA CAPA NÚCLEO[3]

En la capa de núcleo, las políticas se configuran a la salida de las interfaces o subinterfaces de los LER y LSR, con el objetivo de brindar tratamientos diferenciales a los paquetes de cada clase durante su paso por la red MPLS.

Las políticas tienen los mismos parámetros de asignación de recursos configurados en los routers LER y LSR, pero se diferencian por las CoS que utilizan. Los LER trabajan con las mismas clases definidas en la sección 3.4.1.5, ya que deben clasificar los paquetes según el campo Tipo de Servicio en IPv4 o Clase de Tráfico en IPv6. Mientras, los LSR deben configurar las CoS de la Tabla 3.6 con sus valores EXP respectivos, para clasificar los paquetes en base al campo EXP de la misma manera que se hizo en los LER. Es decir, si un paquete tiene el valor de 4 en el campo EXP, se lo asociará a la clase *Gold*.

Para asegurar las mejores características de envío en caso de congestión, se definen diferentes tratamientos de ancho de banda y colas en cada CoS configurada en la política. Como mecanismo de encolamiento se ha seleccionado LLQ, gracias a que garantiza una cola prioritaria y varias colas con prioridades personalizadas. Mientras como mecanismo de evasión de la congestión, se ha seleccionado WRED porque permite descartar los paquetes probabilísticamente evitando en lo posible, que las colas se llenen.

Los parámetros definidos en cada CoS de la política son:

- Clase *Routing*

  Para esta clase se tiene un ancho de banda prioritario del 5%. Es decir que en caso de congestión, se garantiza enviar máximo el 5% de tráfico perteneciente a la clase *Routing*. LLQ permite que la clase prioritaria tenga la mayor preferencia en la red, pero limita su ancho de banda para evitar que el resto de CoS se queden sin recursos.
- Clase *Platinum*

  Esta clase también es prioritaria como la clase *Routing.* Tiene un ancho de banda del 10% por lo que en caso de congestión, se enviará máximo el 10% del tráfico de la clase *Platinum.*
- Clase *Gold*

  A diferencia de las dos clases anteriores, esta tiene un ancho de banda garantizado del 15%, es decir que en caso de congestión se envía al menos

el 15% de tráfico de la clase *Gold*; pero si a una de las clases restantes les sobra ancho de banda, esta clase puede aumentar su capacidad de envío. Además, tiene una cola de 100 paquetes que evita el descarte automático de los mismos al ponerlos en espera.

- Clase *Silver*

  Tiene un ancho de banda garantizado del 35% y una cola de 100 paquetes como la clase *Gold*.

- Clase *Bronze*

  Esta clase tiene un ancho de banda garantizado del 30%, una cola de 100 paquetes y un 40% de ancho de banda con el mecanismo *traffic shaping.* Cuando exista congestión en la red, se enviará al menos el 30% de tráfico perteneciente a la clase *Bronze*; pero a diferencia de las clases *Gold* y *Silver,* se podrá aumentar su capacidad de envío hasta un 40% ya que *traffic shaping* limita el umbral máximo para evitar que la CoS se consuma todo el tráfico restante.

- Clase *Default*

  En esta clase no se garantiza ningún tratamiento preferencial por lo que el tráfico perteneciente a ésta, utilizará el ancho de banda que sobra en la red con un umbral máximo del 50%. Como mecanismo de evasión de la congestión, se implementará WRED para descartar los paquetes en base al valor DSCP configurado.

3.4.7. MANEJO DE LA CONGESTIÓN EN LAS CAPAS DISTRIBUCIÓN Y ACCESO

La Calidad de Servicio debe estar implementada, en lo posible, de extremo a extremo de la red, por lo que los dispositivos de las capas distribución y acceso deben agrupar los paquetes y reenviarlos según el PHB que les corresponde. En estos dispositivos, no se pueden configurar las políticas detalladas en las secciones 3.4.1.4, 3.4.1.5 y 3.4.1.6, debido a que son equipos de capa 2 que no tienen soporte avanzado de QoS.

Las configuraciones de QoS se centrarán en confiar en los valores marcados previamente en el subcampo DSCP, y reenviar los paquetes al siguiente nodo con el PHB respectivo. Mientras que como mecanismo de encolamiento, se ha seleccionado SRR por la facilidad que ofrece en el manejo de las colas con la asignación de pesos.

El número de colas y umbrales de descarte depende del modelo del dispositivo que se utilice. Por ejemplo, los switches Catalyst tienen diferentes características entre un modelo y otro, como se muestra en la Tabla 3.7. Un switch 3650 dispone de: 4 colas de salida con 3 umbrales de descarte cada una (4Q3T), y 2 colas de entrada que pueden dividirse en: 1 prioritaria y 1 normal, con 3 umbrales de descarte cada una (2Q3T o 1P1Q3T).

ENCOLAMIENTO EN LOS SWITCHES CATALYST					
SERIE	**6500**	**4000**	**3750, 2970 & 3650**	**3550**	**2950**
COLAS DE TRANSMISIÓN	2Q2T 1P2Q2T 1P3Q1T 1P2Q1T	1P3Q2T 4Q2T	4Q3T	1P3Q2T 4Q2T	1P3Q 4Q
COLAS DE RECEPCIÓN	1Q4T 1P1Q4T 1P1Q 1P1Q1T	NO	1P1Q3T 2Q3T	NO	NO

Tabla 3.7 Encolamiento de los switches Catalyst
Fuente: [1], volumen 2, página 88

3.5. INGENIERÍA DE TRÁFICO EN LA TECNOLOGÍA MPLS[11][12][20]

La sucursal Quito de Telconet S.A. requiere un esquema de Ingeniería de Tráfico (TE), a fin de mejorar el *performance* de su red MPLS mediante el control de tráfico y la optimización del uso de los recursos. Se emplean túneles TE que manipulan los flujos de tráfico y permiten que las trayectorias sean más flexibles.

Este diseño se basará en analizar las prestaciones que TE ofrece en redes MPLS, como son: el balanceo de carga y la redundancia de enlaces; y en seleccionar los protocolos de enrutamiento y señalización necesarios para la implementación de TE.

3.5.1. BALANCEO DE CARGA

Para la implementación de Ingeniería de Tráfico con balanceo de carga, es necesario establecer túneles TE con rutas explícitas o dinámicas entre los routers LER de la red MPLS. Estos túneles son conexiones unidireccionales seguras por lo que, para una comunicación *full dúplex* se deben configurar dos de ellos, uno en cada sentido.

En el presente rediseño de la red MPLS de Telconet S.A., se utilizarán dos tipos de túneles que se diferencian en el mecanismo para seleccionar las rutas, los túneles explícitos y dinámicos. Un túnel explícito se caracteriza porque el administrador de la red debe configurar los saltos por donde el flujo de tráfico atravesará la red siguiendo una lista de direcciones IP; mientras un túnel dinámico, se obtiene a partir del protocolo IGP configurado en los routers que determine el mejor camino hacia el destino.

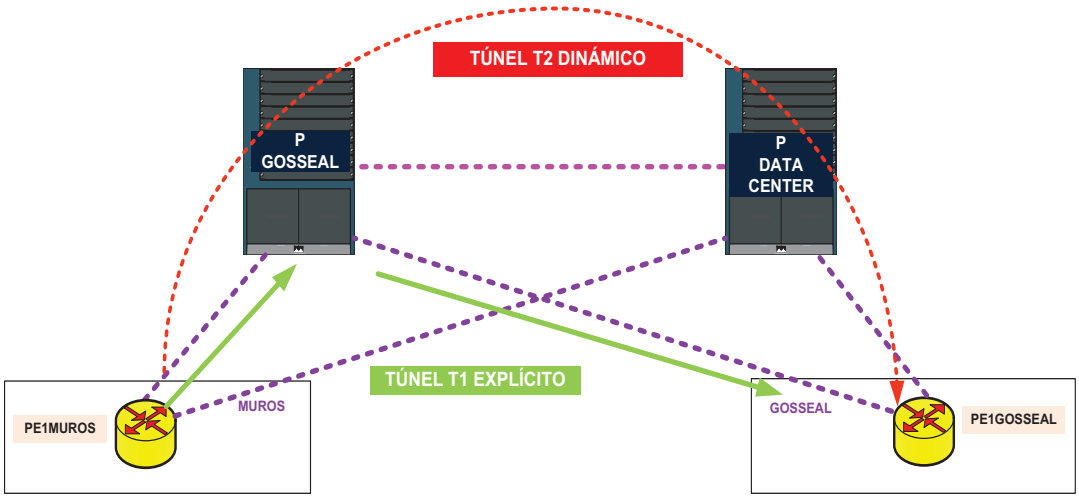


Figura 3.3 Esquema de balanceo de carga

Se establecerán dos túneles: explícito y dinámico en cada sentido de las sesiones BGP configuradas, a fin de poder balancear el tráfico a través de ellos. En la Figura 3.3 se presenta un esquema modelo para la implementación de Ingeniería de Tráfico con balanceo de carga.

3.5.2. REDUNDANCIA DE ENLACES

Otra de las prestaciones de la Ingeniería de Tráfico es garantizar la disponibilidad de una trayectoria en la red MPLS, logrando reenrutar el tráfico por un camino preestablecido. Cuando un enlace falla, este estará protegido por una ruta explícita secundaria configurada previamente por el administrador de la red. El tiempo de conmutación será mucho menor que si se establece dinámicamente por el protocolo IGP a cargo.

En el presente rediseño de la red MPLS de Telconet S.A., se plantea la creación de túneles redundantes frente a fallas en los enlaces de la red. El mecanismo de restauración se llama *Fast-ReRoute* (FRR) que permite la conmutación automática al túnel de *backup* de un enlace determinado. Estos túneles deben estar previamente configurados mediante rutas explícitas, de tal manera que el administrador de la red, los conmute por un enlace secundario.

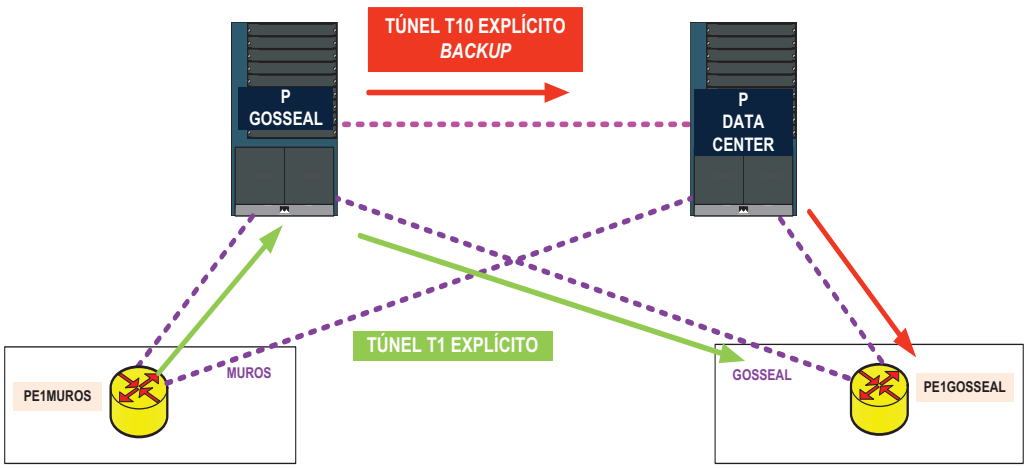


Figura 3.4 Esquema de redundancia de enlaces

En la red de Telconet S.A. se protegerán los enlaces exclusivamente de la red MPLS. Por ejemplo, si en la Figura 3.4 se requiere proteger el enlace PGOSSEAL-PE1GOSSEAL, se establece el túnel 10 de respaldo en el PGOSSEAL, a fin de que se reenrute el tráfico por el router PDATACENTER cuando exista una falla en el enlace protegido.

3.5.3. PROTOCOLO DE ENRUTAMIENTO PARA REDES MPLS CON TE

Los protocolos estado de enlace presentan grandes ventajas sobre todo para redes grandes donde se necesita convergencia rápida y alta escalabilidad. MPLS sugiere solo dos protocolos de enrutamiento para brindar Ingeniería de Tráfico y son: OSPF e IS-IS.

En la Tabla 3.8 se presenta un cuadro comparativo entre los protocolos: OSPF e IS-IS mostrando las principales características de cada uno.

PROTOCOLOS DE ENRUTAMIENTO ESTADO DE ENLACE		
CARACTERÍSTICAS	**OSPF**	**IS-IS**
Soporte de direccionamiento sin clase	Si	Si
Implementa el Algoritmo Dijkstra	Si	Si
Autenticación de origen	Si	Si
Ampliamente difundido	Si	No
Convergencia	Alta	Alta
Tamaño de red	Grande	Grande
Distancia administrativa	110	115
División de la red	Área por interfaces. Un router puede pertenecer a múltiples áreas	Área por router. Un router solo pertenece a un área
Soporte para IPv6	Versión OSPFv3	Versión original de IS-IS
Desarrollo y RFC definido	Estandarizado por la IETF en el RFC 1247	Desarrollado por DEC y adoptado por la ISO en el RFC 1142

Tabla 3.8 Cuadro comparativo OSPF e IS-IS

Fuente: [4]

Según las características mostradas en la Tabla 3.8, se utilizará el protocolo OSPF, debido a que presenta gran flexibilidad al estar estandarizado por la IETF, tiene soporte para IPv6, VLSM, autenticación, múltiples áreas, y sobre todo, porque está ampliamente difundido en el país.

3.5.4. PROTOCOLO DE SEÑALIZACIÓN PARA REDES MPLS CON TE

Los protocolos de señalización que soportan Ingeniería de Tráfico en redes MPLS son: RSVP-TE y CR-LDP. En la Tabla 3.9 se presenta un cuadro comparativo con las principales características de cada uno.

PROTOCOLOS DE SEÑALIZACIÓN PARA TE		
CARACTERÍSTICAS	**RSVP-TE**	**CR-LDP**
Protocolo original	RSVP	LDP
Selección de los LSP	Mediante enrutamiento explícito	Mediante enrutamiento explícito
Comunicación entre pares LSR	Mediante UDP o datagramas IP	Mediante sesiones TCP con los CR-LSP
Mensajes	*Path y Resv*	*Discovery, session, advertisement y notification*
Balanceo de carga	Si	Si
Reenrutamiento de túneles	Si	Si
Protección de enlaces	Si	Si
Observaciones	Reserva el ancho de banda necesario para una clase, por lo que requiere un protocolo de distribución de etiquetas como LDP	No puede coexistir con LDP ya que CR-LDP distribuye las etiquetas MPLS

Tabla 3.9 Cuadro comparativo RSVP-TE y CR-LDP

Fuente: [4]

Tomando en consideración las características mostradas en la Tabla 3.9, se utilizará RSVP-TE como el protocolo de señalización del presente diseño, debido a que soporta balanceo de carga, reenrutamiento de túneles y protección de enlaces sin tener que modificar al protocolo LDP sino con una implementación sencilla de comandos.

3.6. MEJORES PRÁCTICAS DE SEGURIDAD EN IPv6

Telconet S.A. requiere definir un sistema de seguridad a fin de minimizar las amenazas que atenten contra la confidencialidad, la integridad y la disponibilidad de la información que maneja la empresa, así como prevenir los posibles ataques.

Las redes que manejan los protocolos IPv4 e IPv6 simultáneamente pueden ser víctimas de los ataques provenientes de cualquiera de estos dos protocolos. Es por ello que, si se establece una política de seguridad para IPv4, es necesario analizar una similar para IPv6, a fin de garantizar que la red esté completamente protegida.

En el presente diseño se analizarán las Mejores Prácticas de Seguridad en IPv6 detallando tres de ellas en las secciones 3.6.1, 3.6.2 y 3.6.3:

3.6.1. VLAN

Las VLAN son la manera más sencilla de brindar seguridad en capa 2, ya que permiten dividir la red en segmentos más pequeños independientes lógicamente. Transportan tramas *Ethernet* al ser soluciones de capa 2 y permiten el traslado físico de los equipos sin requerir cambios en las direcciones IP.

Para el rediseño de la red de Telconet S.A., se crearán las VLAN según el tipo de cliente. La VLAN nativa y administrativa no será la configurada por defecto (VLAN 1) sino que se cambiarán por la VLAN 129[34].

La encapsulación de los enlaces troncales se configurará con el protocolo IEEE 802.1Q[35] que permite compartir un medio físico, a varias redes, sin que estas presenten problemas. Así, las primeras interfaces del dispositivo y/o aquellas que

[34] En la implementación de la red de Telconet S.A., el valor de la VLAN nativa y administrativa será diferente de 129 ya que por seguridad, se debe establecer un valor que sea de conocimiento solo del personal del proveedor.

[35] Para mayor información de los protocolos de encapsulamiento troncal se recomienda revisar la referencia [7].

sean las más robustas, se configurarán como enlaces troncales 802.1Q en la VLAN nativa 129. Como medida de seguridad, es importante que estos enlaces permitan solo las VLAN configuradas en la red y no todas por defecto.

3.6.1.1. Definición de las VLAN

La definición de las VLAN será por clientes con una numeración que permita, al personal técnico de Telconet S.A., diferenciar el tipo de cliente al que al que está asociada la VLAN. La numeración seguirá el orden mostrado en la Tabla 3.10:

NUMERACIÓN DE LAS VLAN		
Rango	**Normal**	**Extendido**
Clientes corporativos VIP	2-500 (excepto la VLAN 129)	1006-2000
Clientes corporativos	501-1001	2001-4094

Tabla 3.10 Numeración de las VLAN

Las VLAN: 1, 1002, 1003, 1004 y 1005[36] no se pueden renombrar ni borrar por lo que estarán creadas por defecto. Los clientes corporativos VIP tendrán los rangos: 2-500 con excepción de la VLAN nativa/administrativa y 1006-2000; mientras, los corporativos pertenecerán a: 5001-1001 y 2001-4094.

El formato de los nombres de las VLAN estarán conformados por el nombre del cliente en mayúsculas y separadas las palabras por un guión bajo (_), por ejemplo: SUPERMAXI_LA_FAVORITA.

3.6.1.2. Definición de la VLAN de administración

La VLAN de administración será la 129 y estará definida por la dirección IP del dispositivo. El direccionamiento puede ser en IPv4 y/o en IPv6, siempre que el dispositivo lo soporte.

[36] Las VLAN configuradas por defecto en un switch Cisco son: la VLAN 1, definida como la VLAN nativa y administrativa por defecto del dispositivo; las VLAN 1002 y 1004 utilizadas en interfaces FDDI; y las VLAN 1003 y 1005 utilizadas en interfaces *token ring*.

Por ejemplo, para los dispositivos Catalyst Cisco se debe configurar previamente la plantilla de doble pila con el comando “sdm prefer dual-ipv4-and-ipv6 default”. El modelo de switch 3550 no soporta esta plantilla aun cuando soporta el comando IPv6, por lo que se debe configurar en modelos superiores como el switch 3560.

3.6.1.3. Definición de la puerta de salida por defecto

La puerta de salida por defecto será configurada con direcciones IPv4 o IPv6 según se requiera. En IPv4 existe el comando “ip default-gateway” mientras en IPv6, se debe crear una ruta por defecto para definir la puerta de salida con el comando “ipv6 route ::0/0”, ya que no existe un comando como en IPv4.

3.6.2. LISTAS DE CONTROL DE ACCESO EN IPv6 (ACL)[9]

Las ACL son los mecanismos más comunes para brindar seguridad a una red ya que permiten o deniegan el paso del tráfico según: las direcciones IP de origen y destino, los protocolos de capa superiores y los puertos configurados.

Para este proyecto se crearán las ACL en IPv4 e IPv6, a fin de limitar el tráfico según las dos versiones de IP y conocer las diferencias entre las ACL en IPv4 y en IPv6.

Las ACL en IPv4 serán: nombradas y numeradas. Las nombradas utilizarán como formato: la palabra en mayúsculas ACL seguida de la función para la cual están siendo creadas. En caso de que se requiera más de una palabra, se separarán mediante guiones bajos (_).

Por ejemplo, “ACLGESTION_DE_LA_RED_MPLS”. En cambio, las ACL numeradas serán: estándares, si se consideran solo las direcciones IPv4 de origen; o extendidas, si se requiere un análisis más detallado de: las direcciones IPv4 de origen y destino, el protocolo y el puerto utilizado.

En la Tabla 3.11 se presentan los rangos utilizados para las ACL numeradas.

TIPOS DE ACL EN IPv4		
Tipos	**Rangos**	
ACL estándares	1-99	1300-1999
ACL extendidas	100-199	2000-2699

Tabla 3.11 Tipos de ACL en IPv4
Fuente: [8]

Por el contrario, las ACL en IPv6 solo pueden ser extendidas nombradas, y se utilizará como formato para su nombre: la palabra en mayúsculas ACLV6 seguida de la función para la cual están siendo creadas separadas por guiones bajos (_). Por ejemplo, “ACLV6GESTION_DE_LA_RED_MPLS”.

Se permitirá el tráfico de HTTP (puerto 80), HTTPS (puerto 443), FTP (puerto 20), FTP-data (puerto 21), TFTP (puerto 69), entre otros; solo para las redes en IPv4 e IPv6 del departamento NOC a manera de ejemplo; mientras se denegará el tráfico para las redes restantes.

Por seguridad, se recomienda desactivar los servicios de HTTP, HTTPS, FTP y TFTP en todos los dispositivos de la red mientras sea posible; pero en el caso de que se requieran, será importante limitar rigurosamente el acceso mediante las ACL, ya que pueden ser una puerta abierta de seguridad que afecten seriamente el desempeño de la red.

3.6.3. ACCESO REMOTO SEGURO EN IPv6

La gestión mediante acceso remoto es la principal puerta de ataques de una red ya que no se requieren conexiones físicas para ello. Es por ello que es importante definir y limitar el acceso remoto, a fin de que no se exponga el funcionamiento de la red ni la información de la empresa.

En la red de Telconet S.A., la gestión de los dispositivos se establecerá mediante acceso remoto seguro con direcciones IPv4 e IPv6, ya que al manejar las dos versiones de IP, la red será susceptible a ataques por parte de cualquiera de los dos protocolos.

Los routers de la red MPLS podrán ser accedidos remotamente a través de SSH, mientras *telnet* será denegado. Los switches de las capas distribución y acceso serán accedidos mediante *telnet* y SSH, pero estos no podrán acceder a los routers MPLS. Por el contrario, los routers CE serán accedidos remotamente por los dispositivos que pertenecen a la misma VRF incluyendo los LER de la red MPLS, pero estará restringido el acceso desde los routers CE hacia los LER. En la Figura 3.5 se presentan las conexiones remotas permitidas y denegadas.

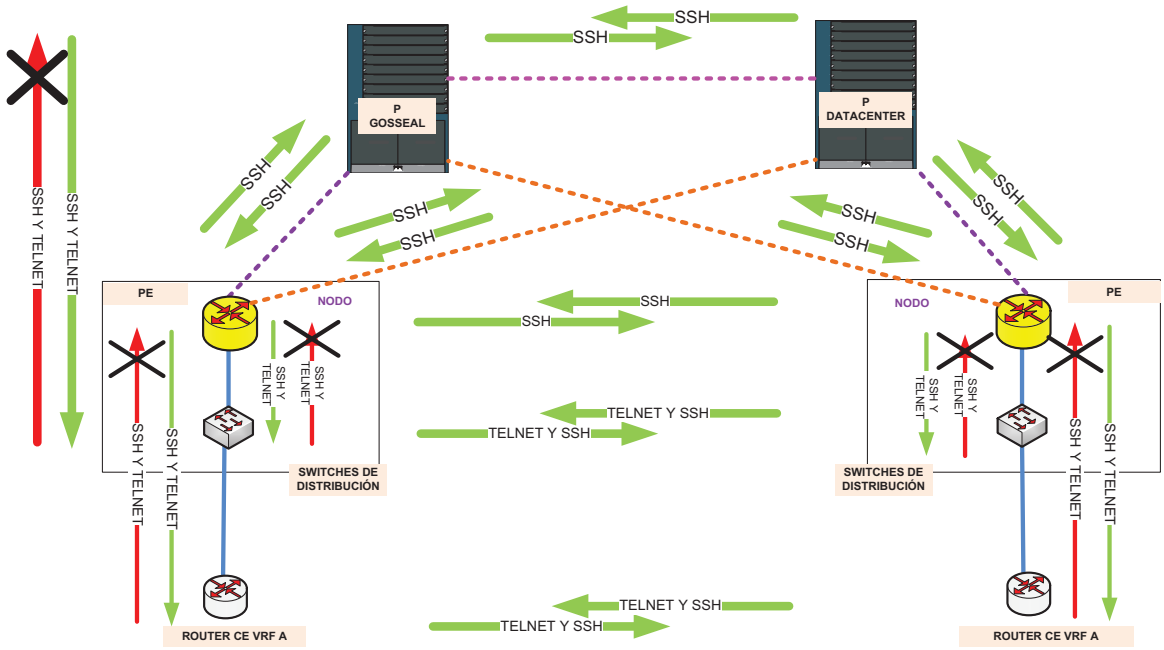


Figura 3.5 Accesos remotos permitidos y denegados

Para poder limitar el acceso de las capas distribución y acceso hacia los dispositivos de la red MPLS, se utilizarán listas de control de acceso (ACL) en IPv4 e IPv6 configuradas a la entrada de las líneas vty.

En lo referente a SSH, se utilizará el algoritmo de encriptación RSA con llaves de 1.024 bits, se limitará el número de reintentos de autenticación a 1 y el tiempo de conexión sin actividad a 30 segundos y se empleará la versión 2 de SSH.

3.7. TOPOLOGÍA FÍSICA DE LA RED DE TELCONET S.A.

En el rediseño original de la red de Telconet S.A.- Quito a la tecnología MPLS se diseñó usando el modelo jerárquico de tres capas con una topología física de estrella en el núcleo, y de anillo, en las capas de distribución y de acceso. El presente diseño tiene por objetivo mantener esta infraestructura jerárquica de tres capas y las topologías físicas de: estrella en el *backbone,* y anillo en las capas de distribución y de acceso.

La capa núcleo estará conformada por: dos dispositivos redundantes entre sí en calidad de routers LSR; y siete, como routers LER. En vista de que la redundancia también es un factor importante en los LER, cada uno dispondrá de doble *Route Switch Processing Memory* (RSP) y un módulo adicional de interfaces *Gigabit Ethernet*.

En la capa distribución se tendrán dos switches agregadores redundantes entre si en cada uno de los routers LER. Mientras, la capa acceso estará distribuida por anillos de 10 nodos como máximo, conectados en cascada a fin de ofrecer redundancia de enlaces.

En el presente rediseño se procurará en lo posible, conservar la infraestructura de red de Telconet S.A. con el fin de ahorrar en costos. En las secciones 3.7.1, 3.7.2 y 3.7.3 se detallan las recomendaciones de hardware y software requeridas para la solución, así como, cada uno de los componentes de la red pertenecientes a las capas del modelo jerárquico.

3.7.1. CAPA NÚCLEO

La capa núcleo se encargará de transportar grandes cantidades de tráfico provenientes de las capas distribución y acceso. Es el punto más importante de la red ya que una falla podría afectar seriamente su desempeño.

Los principales requerimientos que deben cumplir los routers MPLS: LSR y LER, se presentan en las secciones 3.7.1.1 y 3.7.1.2 respectivamente.

3.7.1.1. Routers LSR[17]

Los LSR deben ser dispositivos sumamente robustos ya que van a manejar todo el tráfico de la red de la sucursal de Quito. La capacidad esperada será de 45 Gbps según el análisis de la sección 2.7.4.3, por lo que el *throughput* del dispositivo tiene que ser mayor, o al menos, equivalente a este valor. La redundancia es un factor importante ya que una falla en estos equipos podría dejar inoperativa a gran parte de la red.

Estos dispositivos deben tener interfaces de 1 y 10 Gbps dependiendo de los enlaces con los que se conectan a los LER. No necesitan soporte a IPv6 ya que el mecanismo 6PE/6VPE no amerita que los LSR de la red, cambien sus configuraciones.

A continuación, se presentan las principales características requeridas para los routers LSR:

- Dispositivo de capa 3 como: routers o switches capa 3
- Soporte de la tecnología MPLS
- Soporte para IPv4 y políticas de acceso
- Soporte a los protocolos de capa de red: OSPFv2 y BGPv4
- Soporte a los protocolos de señalización: RSVP-TE y LDP
- Soporte de Calidad de Servicio en MPLS
- Soporte de Ingeniería de tráfico con balanceo de carga y *Fast-ReRoute*

- Interfaces de 1 y 10 Gbps
- Alta capacidad de redundancia
- Un *throughput* mayor a 45 Gbps[37]

En el apartado 2.1.2.2.1 se indicaron las principales características de los dispositivos LSR que dispone el proveedor Telconet S.A. en la sucursal de Quito. Los CAT-WS-C6509-E son equipos muy robustos con un throughput de 720 Gbps[17] y soporte para: MPLS, TE, QoS, etc; por lo que cambiarlos sería innecesario ya que cumplen con las funciones requeridas, y sobre todo, porque pertenecen a los recursos activos de la empresa. Esto no quiere decir que no existen dispositivos con mejores características como el soporte de interfaces a 40 Gbps, pero para los requerimientos de Telconet S.A., los Catalyst 6500 son más que adecuados.

La redundancia vendrá definida por el equivalente router LSR instalado y los enlaces adicionales entre los routers LER y LSR de la red. En la Tabla 3.12 se resumen las principales características de los LSR.

CARACTERÍSTICAS DE LOS ROUTERS LSR	
DESCRIPCIÓN	**CARACTERÍSTICAS**
Marca	CISCO
Modelo	CAT-WS-C6509-E
Versión IOS	12.2(33)SXI6
Memoria No volátil NVRAM	1917K bytes
Memoria del buffer de paquetes	8192K bytes
Memoria Flash	65536K bytes
Performance	400 Mpps/720Gbps
Ten Gigabit Ethernet Interfaces	12
Gigabit Ethernet Interfaces	46

Tabla 3.12 Características de los Ps

[37] Según el análisis de la sección 2.2.4.3.

Se recomienda levantar un enlace adicional de 10 Gbps entre los routers PGOSSEAL y PDATACENTER como se muestra en la Figura 3.6, para tener un enlace redundante y brindar balanceo de carga entre los LSR.

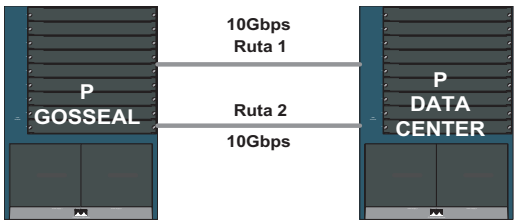


Figura 3.6 Interconexión de los LSR

3.7.1.2. Routers LER[10][18][29][31]

Los LER son dispositivos que se ubican en la frontera de la red MPLS y *Ethernet,* es por ello, que estos deben poder soportar las dos tecnologías y ser lo suficientemente robustos para manejar el tráfico proveniente de las capas: distribución y acceso. El *throughput* dependerá del nodo y fueron definidos en la sección 2.2.4.3.

Estos dispositivos deben tener interfaces de 1 y 10 Gbps dependiendo de los enlaces con los que se conectan a los LSR; pero sobre todo, deben tener soporte para IPv6. A continuación, se presentan las principales características requeridas para los LER:

- Dispositivo de capa 3
- Soporte de la tecnología MPLS
- Soporte para IPv6 e IPv4
- Políticas de Acceso en IPv4 e IPv6
- Soporte para los protocolos de capa de red: OSPFv2 y BGPv4
- Soporte para los protocolos de señalización: RSVP-TE y LDP
- Funcionalidades de MPLS con manejo de las VPN de capa 2 y 3
- Soporte de Calidad de Servicio en MPLS
- Soporte de Ingeniería de Tráfico con balanceo de carga y *Fast-ReRoute*

- Interfaces de 1 y 10 Gbps
- Alta capacidad de redundancia
- El *throughput* del dispositivo dependerá del nodo según el análisis de la sección 2.2.4.3

En la sección 2.1.2.2.1 se indican las principales características de los routers LER que dispone la sucursal de Quito de Telconet S.A. Estos equipos necesitan ser cambiados o actualizados, frente a la cantidad de tráfico y al soporte de IPv6 que se espera brindar en los próximos cinco años (2017).

Con respecto al tráfico generado por el nuevo Centro de Datos de Quito, se considera necesario establecer un LER adicional, como se muestra en la Figura 3.7, que concentre todo este tráfico, debido a que se esperan aproximadamente 20 Gbps para el 2017, por lo que se diferenciarán como dos routers diferentes PE1BODEGA y PE1DATACENTER.

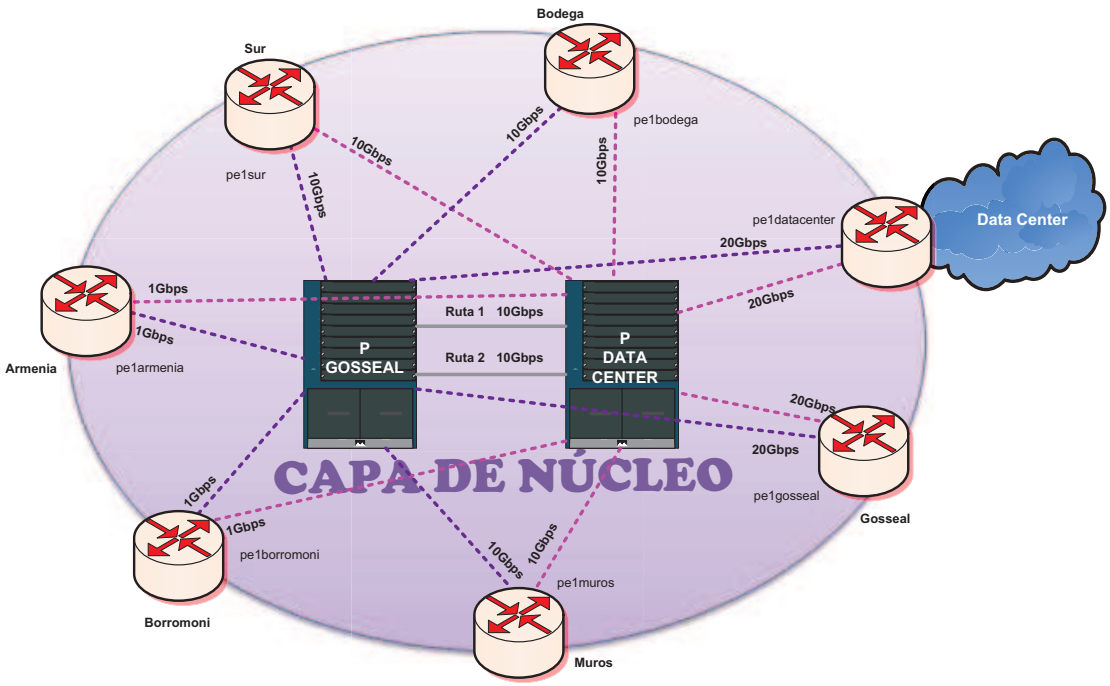


Figura 3.7 Dispositivos LER y LSR

Además, en la Figura 3.7 se indican las capacidades de los enlaces entre los

routers LER y LSR, definidas según los requerimientos de tráfico analizados en la sección 2.2.4.3. Los nodos que para el año 2017, requieren interfaces superiores a 10 Gbps, se configurarán con balanceo de carga para que puedan transportar la capacidad de tráfico esperada.

La redundancia en esta parte de la red es importante pero ubicar un equipo adicional a cada LER resulta demasiado costoso. En la Tabla 3.14 se presenta un análisis de los cambios a realizar en los routers LER de la red de Telconet S.A.

No todas las versiones de los IOS de Cisco soportan MPLS, las aplicaciones de QoS, TE y VPN, o IPv6; es por ello que, en los routers LER de Armenia y Borromoni es necesario actualizar su IOS. En la Tabla 3.13 se presentan las versiones de los IOS de Cisco, a partir de los cuales, se tiene soporte para las diferentes aplicaciones.

DESCRIPCIÓN	VERSIÓN DE IOS	SERIE DE ROUTERS
Tecnología MPLS	11.1 CT o superior	Cisco 7000, 7200, 7600, 12000
Protocolo LDP en MPLS	12.0(10)ST o superior	Cisco 1900, 2600, 3600, 7200, 7600, 12000
Calidad de Servicio en MPLS	12.0(19)SL o superior	Cisco 1800, 1900, 2600, 3600, 7200, 7600, 12000
Ingeniería de Tráfico en MPLS	12.0(5)S o superior	Cisco 1900, 2600, 3600, 7200, 7600, 12000
Redes Privadas Virtuales en MPLS	12.0(5)T o superior	Cisco 1900, 2600, 3600, 7200, 7600, 12000
Soporte a IPv6	12.4 o superior	Cisco 7200, 7600, 12000

Tabla 3.13 Versiones de los IOS de Cisco

Fuente: [12][13][14][15][34][41]

ROUTERS LER DE LA RED DE TELCONET S.A.-QUITO						
DISPOSITIVO	TRÁFICO 2017 (Mbps)	MODELO	VERSIÓN IOS	CAMBIOS		MOTIVO
				IOS	EQUIPO	
PE1SUR2	2.462,22	7206VXR (NPE-G2)	12.2(33)SRD5	-	Si	Se requiere un dispositivo con interfaces a 10 Gbps, pero el 7206VXR solo tiene capacidad para tres interfaces *Gigabit Ethernet,* por lo que será necesario cambiarlo por un equipo más robusto
PE1ARMENIA	498,78	7206VXR (NPE-G2)	12.2(33)SRD5	Si	-	El rediseño requiere que Armenia disponga de interfaces de 1 Gbps y el 7206VXR cuenta con tres, las cuales son más que suficientes; pero la versión que tiene instalada no soporta IPv6, por lo que será necesario actualizarlo
PE1BORROMONI	808,94	7206VXR (NPE-G2)	12.2(33)SRD5	Si	-	De la misma manera que el PE1ARMENIA, PE1BORROMONI requiere interfaces de 1 Gbps y soporte a IPv6, por lo que será necesario actualizar el IOS
PE1BODEGA	3.121,30	7206VXR (NPE-G2)	15.0(1)M7	-	Si	Se requiere un dispositivo con interfaces de 10 Gbps, por lo que será necesario cambiar el dispositivo a uno más robusto
PE1GOSSEAL	15.110,88	7609-S	15.0(1)S4	-	-	Para cubrir los requerimientos del diseño, se necesita un dispositivo que tenga interfaces de 40 Gbps, o a su vez, se puede mantener el router 7609, y agregarle interfaces de 10 Gbps conforme crezca el tráfico de la red, a fin de utilizar los equipos de la empresa
PE1MUROS	1.972,94	7609-S	15.0(1)S4	-	-	El equipo cubre los requerimientos del rediseño, pero será necesario agregar un módulo adicional de interfaces de 10 Gbps para garantizar la redundancia de puertos
PE1DATACENTER	20.000,00	NO EXISTE	NO EXISTE	-	-	Se requiere un dispositivo con cuatro interfaces de 10 Gbps, o a su vez, 2 interfaces de 40 Gbps

Tabla 3.14 Cambios en los routers LER

Por cada router LER, se dispondrán de dos enlaces hacia los LSR, una tarjeta *Route Switch Processor* (RSP) extra y un módulo de interfaces 10 *Gigabit Ethernet* adicional, a fin de brindar una red robusta, redundante y tolerante a fallas. La memoria RSP permitirá brindar redundancia al procesador del dispositivo, mientras el módulo de interfaces garantizará puertos adicionales.

3.7.2. CAPA DISTRIBUCIÓN[7][30]

La capa distribución se encarga de transportar el tráfico desde la capa acceso hasta la capa núcleo y viceversa. Está formada por los switches agregadores que se conectan a los routers LER por un extremo, y a los switches de acceso por el otro.

Los agregadores deben ser dispositivos de capa 2 a fin de que ofrezcan mayor rapidez en la transmisión, con interfaces de 1 y 10 Gbps dependiendo del nodo LER al que se conecten. Una vez que se reemplace por completo al protocolo IPv4, la dirección IP de gestión del switch también debe migrarse a IPv6; es por ello que, en lo posible, los agregadores deben tener soporte a la plantilla de doble pila IPv4-IPv6.

Los principales requerimientos que deben cumplir los agregadores para que trabajen en la capa distribución son los siguientes:

Requerimientos de los agregadores

- Dispositivo de capa 2
- Soporte de la tecnología *Ethernet*
- Soporte de la plantilla “sdm prefer dual-ipv4-and-ipv6 default”
- Soporte de Calidad de Servicio con MLS
- Manejo de VLAN
- Soporte para el protocolo *Spanning-Tree*
- Soporte de la encapsulación *trunk* dot1q (IEEE 802.1q)
- Soporte para el protocolo VLAN *Trunking Protocol* (VTP)

- Interfaces a 1 y 10 Gbps según el nodo
- Redundancia

La redundancia es importante en esta parte de la red porque estos dispositivos son los encargados de manejar el tráfico proveniente de los pétalos de acceso; es por ello que, se incluirán dos agregadores por cada LER de la red. En la Figura 3.8 se muestran las capacidades de los enlaces de los agregadores, definidas según los requerimientos de tráfico analizados en la sección 2.2.4.3.

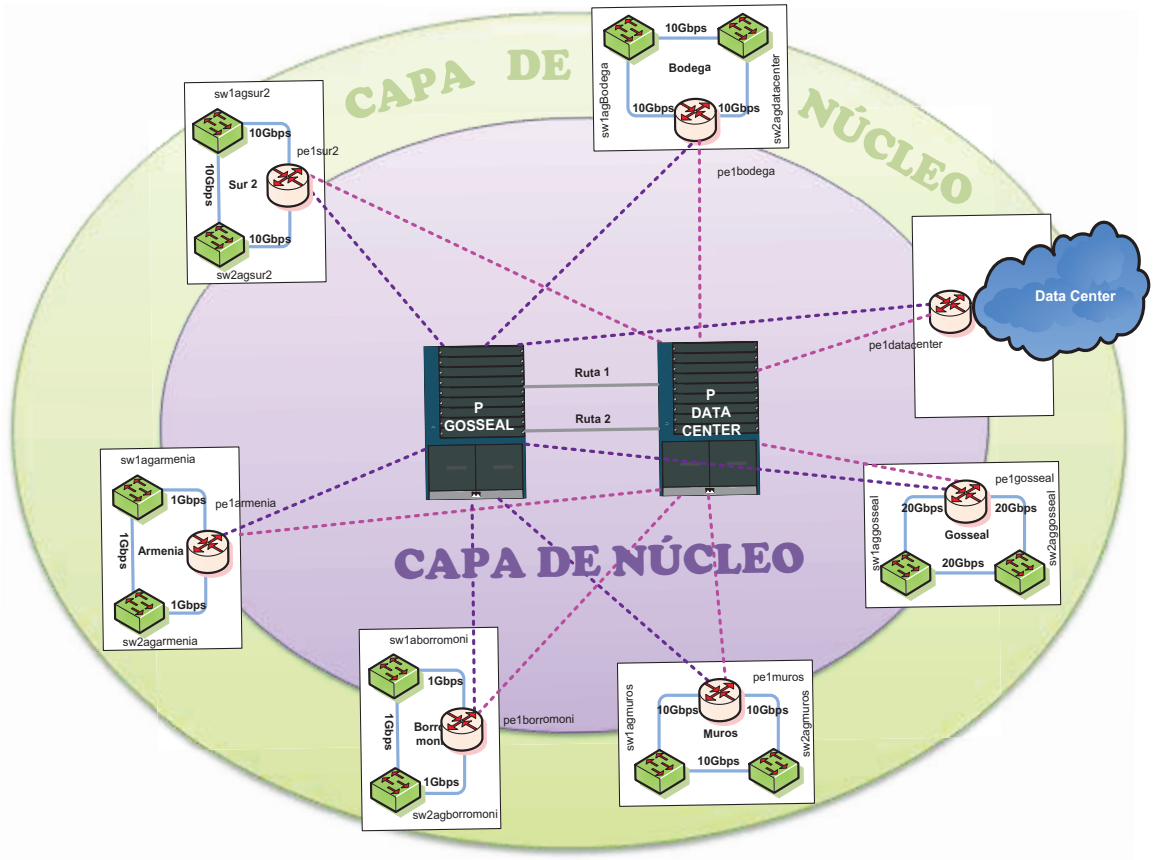


Figura 3.8 Capacidades de los enlaces de los agregadores

En la Tabla 3.15 se presenta un análisis de los cambios a realizar en los agregadores de la red de Telconet S.A.

AGREGADORES DE LA RED DE TELCONET S.A.-QUITO						
DISPOSITIVO	TRÁFICO 2017 (Mbps)	MODELO	VERSIÓN IOS	CAMBIOS		MOTIVO
				IOS	EQUIPO	
SW1AGSUR2 SW2AGSUR2	2.462,22	WS-C3750E-24TD-S	12.2(50)SE	-	Si	Para este nodo se requieren 3 interfaces de 10 Gbps, pero el Cisco 3750 solo dispone de 2 de ellas, por lo que será necesario cambiarlo por uno más robusto
SW1AGARMENIA SW2AGARMENIA	498,78	WS-C3750E-24TD-S	12.2(50)SE	-	-	En el rediseño se requieren interfaces de 1 Gbps y dispositivos que soporten IPv6 como los switches Cisco 3750E que cumplen con estos requerimientos. La serie 3750 tiene soporte a IPv6 *forwarding* a partir de la versión 12.2(50) SE, por lo que no es necesario actualizar su IOS
SW1AGBORROMONI SW2AGBORROMONI	808,94	WS-C3750E-24TD-S	12.2(50)SE	-	-	De la misma manera que el PE1ARMENIA, PE1BORROMONI requiere interfaces de 1 Gbps y soporte para IPv6, por lo que no será necesario actualizar este dispositivo
SW1AGBODEGA SW2AGBODEGA	3.121,30	WS-C3750E-24TD-S	12.2(50)SE	-	Si	Se requieren dispositivos con al menos 3 interfaces de 10 Gbps, por lo que será necesario cambiarlo a uno más robusto
SW1AGGOSSEAL SW2AGGOSSEAL	15.110,88	WS-C3750E-24TD-S	12.2(50)SE	-	Si	Para este nodo se requieren 4 interfaces de 10 Gbps, pero el Cisco 3750 solo dispone de 2 de ellas, por lo que será necesario cambiarlo por uno más robusto. La interfaz adicional es para la conexión con el pétalo de AEPROVI que requiere interfaces de 10 Gbps como se indica en el ANEXO A
SW1AGMUROS SW2AGMUROS	1.972,94	WS-C3750E-24TD-S	12.2(50)SE	-	Si	Se requieren 3 interfaces de 10 Gbps, pero el Cisco 3750 solo dispone de 2 de ellas, por lo que será necesario cambiarlo por uno más robusto

Tabla 3.15 Cambios en los agregadores

Para el nodo DATACENTER no se incluye este tipo de agregadores porque la infraestructura de un Centro de Datos requiere dispositivos mucho más robustos que salen del alcance de este proyecto, para mayor información se recomienda revisar [35].

3.7.3. CAPA ACCESO[7][32][33]

La capa acceso es la capa más cercana al usuario y se encarga de trasportar el tráfico proveniente de los clientes hacia la red del proveedor. La redundancia no es vital en esta parte de la red, como para ubicar otro dispositivo de acceso en cada nodo; pero si es importante brindar redundancia de enlaces de tal manera que los switches dispongan de una ruta alterna para redireccionar el tráfico hacia los LER correspondientes; es por ello que, se mantendrá la topología física de anillo entre los switches de acceso.

Las características mínimas que deben presentar los switches de acceso son:

Requerimientos de los switches de acceso

- Dispositivo de capa 2
- Soporte de la tecnología *Ethernet*
- Soporte de la plantilla “sdm prefer dual-ipv4-and-ipv6 default”
- Soporte de Calidad de Servicio con MLS
- Manejo de VLAN
- Soporte para el protocolo *Spanning-Tree*
- Soporte de la encapsulación *trunk* dot1q (IEEE 802.1q)
- Soporte para el protocolo VLAN *Trunking Protocol* (VTP)
- Interfaces a 100Mbps y 1 Gbps
- Alta densidad de puertos

En el ANEXO A se muestran los modelos de los dispositivos que se tienen en cada nodo de la red. En la Figura 3.9 se presenta el esquema rediseñado para la sucursal de Quito de Telconet S.A.

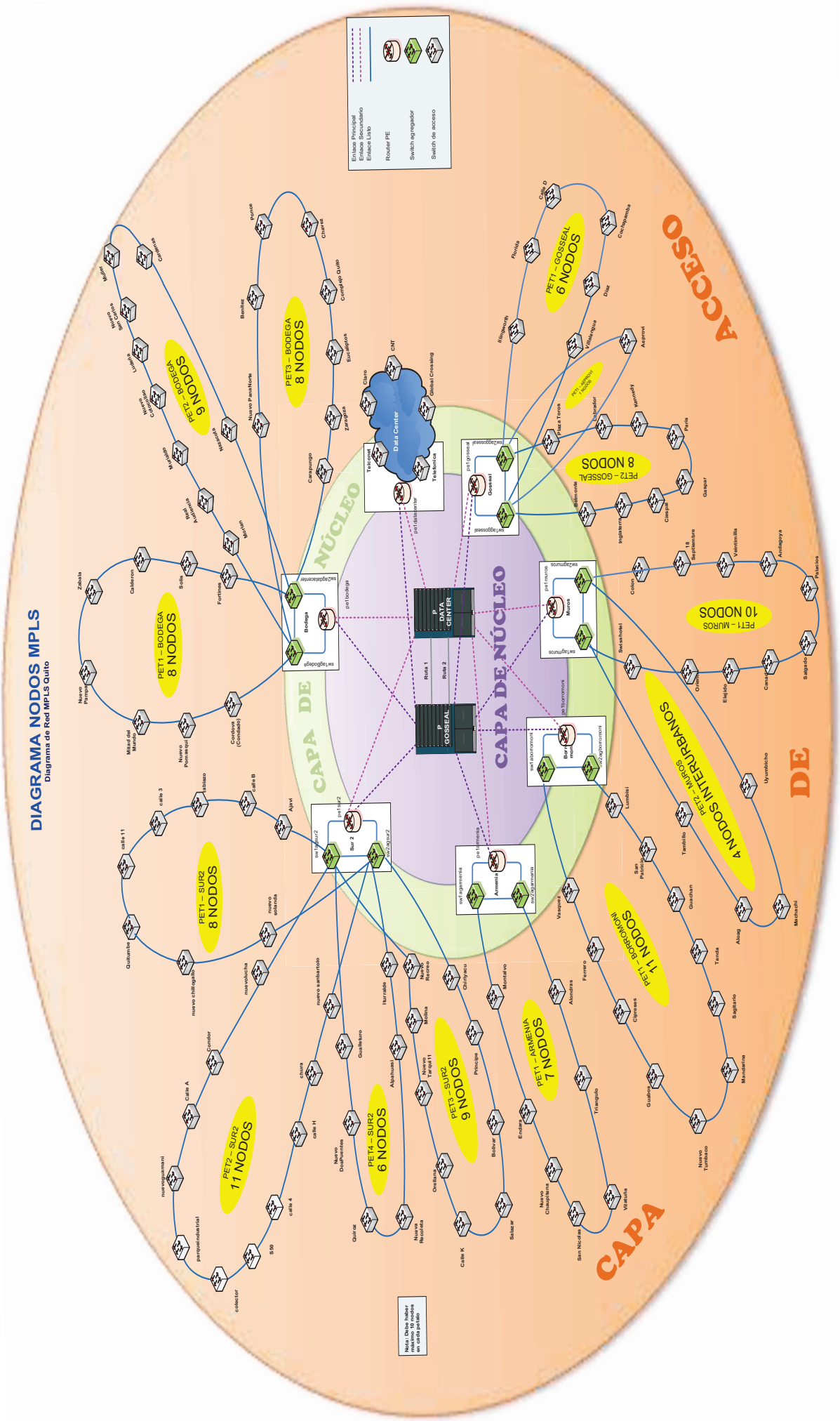


Figura 3.9 Red rediseñada de la sucursal Quito de Telconet S.A.

De la misma manera que los agregadores, los switches de acceso requerirán una dirección IP de gestión en IPv6 cuando se reemplace por completo al protocolo IPv4; es por ello que, estos dispositivos deben tener soporte a la plantilla SDM de doble pila. Los switches Cisco Catalyst 3550 no tienen soporte para IPv6, aun cuando se actualice su IOS a la última versión disponible. Las series de los switches Cisco que presentan soporte para IPv6 son los 3560 y los 3750, a partir de la versión de IOS 12.2(50)SE.

Además, es importante que la densidad de puertos sea alta, debido a que los routers de los usuarios se conectarán directamente a estos dispositivos. En lo posible, se deben tener switches con 48 o más puertos, ya que se evitará ubicar 2 o más dispositivos en cascada por nodo.

Los switches de acceso son marca Cisco 3550 que no tienen soporte a la plantilla de doble pila, por lo que deben ser migrados a una serie más robusta. A excepción del nodo AEPROVI que es un Cisco C4900M que no amerita ser migrado.

3.7.4. DIRECCIONAMIENTO IP[26][27][28]

Para el presente proyecto se describirá el direccionamiento IP para IPv4 e IPv6. Los LSR de la red MPLS manejarán solo direcciones IPv4, mientras que los LER, los agregadores, los switches de acceso y los routers CE pueden ser o no de doble pila (IPv4 e IPv6). En los apartados 3.7.4.1 y 3.7.4.2 se detalla el direccionamiento IPv4 e IPv6 respectivamente para los nodos de la red.

3.7.4.1. Direccionamiento IPv4

La nube MPLS, los agregadores, los switches de acceso y los routers de los clientes, es decir toda la red de Telconet S.A.-Quito manejará direccionamiento IPv4, aunque partes de ella serán doble pila para tener soporte a IPv6.

Los routers de la nube MPLS se configurarán con direcciones que pertenezcan a subredes de máscara /30 ya que son enlaces punto a punto. La red utilizada para el presente proyecto será la 192.168.1.0/24.

En la Tabla 3.16 se presenta la distribución de subredes para cada enlace de la red MPLS.

ENLACE	DIRECCIÓN
PGOSSEAL-PDATACENTER 1	192.168.1.0/30
PGOSSEAL-PDATACENTER 2	192.168.1.4/30
PGOSSEAL-PE1SUR2	192.168.1.8/30
PGOSSEAL-PE1ARMENIA	192.168.1.12/30
PGOSSEAL-PE1BORROMONI	192.168.1.16/30
PGOSSEAL-PE1BODEGA	192.168.1.20/30
PGOSSEAL-PE1DATACENTER	192.168.1.24/30
PGOSSEAL-PE1GOSSEAL	192.168.1.28/30
PGOSSEAL-PE1MUROS	192.168.1.32/30
PDATACENTER-PE1SUR2	192.168.1.36/30
PDATACENTER-PE1ARMENIA	192.168.1.40/30
PDATACENTER-PE1BORROMONI	192.168.1.44/30
PDATACENTER-PE1BODEGA	192.168.1.48/30
PDATACENTER-PE1DATACENTER	192.168.1.52/30
PDATACENTER-PE1GOSSEAL	192.168.1.56/30
PDATACENTER-PE1MUROS	192.168.1.60/30

Tabla 3.16 Direccionamiento IPv4 para la nube MPLS

Los agregadores y los switches de acceso se configurarán en IPv4, pudiendo tener o no soporte para IPv6. La red utilizada será la 10.0.0.0/8, donde cada pétalo tendrá una subred de máscara /24 que seguirá el formato mostrado en la Figura 3.10.

Figura 3.10 Esquema de direccionamiento IPv4 para los switches

El primer y segundo octeto serán fijos (10.2). El tercer octeto será establecido por dos números: el primero, definirá el router LER al que pertenece el switch (numeración en sentido antihorario); y el segundo, definirá el pétalo en el que se encuentra (numeración indicada en la Figura 3.11). Finalmente, el último octeto indicará la ubicación del switch dentro del pétalo y vendrá numerado en sentido horario.

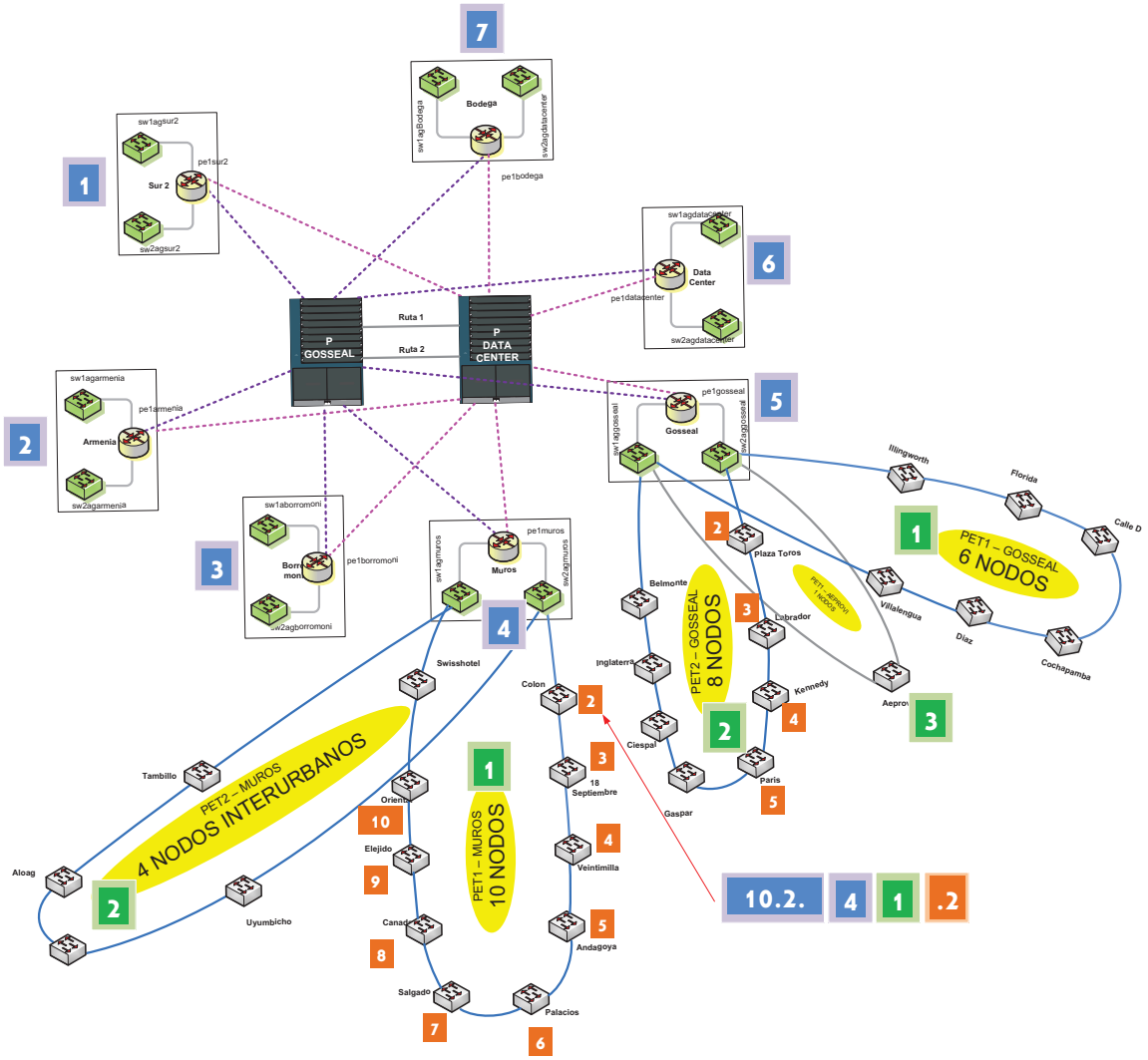


Figura 3.11 Esquema de direccionamiento para los switches de acceso

De la misma manera, los agregadores aunque son dispositivos de capa 2, deben tener al menos una dirección IP de administración; es por ello que, para el presente proyecto, se utilizarán las dos últimas direcciones disponibles de la red

correspondiente al primer pétalo conectado al LER. El agregador principal tendrá la última dirección IP (.254), mientras el agregador secundario utilizará la penúltima dirección IP (.253). La primera dirección IP (.1) estará reservará como la puerta de salida de la red hacia el LER respectivo.

Por ejemplo, la dirección IP que identificará al switch de acceso COLON será: 10.2.41.2/24, según se muestra en la Figura 3.11. El primer y segundo octeto estará previamente determinados (10.2); el tercer octeto vendrá definido por el PEMUROS (4) y el número de pétalo (1); finalmente, el cuarto octeto identificará la ubicación del nodo dentro del pétalo (2). El SW1AGMUROS tendrá la dirección 10.2.41.254/24, el SW2AGMUROS utilizará la dirección 10.2.41.253/24, y tendrán como puerta de salida, la interfaz configurada en el PEMUROS con la dirección 10.2.41.1/24.

3.7.4.2. Direccionamiento IPv6

Los routers LER y CE manejarán direccionamiento IPv6 según lo requieran los clientes de Telconet S.A., mientras los agregadores y switches de acceso tendrán una dirección IPv6 de gestión, conforme la red desplace a IPv4 y migre a IPv6. La asignación de direcciones IPv6 utilizará los mismos principios que la numeración de los LER y switches en IPv4, solo que se utilizará un contexto de 128 bits.

El rango de direcciones IPv6 asignado a Telconet S.A. es: 2001:29::0/32. El formato de numeración para los switches de acceso estará definido según el esquema mostrado en la Figura 3.12 con máscara /64, donde los dos primeros valores de la dirección, estarán previamente establecidos por el prefijo IPv6 asignado (2001:29), el tercero será 2 para representar a la sucursal Quito, el cuarto indicará el LER y el pétalo al que pertenece el switch, como se indicó para el direccionamiento en IPv4; y finalmente, se llenarán de ceros hasta definir en el último grupo de 16 bits, la ubicación del switch dentro del pétalo correspondiente.

Los LER tendrán configurada la primera dirección IPv6 disponible (:1) como la puerta de salida de la red de cada uno de los pétalos. Mientras, los agregadores utilizarán las dos últimas direcciones disponibles de la red del primer pétalo configurado. El agregador principal tendrá la última dirección IP (0xFFFF), y el secundario, utilizará la penúltima dirección IP (0XFFEF).

Figura 3.12 Esquema de direccionamiento IPv6

Por ejemplo, las direcciones IPv6 que identificarán a los dispositivos de la red se especifican en la Tabla 3.17.

ENLACE	DIRECCIÓN IPv6	GATEWAY
SW1COLON	2001:29:2:41::2/64	2001:29:2:41::1/64
SW1AGMUROS	2001:29:2:41::FFFF/64	2001:29:2:41::1/64
SW2AGMUROS	2001:29:2:41::FFEF/64	2001:29:2:41::1/64

Tabla 3.17 Direccionamiento IPv4 para la nube MPLS

3.8. SELECCIÓN DEL HARDWARE Y SOFTWARE

Después de determinar los requerimientos de hardware y software requeridos para el rediseño, se analizarán las características técnicas, las funcionalidades y los costos de tres marcas diferentes del mercado, a través de cuadros comparativos.

En lo referente a la actualización del software de los dispositivos de Telconet S.A., no se pueden comparar varias marcas del mercado debido a que los sistemas operativos son diferentes para cada marca y dispositivo; por lo que se nombrará la versión del IOS, a partir de la cual, se tiene soporte a la aplicación requerida.

En los cuadros comparativos se definen tres marcas accesibles en el mercado ecuatoriano, como son: Cisco Systems, Inc., Hewlett-Packard y Huawei Technologies Co. Ltd. La selección de los dispositivos se determinará mediante matrices de decisión que permitan analizar las ventajas y desventajas de cada marca, en lo referente al *throughput,* los costos, la densidad de puertos, etc.

En el ANEXO D se muestran las cotizaciones, a partir de las cuales, se hizo el análisis de las secciones 3.8.1, 3.8.2 y 3.8.3. Mientras, en el ANEXO E se presentan los *data sheets* de los dispositivos que intervienen en el análisis.

3.8.1. CAPA NÚCLEO[6][18][36][37]

La capa núcleo está formada por los routers LSR y LER de la red MPLS. Como se analizó en la sección 3.7.1.1, no se requiere actualizar el hardware y/o el software de los routers LSR, ya que los dispositivos que actualmente dispone Telconet S.A. cubren los requerimientos planteados.

Por el contrario, se necesitan siete LER de los cuales, según la sección 3.7.1.2 se requieren migrar los nodos: PE1SUR2, PE1BODEGA y PE1DATACENTER a routers más robustos que tengan interfaces de 10 Gbps; mientras, los nodos PE1ARMENIA y PE1BORROMONI deben ser actualizados a un IOS que soporte IPv6. Mientras que no se requieren cambios en los nodos PE1GOSSEAL y PE1MUROS porque cumplen con los requerimientos planteados

Para seleccionar los equipos de los nodos PE1SUR2, PE1BODEGA y PE1DATACENTER, en la Tabla 3.18 se presenta el cuadro comparativo de tres equipos con características similares y marcas diferentes, a fin de conocer las ventajas y desventajas de cada modelo.

Los equipos mostrados en la Tabla 3.18 presentan excelentes características técnicas, como: alta redundancia en el procesador, interfaces de 10 Gbps, soporte a IPv6, MPLS, etc; pero, para seleccionar el equipo que mejor se adapte a los requerimientos de Telconet S.A., se analizarán las principales

características de estos, a través de la matriz de decisión presentada en la Tabla 3.19 que permitirá obtener el mayor indicador de aprobación del dispositivo.

MODELO DEL DISPOSITIVO	CISCO	HP	HUAWEI
	7609S-RSP720CXL-R	HP 6608 Router Chassis (JC177B)	NE40E-8
Puertos			
Número de slots	Chasis de 9 slots con dos RSP de respaldo	8 HIM slots, 2 slots MPU (módulos de administración)	12 slots, incluyendo 2 SRU (1:1 backup), 1 SFU y 8 LDU
Tipo de interfaces	Interfaces *Fast Ethernet*, *Gigabit Ethernet*, 10 *Gigabit Ethernet*; OC-3/STM-1, OC-12/STM-4, OC-48/STM-16 Packet over SONET/SDH (PoS), and OC-192/STM-64 PoS, OC-3/STM-1 ATM, OC-12/STM-4 ATM y OC-48/STM-16 ATM	Interfaces FE, GE, 10 GE, OC-3/STM-1, OC-12/STM-4, OC-48/STM-16 Packet over SONET/SDH (PoS), and OC-192/STM-64 PoS, OC-3/STM-1 ATM, OC-12/STM-4 ATM y OC-48/STM-16 ATM	Interfaces 10GE- LAN /WAN; GE/FE; OC-192c/STM-64c POS; OC-48c/STM-16c POS; OC-12c/STM-4c POS; OC-3c/STM-1c POS; OC-3/STM-1; OC-3c/STM-1c ATM; OC-12c/STM-4c ATM; E3/CT3; CE1/CT1; E1/T1
Modulares	Si	Si	Si
Interfaces adicionales	2 módulos WS-X6704-10GE (4 port 10-Gigabit Ethernet) y 2 módulos SPA-2X1GE-V2 (4-port Gigabit Ethernet Shared Port Adapter)	4 HP 6600 1 puerto 10GbE XFP HIM Router Module; 8 HP X120 1G SFP LC SX Transceiver	4 puertos 10GBase LAN/WAN-XFP+ 8 puertos 100/1000Base-X-SFP Integrated Line Processing Unit (LPUI-41)
Rendimiento			
Throughput	Sobre los 400 Mpps	Sobre los 108 Mpps	400 Mpps
Capacidad de envío	720 Gbps	153.6 Gbps	640 Gbps
Memoria y Procesamiento			
Capacidades de las memorias y búferes	256 MB de memoria *flash*; tamaño del búfer de paquetes: 128 MB	2 GB DDR2 SDRAM, 4 GB DDR2 SDRAM, 1 GB de memoria *flash*; tamaño del búfer de paquetes: 128 MB	256 MB de memoria *flash*; tamaño del búfer de paquetes: 128 MB
Conectividad			
IPv4	Enrutamiento estático y protocolos de enrutamiento dinámico: RIP, OSPF, IS-IS y BGP-4	Soporte a enrutamiento estático, RIP, OSPF, IS-IS y BGP-4	Enrutamiento estático y protocolos de enrutamiento dinámico: RIP, OSPF, IS-IS y BGP-4

IPv6	Soporte para la transición de IPv4 a IPv6: túneles 4/6, GRE y 6PE/6VPE; enrutamiento: IPv6 estático, RIPng, OSPFv3, IS-ISv6 y BGPv6; conectividad: *ping* y *traceroute* en IPv6; soporte de ACLs en IPv6	ACL en IPv6; enrutamiento de IPv6 estático, dual IP stack, RIPng, OSPFv3, IS-ISv6, BGP4+ for IPv6 y tunelización en IPv6	Soporte para la transición de IPv4 a IPv6: túneles IPv6 a IPv4, IPv4 sobre IPv6 Router Proveedor de túneles IPv6 y Edge (6PE); protocolos de enrutamiento: IPv6 estático, RIPng, OSPFv3, IS-ISv6 y BGP4 +; conectividad: *ping y traceroute* en IPv6; ACLs en IPv6
Soporte a MPLS			
Aplicaciones	Soporte de LDP, *Tag Switching*, MPLS *Traffic Engineering*, MPLS QoS, VPLS, HVPLS, FRR y MPLS VPNs	Soporte de LDP, MPLS *Traffic Engineering*, MPLS QoS, VPLS, HVPLS, FRR y MPLS VPNs	Soporte de LDP over TE, MPLS TE, VPLS, H-VPLS, MPLS QoS, FRR y *policy-based routing* in VPN
Calidad de Servicio			
QoS	Soporte de FIFO, PQ, CQ, WFQ, CBQ, RTPQ, *traffic shaping*, FR QoS, MPLS QoS, *Weighted Random Early Detection* (WRED)/RED	*Traffic Policing*; administración de congestión con soporte a FIFO, PQ, CQ, WFQ, CBQ; para evitar la congestión: WRED y RED; otras tecnologías como: FR QoS y MPLS QoS	Soporte de PQ, WFQ, *DiffServ* e *InterServ*, WRED y RED
Estándar de prioridad	*Class of Service (*CoS) IEEE 802.1p	*Class of Service* (CoS) IEEE 802.1p	*Class of Service* (CoS) IEEE 802.1p priority *tag*
Costo			
sin IVA	77.408,47 USD	68.526,74 USD	61.124,45 USD
Garantía e información adicional			
Tiempo de entrega, validez de la oferta y garantía	El tiempo de entrega: previa verificación de *stock* a la fecha de la orden de compra. Validez de la oferta: 15 días. Los precios no incluyen instalación ni configuración de hardware ni software	Garantía de 1 año con reemplazo de dispositivos previo anticipo. Validez de la oferta: 10 días del calendario. Soporte por teléfono. Tiempo de entrega: previa verificación de stock	Validez de la oferta: 1 mes. Tiempo de entrega: 45 a 60 días con la Orden de Compra. Garantía: 1 año. Los precios no incluyen instalación, ni configuración, este servicio se lo determina previa definición del alcance de los mismos

Tabla 3.18 Cuadro comparativo: routers LER

Una matriz de decisión define varios criterios de selección que se evalúan mediante la asignación de los grados de importancia para el proveedor (la suma no debe ser mayor al 100%). Posteriormente, los dispositivos de análisis tendrán definido un grado de PERT[38] (0-10) para cada criterio de selección, siendo 10 el dispositivo que presente las mejores características de este criterio y 0, aquel que no las disponga. La aprobación (APROB.) será el producto entre los grados de importancia y de PERT, para finalmente, obtener los totales de decisión de cada producto analizado. El equipo seleccionado será aquel que tenga el mayor valor de decisión total, ya que representa las mejores características de análisis del proveedor.

MODELO DEL DISPOSITIVO		CISCO		HP		HUAWEI	
		7609S-RSP720CXL-R		HP 6608 (JC177B)		NE40E-8	
CRITERIO DE SELECCIÓN	GRADO DE IMPORTANCIA	G. PERT (0-10)	APROB.	G. PERT (0-10)	APROB.	G. PERT (0-10)	APROB.
Capacidad de slots	10%	9	0,9	7	0,7	10	1
Redundancia	22%	10	2,2	10	2,2	10	2,2
Throughput	15%	10	1,5	3	0,45	10	1,5
Capacidad de envío	18%	10	1,8	3	0,54	9	1,62
Memoria y Procesamiento	15%	8	1,2	10	1,5	8	1,2
Inversión	10%	8	0,8	9	0,88	10	1,00
Garantía	10%	10	1	9	0,9	8	0,8
Total	**100%**	**Total P1:**	**9,4**	**Total P2:**	**7,17**	**Total P3:**	**9,32**

Tabla 3.19 Matriz de decisión: LER

Los grados de importancia de los criterios de selección se establecen con: 22% para la redundancia debido a que estos equipos pertenecen a la capa núcleo donde la disponibilidad es importante, 18% para la capacidad de envío y 15% para el *throughput* ya que se necesitan equipos robustos que envíen la información a alta velocidad, 15% para la memoria y procesamiento porque al ser dispositivos de núcleo, deben tener suficiente memoria y capacidad de procesamiento de los paquetes para mejorar el desempeño de la red, 10% para

[38] El grado de PERT es una técnica de evaluación de elementos, donde se define un rango de valores que representan numéricamente las mejores características del producto analizado.

la capacidad de *slots* ya que no se necesita gran densidad de puertos como un switch de acceso que se conecta a los clientes, 10% para la inversión y 10% para la garantía ya que las dos son importantes en dispositivos costos.

En la Tabla 3.19 se muestra la matriz de decisión para seleccionar el LER que mejor cumpla con los requerimientos de los nodos: PE1SUR2, PE1BODEGA y PE1DATACENTER. Según los resultados obtenidos en el análisis, se selecciona el router Cisco 7609S-RSP720CXL-R con un total de aprobación de 9,4/10.

Para los nodos PE1ARMENIA y PE1BORROMONI, es importante actualizar las versiones de sus IOS de tal manera que los dispositivos tengan soporte a IPv6. Como se analizó en la Tabla 3.14, todas las versiones superiores a 12.4 presentan IPv6 forwarding, pero como ARMENIA y BORROMONI tienen la versión: 12.2(33)SRD5[19], no podrán brindar soporte a IPv6 hasta que se migren a una versión igual o superior a 12.4. Estos dispositivos serán actualizados a la versión más reciente de Cisco: 15.0(1)M7.

Será importante agregar un módulo de interfaces de 10 Gbps (WS-X6704-10GE) para los dispositivos: PGOSSEAL, PDATACENTER, PE1SUR2, PE1BODEGA, PE1GOSSEAL, PE1MUROS y PE1DATACENTER; y un módulo de interfaces de 1 Gbps (SPA-2X1GE-V2) para PE1ARMENIA y PE1BORROMONI, a fin de brindar redundancia de puertos en los routers de núcleo.

3.8.2. CAPA DISTRIBUCIÓN[5][31][39][40]

La capa distribución está formada por los agregadores de la red que trasportan el tráfico entre las capas núcleo y acceso. Según la sección 3.7.2, se necesitan migrar los nodos SW1AGSUR2, SW2AGSUR2, SW1AGBODEGA, SW2AGBODEGA, SW1AGGOSSEAL, SW2AGGOSSEAL, SW1AGMUROS Y SW2AGMUROS a dispositivos más robustos con interfaces a 10 Gbps, mientras los agregadores restantes se mantienen sin cambios.

En la Figura 3.20 se presenta un cuadro comparativo de las principales características de tres switches agregadores de diferentes marcas.

MODELO DEL DISPOSITIVO	CISCO	HP	HUAWEI
	Catalyst WS-4900M	HP 5820-14XG-SFP+ Switch with 2 Slots (JC106A)	S5328C-EI-24S
Puertos			
Número de slots e interfaces	Dispositivo modular con capacidad variable según las tarjetas asignadas: tarjeta de 20 puertos 10/100/1000 (RJ-45), tarjeta de 4 puertos 10GbE (X2), tarjeta de 8 puertos (2:1) 10GbE (X2); logrando como máximo: 40 puertos 10/100/1000 (RJ-45) distribuidos en dos módulos de 20; 16 puertos a 10 Gigabit Ethernet (RJ-45); 24 puertos a 10 Gigabit Ethernet (fibra); 32 puertos a Gigabit Ethernet (fibra)	14 puertos SFP+ de 10 Gbps, dúplex; 2 ranuras para módulos ampliados; 4 puertos RJ-45 10/100/1000 de negociación automática (IEEE 802.3 tipo 10BASE-T, IEEE 802.3u tipo 100BASE-TX, IEEE 802.3ab tipo 1000BASE-T); 1 puerto RJ-45 para consola; admite un máximo de 14 puertos SFP+	20 puertos 10/100/1000Base-T, 4 puertos *autosensing* 10/100/1000BASE-T o SFP GbE, 2 subtarjetas 10GE XFP y 4 subtarjetas 10GE SFP+
Modular	Si, dos slots modulares	No	No
Interfaces adicionales	1 tarjeta WS-X49020-GB-RJ45 y 1 tarjeta WS-X4904-10GE	4 *Transceiver* HP X130 10G SFP+ LC SR	4 puertos GE SFP ópticos (usados en Serie incluyendo 4 puertos SFP-GE-LX-SM1310 ópticos LS5D00E4GF01, *Extend Channel Card* of ES5D00ETPB00)
Rendimiento			
Throughput	250 Mpps para IPv4 y 125 Mpps para IPv6	363 Mpps	96 Mpps
Capacidad de envío y conmutación	320 Gbps	488 Gbps	128 Gbps
Memoria y Procesamiento			
Capacidades de las memorias y búferes	512 MB de memoria *flash*; tamaño del búfer de paquetes: 128 MB	SDRAM de 1024 MB, tamaño del búfer de paquetes: 2 MB, 512 MB de memoria *flash*	256 MB de memoria *flash*; tamaño del búfer de paquetes: 2 MB
Conectividad			
IPv4	Enrutamiento estático, RIP, OSPF, IS-IS, BGPv4	Enrutamiento estático, RIP, OSPF, IS-IS	Enrutamiento OSPF, IS-IS, BGP

IPv6	Enrutamiento estático en IPv6, RIPng, OSPFv3, IS-ISv6, BGPv4 +	Enrutamiento estático en IPv6, RIPng, OSPFv3, IS-ISv6	Soporte de OSPFv3, RIPng, túneles manuales, túneles 6-a-4 y túneles ISTAP
Power over Ethernet	No	No	No
Características de capa 2			
Spanning- Tree	IEEE 802.1d *Spanning Tree Protocol*, IEEE 802.1s *Multiple Spanning Tree Protocol* (MSTP)	Soporte a *spanning Tree*/MSTP, RSTP y STP *Root Guard*	Soporte de STP, RSTP y MSTP
Manejo de VLANs	VLAN *Switching*; manejo de 4k entradas	Soporte de 4094 VLAN	VLAN *Switching*; manejo 4096 entradas
Calidad de Servicio			
QoS	Soporte de FIFO, PQ, CQ, WFQ, CBQ, RTPQ, *traffic shaping,* FR QoS, *Weighted Random Early Detection* (WRED)/RED	Tecnologías soportadas: SP, WRR, WFQ, WRED, WDRR y SP+WDRR	Soporte de FIFO, PQ, CQ, WFQ, CBQ, RTPQ, WRED y RED
Estándar de prioridad	*Class of Service* (CoS) IEEE 802.1p	*Class of Service* (CoS) IEEE 802.1p	*Class of Service* (CoS) IEEE 802.1p priority tag
Costo			
sin IVA	14.840,80 USD	12.466,02 USD	8.940,70 USD
Garantía e información adicional			
Tiempo de entrega, validez de la oferta y garantía	El tiempo de entrega: previa verificación de *stock* a la fecha de la orden de compra. Validez de la oferta: 15 días. Los precios no incluyen instalación ni configuración de hardware ni software	Garantía de 1 año con reemplazo de dispositivos previo anticipo. Validez de la oferta: 10 días del calendario. Soporte por teléfono. Tiempo de entrega: previa verificación de stock	Validez de la oferta: 1 mes. Tiempo de entrega: 45 a 60 días con la Orden de Compra. Garantía: 1 año. Los precios no incluyen instalación, ni configuración, este servicio se lo determina previa definición del alcance de los mismos

Tabla 3.20 Cuadro comparativo: agregadores

Se seleccionará dispositivo que mejor se adapte a los requerimientos del rediseño, a través de la matriz de decisión mostrada en la Tabla 3.21, donde los grados de importancia se definieron como: 22% para la redundancia debido a que estos equipos pertenecen a la capa de distribución donde la disponibilidad es importante, 18% para la capacidad de envío y 15% para el *throughput* para enviar la información a alta velocidad, 15% para la memoria y procesamiento, 10% para la capacidad de *slots* ya que no se necesita gran densidad de puertos como en los switches de acceso, 10% para la inversión y 10% para la garantía.

MODELO DEL DISPOSITIVO		CISCO		HP		HUAWEI	
		Catalyst WS-4900M		HP 5820-14XG-SFP+ (JC106A)		S5328C-EI-24S	
CRITERIO DE SELECCIÓN	GRADO DE IMPORTANCIA	G. PERT (0-10)	APROB.	G. PERT (0-10)	APROB.	G. PERT (0-10)	APROB.
Capacidad de slots	10%	10	1	7	0,7	8	0,8
Redundancia	22%	8	1,76	4	0,88	5	1,1
Throughput	15%	8	1,2	10	1,5	3	0,45
Capacidad de envío y conmutación	18%	8	1,44	10	1,8	3	0,54
Memoria y Procesamiento	15%	8	1,2	10	1,5	6	0,9
Inversión	10%	6	0,6	7	0,7	10	1
Garantía	10%	10	1	10	1	10	1
Total	**100%**	**Total P1:**	**8,2**	**Total P2:**	**8,08**	**Total P3:**	**5,79**

Tabla 3.21 Matriz de decisión: agregadores

Según los resultados obtenidos en el análisis de la Tabla 3.21, se selecciona el switch Catalyst WS-4900M ya que presenta la mejor aprobación con un total de 8,20/10. Presenta altas capacidades de conmutación y envío de paquetes, es modular y tiene soporte a IPv6 y QoS, entre otras características.

3.8.3. CAPA ACCESO[5][32][38][40]

La capa acceso requiere entre otras características, alta densidad de puertos y soporte a la plantilla SDM de doble pila. Según el análisis de la sección 3.7.3, se requieren dispositivos más robustos ya que actualizar el IOS no será suficiente para soportar IPv6 *forwarding*. En la Tabla 3.22 se indica el cuadro comparativo de tres switches de acceso.

MODELO DEL DISPOSITIVO	CISCO	HP	HUAWEI
	3560v2-48TS	HP 5500-48G EI Switch with 2 Interface Slots (JD375A)	S5352C-EI
Puertos			
Tipo de interfaces	48 puertos *Ethernet* 10/100 y 4 puertos SFP *Gigabit Ethernet*; 1RU	48 puertos RJ-45 *autosensing* 10/100/1000 (IEEE 802.3 Type 10BASE-T, IEEE 802.3u *Type* 100BASE-TX, IEEE 802.3ab Type 1000BASE-T), 4 puertos *autosensing* 10/100/1000BASE-T o SFP y 1 puerto de consola RJ-45	48 puertos 10/100/1000Base-T, 2 subtarjetas 10GE XFP y 4 subtarjetas 1000Base-X SFP
Rendimiento			
Throughput	Sobre los 13.1 Mpps	Sobre los 142.9 Mpps	132 Mpps
Capacidad de envío y conmutación	32 Gbps	192 Gbps	176 Gbps
Memoria y Procesamiento			
Capacidades de las memorias y búferes	512 KB de memoria *flash*; tamaño del búfer de paquetes: 512 KB	256 MB SDRAM; *flash* de 32 MB ; tamaño del buffer de paquetes: 4 MB	512 KB de memoria *flash*; tamaño del búfer de paquetes: 500 KB
Conectividad			
IPv4	Protocolos de enrutamiento dinámico: RIP, OSPF, IS-IS y BGP-4	Enrutamiento en capa 3 con soporte a rutas estáticas, RIP, OSPF, IS-IS y BGP	Enrutamiento OSPF, IS-IS, BGP
IPv6	Enrutamiento en IPv6 (estático, RIPng, OSPFv3 y EIGRP para IPv6) y soporte de IPv6 ACLs	Enrutamiento en IPv6 con soporte a rutas estáticas, RIPng, OSPFv3, IS-ISv6 y BGP4+ for IPv6; ACLs en IPv6	Soporte de OSPFv3, RIPng, túneles manuales, túneles 6-a-4 y túneles ISTAP
***Power* over Ethernet**	No	No	No
Características de capa 2			
Spanning- Tree	IEEE 802.1d *Spanning Tree Protocol*, IEEE 802.1s *Multiple Spanning Tree Protocol* (MSTP)	*Spanning Tree*/MSTP, RSTP y 10 GbE *port aggregation*	Soporte de STP, RSTP y MSTP
Manejo de VLANs	VLAN *Switching*; manejo de 4k entradas	VLAN *Switching*; manejo 4096 entradas	VLAN *Switching*; manejo 4096 entradas
Calidad de Servicio			

QoS	Soporte de FIFO, PQ, CQ, WFQ, CBQ, RTPQ, *traffic shaping*, FR QoS, *Weighted Random Early Detection* (WRED)/RED	*Traffic Policing,* clasificación avanzada de QoS: basada en ACLs, IEEE 802.1p, IP, DSCP or ToS precedence; soporte de las acciones de congestión: *strict priority queuing* (SP), *weighted round robin* (WRR), SP+WRR, *weighted fair queuing* (WFQ) y *weighted random early discard* (WRED)	Soporte de FIFO, PQ, CQ, WFQ, CBQ, RTPQ, WRED y RED
Estándar de prioridad	*Class of Service* (CoS) IEEE 802.1p	*Class of Service* (CoS) IEEE 802.1p	*Class of Service* (CoS) IEEE 802.1p priority tag
Costo			
sin IVA	7.511,91 USD	5.840,49 USD	4.374,08 USD
Garantía e información adicional			
Tiempo de entrega, validez de la oferta y garantía	El tiempo de entrega: previa verificación de *stock* a la fecha de la orden de compra. Validez de la oferta: 15 días. Los precios no incluyen instalación ni configuración de hardware ni software	Garantía de 1 año con reemplazo de dispositivos previo anticipo. Validez de la oferta: 10 días del calendario. Soporte por teléfono. Tiempo de entrega: previa verificación de stock	Validez de la oferta: 1 mes. Tiempo de entrega: 45 a 60 días con la Orden de Compra. Garantía: 1 año. Los precios no incluyen instalación, ni configuración, este servicio se lo determina previa definición del alcance de los mismos

Tabla 3.22 Cuadro comparativo: switches de acceso

Después de comparar las principales características de los switches de la Tabla 3.22, se seleccionará el dispositivo que cumpla con los requerimientos del rediseño, mediante la matriz de decisión mostrada en la Tabla 3.23.

Los grados de importancia de los criterios de selección se definen con: 22% para la capacidad de puertos debido estos equipos pertenecerán a la capa de acceso de la red, 15% para la capacidad de envío y 15% para el *throughput* ya que se necesitan equipos robustos que envíen la información a alta velocidad, 15% para la memoria y procesamiento, 13% para la redundancia porque no son dispositivos cruciales para el desempeño de la red como los LER o LSR, 10% para la inversión y 10% para la garantía.

MODELO DEL DISPOSITIVO		CISCO		HP		HUAWEI	
		3560v2-48TS		HP 5500-48G (JD375A)		S5352C-EI	
CRITERIO DE SELECCIÓN	GRADO DE IMPORTANCIA	G. PERT (0-10)	APROB.	G. PERT (0-10)	APROB.	G. PERT (0-10)	APROB.
Capacidad de puertos	22%	9	1,98	9	1,98	10	2,2
Redundancia	13%	0	0	0	0	0	0
Throughput	15%	2	0,3	10	1,5	9	1,35
Capacidad de envío	15%	2	0,3	10	1,5	9	1,35
Memoria y procesamiento	15%	4	0,6	10	1,5	3	0,45
Inversión	10%	7	0,7	8	0,8	10	1
Garantía	10%	10	1	10	1	10	1
Total	**100%**	**Total P1:**	**4,88**	**Total P2:**	**8,28**	**Total P3:**	**7,35**

Tabla 3.23 Matriz de decisión: switches de acceso

Se selecciona el switch HP 5500-48G ya que presenta el mayor valor de aprobación (8,28/10) según la matriz de decisión de la Tabla 3.23. Este switch tiene soporte a IPv6 *forwarding* y QoS, así como alta densidad de puertos.

3.9. COSTOS REFERENCIALES

En la presente sección se realizará el cálculo de los costos referenciales para los dispositivos a utilizarse en el rediseño de la red MPLS de Telconet S.A.-Quito, con fin de tener una idea de la inversión económica a realizar.

Las cotizaciones de los productos se obtuvieron de los distribuidores autorizados en Ecuador de las marcas: Cisco Systems, Inc., Hewlett-Packard y Huawei Technologies Co. Ltd; y se muestran en el ANEXO D.

En la Tabla 3.24 se presentan los costos referenciales del hardware y software requerido en la sección 3.8, detallando las cantidades, los precios unitarios y totales de cada producto.

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO (USD)	PRECIO TOTAL (USD)
Router Cisco 7609S	**3**	**77.408,47**	**232.225,41**
Chassis 7609S-RSP720CXL-R; 2 mod WS-X6704-10GE; 2 mod SPA-2X1GE-V2			
Switch Catalyst WS-4900M	**8**	**14.840,80**	**118.726,36**
Chassis WS-4900M; 1 mod WS-X49020-GB-RJ45; 1 mod WS-X4904-10GE			
Switch HP 5500-48G EI	**142**	**5.840,49**	**829.350,02**
Switch HP 5500-48G EI with 2 Interface Slots (JD375A)			
Software IOS 15.0(1)M7	**2**	**3.980,38**	**7.960,76**
Software 7206VXR (NPE-G2), versión IOS 15.0(1)M7			
Module WS-X6704-10GE	**7**	**7.754,37**	**54.280,59**
Módulo de 4 puertos 10 *Gigabit Ethernet* WS-X6704-10GE			
Module SPA-2X1GE-V2	**2**	**4.330,17**	**8.660,34**
Módulo de 4 puertos *Gigabit Ethernet Shared Adapter* SPA-2X1GE-V2			
OBSERVACIONES -Validez de la oferta: 10 días		**SUBTOTAL**	**1'251.203,48**
		IVA (12%)	**150.144,42**
		TOTAL	**1'401.347,90**

Tabla 3.24 Costos referenciales

Para la capa núcleo se analizan 3 routers LER, 2 licencias de IOS para el router 7206VXR (NPE-G2), 7 módulos de interfaces de 10 Gbps y dos de 1 Gbps para brindar redundancia de puertos; en la capa distribución se requieren 8 agregadores; y 142 switches de 48 puertos, para la capa acceso.

Los costos detallados en la Tabla 3.24 fueron cotizados durante los meses de noviembre y diciembre de 2012 y tienen una vigencia de 10 días. Los precios pueden diferir según la fecha, el distribuidor y la cantidad de los dispositivos que se analicen en la cotización; es por ello que, los valores indicados son referenciales.

REFERENCIAS BIBLIOGRÁFICAS

CAPÍTULO 3

LIBROS Y MANUALES

[1] ANÓNIMO, “Implementing Cisco Quality of Service”. *Student Guide* Cisco *Systems*, Inc. Versión 2.2. Volúmenes 1 y 2. 2006.

[2] TIPÁN, Milton. “Diagrama de Red MPLS Quito-Telconet S.A.”. PROY 06 Ver 17-02-2012. Quito, Ecuador. Febrero, 2011.

[3] ALMEIDA ARCOS, Andrés. “BGP y Calidad de Servicio en Redes Convergentes”. Academia de Certificaciones Internacionales en Redes y Tecnologías de Información ACIERTE-EPN. Quito, Ecuador. Junio, 2011.

[4] ANÓNIMO. “Conceptos y Protocolos de Enrutamiento - CCNA 2”. Academia de red Cisco. Módulo dos. Cuarta edición. Capítulos 4 y 5. Madrid, España. 2007-2008.

[5] ANÓNIMO, “Portable Product Sheet – Switch Perf”. *Catalyst Switching Performance.* Cisco *Systems* Inc. 25 de agosto de 2005.

[6] ANÓNIMO, “Portable Product Sheet – Router Perf”. *Router Switching Performance in Packets Per Second (PPS).* Cisco *Systems* Inc. 15 de diciembre de 2006.

[7] ANÓNIMO. “Conmutación y Conexión Inalámbrica de LAN - CCNA3”. Academia de red Cisco. Módulo cuatro. Cuarta edición. Capítulo 1. Madrid, España. 2007-2008.

[8] ANÓNIMO. “Acceso a la WAN - CCNA 4”. Academia de red Cisco. Módulo cuatro. Cuarta edición. Capítulos 4 y 7. Madrid, España. 2007-2008.

[9] ANÓNIMO. “Acceso a la WAN - CCNA 4”. Academia de red Cisco. Módulo cuatro. Cuarta edición. Capítulos 7. Madrid, España. 2007-2008.

PROYECTOS DE TITULACIÓN

[10] NIETO PORRAS, Luisana Bertilda. “Diseño y Configuración de Calidad de Servicio en la Tecnología MPLS para un Proveedor de Servicios de Internet”. EPN. Mayo, 2010.

[11] MARCHÁN MERINO, Julia Soledad. YÁNEZ QUINTANA, Daniel Alfonso. “Estudio y Diseño para la Migración de una Red Gigabit Ethernet de datos de una Empresa Portadora de Servicios a la Tecnología MPLS (Multiprotocol Label Switching)”. Abril, 2008.

DIRECCIONES ELECTRÓNICAS

[12] ANÓNIMO. “MPLS Traffic Engineering”. Cisco IOS Software Releases 12.2S. Cisco Systems.
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/TE_1208S.html

[13] ANÓNIMO. “Configuring Quality of Service for MPLS Traffic”. Cisco 10000 Series Router Calidad de Servicio: Guía de Configuración. Cisco Systems.
http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/qos/10qmpls.html

[14] ANÓNIMO. “MPLS Label Distribution Protocol” Cisco IOS Software Releases 12.2 T. Cisco Systems.
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ft_ldp7t.html

[15] ANÓNIMO. “Configuring IP Version 6”. Cisco 10000 Series Router Calidad de Servicio: Guía de Configuración. Cisco Systems.
http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/broadband/ipv6.html

[16] ANÓNIMO. “Cisco Catalyst 3550 Series Intelligent Ethernet Switches”. Cisco Systems, Inc. 1992–2008.
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps646/product_data_sheet09186a00800913d7.html

[17] ANÓNIMO. “Cisco Catalyst 6500 and 6500-E Series Datasheet”. Cisco Systems, Inc. 2009.
http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a00800ff916_ps708_Products_Data_Sheet.html

[18] ANÓNIMO. “Cisco 7609 Chassis”. Cisco Systems, Inc. 1992-2006.
http://www.cisco.com/en/US/prod/collateral/routers/ps368/ps367/product_data_sheet09186a0080169ead_ps368_Products_Data_Sheet.html

[19] ANÓNIMO. “Cisco IOS Router IPv6”. IPv6INT.NET. Enero, 2012.
http://ipv6int.net/systems/cisco_ios_router-ipv6.html

[20] DELFINO, Adrián. RIVERO, Sebastián. SAN MARTÍN, Marcelo. BELZARENA, Pablo. “Ingeniería de Tráfico en Redes MPLS”. Instituto de Ingeniería Eléctrica, Facultad de Ingeniería de la República. Agosto, 2005.
http://iie.fing.edu.uy/investigacion/grupos/artes/fce/nette/Ingenieria_de_Trafico_en_Redes_MPLS.pdf

[21] CLAUBERG, Axel. “Deploying IPv6 Networks Cisco”, Session RST-231. Cisco IOS Software. 2002.
http://www.ipv6-es.com/02/docs/patrick_grossetete_1.pdf

[22] VIVES, Álvaro. “Despliegue de IPv6”. WALC2011. Guayaquil, Ecuador. 10-14 de octubre de 2011.
http://www.6deploy.eu/workshops2/20111010_guayaquil_ecuador/DIA5-1-2-Consulintel _Curso-IPv6_WALC2011.pdf

[23] LIAKOPOULOS, Athanassios. “IPv6 over IPv4/MPLS Networks: The 6PE Approach”. III Global IPv6 Summit. Greek Research & Technology Network (GRNET). Moscow, Rusia. 25 de noviembre de 2004.
http://www.free.net/NTL/IP6/presentation/ALiakopoulos%20-%206PE%20-%203rd%20Global%20IPv6%20Summit.pdf

[24] ANÓNIMO. “Cisco IOS IPv6 Provider Edge Router (6PE) over MPLS”. Cisco IOS Software Releases 12.2 Mainline.

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_data_sheet09186a008052edd3.html

[25] GROSSETET, Patrick. “IPv6 over MPLS: Cisco IPv6 Provider, Edge Router (6PE), Cisco IPv6 VPN, Provider Edge y Router (6VPE)”. Cisco Systems, Inc. Estados Unidos de América. 2006. http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/prod_presentation0900aecd80311df4.pdf

[26] ANÓNIMO. “Políticas para la Distribución y Asignación de Direcciones IPv6”. Manual de Políticas de LACNIC. Capítulo 4 v1.9 – 23/05/2012. http://lacnic.net/sp/politicas/manual5.html

[27] ANÓNIMO. “IAB/IESG Recommendations on IPv6 Address Allocations to Sites”. Network Working Group. RFC 3177. Septiembre, 2001. http://tools.ietf.org/html/rfc3177

[28] NARTEN, T. HUSTON, G. ROBERTS, L. “IPv6 Address Assignment to End Sites”. Internet Engineering Task Force (IETF). RFC 6177. Marzo, 2011. http://tools.ietf.org/html/rfc6177

[29] ANÓNIMO. “Cisco 7200 VXR Series Routers Overview”. Cisco Systems, Inc. 1992–2008. http://www.cisco.com/en/US/prod/collateral/routers/ps341/data_sheet_c78_339749.pdf

[30] ANÓNIMO. “Cisco Catalyst 3750 Series Switches”. Cisco Systems, Inc. 1992–2008. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/product_data_sheet0900aecd80371991.pdf

[31] ANÓNIMO. “Cisco Catalyst 4900M Series”. Cisco Systems, Inc. 1992–2008. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6021/ps9310/Prod_Bulletin_447737_Cat_4900M-Ex.html

[32] ANÓNIMO. “Cisco Catalyst 3560 v2 Series Switches”. Cisco Systems, Inc. 1992–2008.
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/data_sheet_c78-530976.html

[33] ANÓNIMO. “Cisco Catalyst 3550 Series Intelligent Ethernet Switches”. Cisco Systems, Inc. 1992-2008.
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps646/product_data_sheet09186a00800913d7.html

[34] ANÓNIMO. “Release Notes for MPLS Cisco IOS Release 11.1(28a)CT”. Cisco Systems, Inc. 25 de febrero, 2002.
http://www.cisco.com/en/US/docs/ios/11_1/release/notes/rn111ct.pdf

[35] ANÓNIMO. “Data Center and Virtualization”. Cisco Systems, Inc. 2012.
http://www.cisco.com/en/US/netsol/ns340/ns394/ns224/index.html

[36] ANÓNIMO. “The HP 6600 Router Series feature an innovative multi-core and distributed architecture”. *Hewlett-Packard*. 2012.
http://h17007.www1.hp.com/us/en/products/routers/HP_6600_Router_Series/index.aspx

[37] ANÓNIMO. “NE40E Universal Service Router”. Huawei *Technologies* Co. Ltd. 2012.
http://www.huawei.com/ucmf/groups/public/documents/attachments/hw_132368.pdf

[38] ANÓNIMO. “The HP 5500 EI Switch Series”. *Hewlett-Packard*. 2012.
http://h17007.www1.hp.com/us/en/products/switches/HP_5500_EI_Switch_Series/index.aspx?jumpid=reg_r1002_usen_c-001_title_r0001#JD375A

[39] ANÓNIMO. “The HP 5820 Switch Series are advanced flex-chassis switches”. *Hewlett-Packard*. 2012.
http://h17007.www1.hp.com/us/en/products/switches/HP_5820_Switch_Series/index.aspx

[40] ANÓNIMO. “S5300 Switches Product Brochure”. Huawei *Technologies* Co. Ltd. 2012.
http://www.huawei.com/ucmf/groups/public/documents/attachments/hw_093970.pdf

[41] ANÓNIMO. “MPLS Virtual Private Networks (VPN)”. Cisco IOS Software Releases 12.2 T. Cisco Systems.
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftvpn13.html

CAPÍTULO 4

CONFIGURACIÓN E IMPLEMENTACIÓN DEL PROTOTIPO DE LA RED DISEÑADA

4.1. INTRODUCCIÓN

En el presente capítulo, se describirán las configuraciones necesarias para el desarrollo del esquema de MPLS con soporte para IPv6 y, a fin de comprobar el funcionamiento del diseño propuesto, se implementará un prototipo de la red considerando dos nodos en particular: Muros y Gosseal.

Las configuraciones de la red diseñada resultarían extensas y repetitivas si se detallan en su totalidad, es por ello que, serán definidas para un dispositivo de cada capa con el fin de que sirvan de guía para los restantes dispositivos.

La implementación del prototipo tendrá por objetivo corroborar las configuraciones presentadas y obtener los resultados que demuestren el correcto funcionamiento de las aplicaciones IPv6 en la red MPLS de Telconet S.A. empleando las Mejores Prácticas de Seguridad.

4.2. CONFIGURACIÓN DE LA RED DISEÑADA[2][7][21]

Una vez realizado el rediseño de la red MPLS de Telconet S.A., se procederá a describir los comandos de configuración necesarios para el desarrollo del esquema de red basándose en la topología presentada en la Figura 3.9.

Después de conectar adecuadamente los dispositivos, se deberán configurar los parámetros básicos de los dispositivos de red, como son: los nombres de *host,* la contraseña de modo EXEC, el mensaje del día, la contraseña de consola, la contraseña de las líneas de terminal virtual y las direcciones IP de las interfaces, entre otros.

Los nombres de los dispositivos se identifican en el ANEXO A, mientras que las direcciones IP serán diferentes para cada interfaz y se configurarán según las subredes definidas en la sección 3.7.4.

A continuación se presentan los comandos de configuración básica para el nodo PE1MUROS, a fin de que sirvan de guía para los restantes dispositivos de la red de Telconet S.A.-Quito.

a. Ingresar al modo EXEC privilegiado

```
Router> enable
Router#
```

b. Ingresar al modo de configuración global

```
Router# configure terminal
Router(config)#
```

c. Configurar el nombre del dispositivo

```
Router(config)# hostname PE1MUROS
PE1MUROS(config)#
```

d. Habilitar el cifrado de todas las contraseñas

```
PE1MUROS(config)# service password-encryption
```

e. Configurar el mensaje del día

```
PE1MUROS(config)# banner motd #
**********************************************************

                        ADVERTENCIA
                       ------------
 ACCESO RESTRINGIDO SOLO A PERSONAL AUTORIZADO DE TELCONET S.A.
----------------------------------------------------------------
Usted se ha conectado a un Sistema Monitoreado de TELCONET S.A.
Las  Violaciones a este sistema  son  penalizadas por la LEY DE
COMERCIO ELECTRONICO ECUATORIANA y demas LEYES INTERNACIONALES.

**********************************************************
#
```

f. Desactivar DNS[39]

```
PE1MUROS(config)#no ip domain-lookup
```

g. Configurar la contraseña del modo EXEC

```
PE1MUROS(config)# enable secret telconet
```

h. Configurar la contraseña de consola

```
PE1MUROS(config)#line console 0
PE1MUROS(config-line)#password telconet
PE1MUROS(config-line)#login
```

Para evita que la presentación de los mensajes de *logs* se distorsione:

```
PE1MUROS(config-line)#logging synchronous
```

i. Configurar la contraseña de las líneas de terminal virtual

```
PE1MUROS(config)#line vty 0 4
PE1MUROS(config-line)#password telconet
PE1MUROS(config-line)#login
PE1MUROS(config-line)#logging synchronous
```

j. Configurar el sistema de autenticación basado en usuarios y contraseñas[21]

```
PE1MUROS(config)#username telconetuio privilege 15 secret
telconetuio
PE1MUROS(config)#username test privilege 15 secret test
PE1MUROS(config)#username laguirre privilege 15 secret laguirre
```

Para la activación del sistema de autenticación basado en usuarios y contraseñas, es necesario modificar las configuraciones anteriores de las líneas: consola y vty, como se indican a continuación:

```
PE1MUROS(config)#line con 0
PE1MUROS(config-line)#login local
PE1MUROS(config-line)#logging synchronous
PE1MUROS(config-line)#exit
```

[39] Es importante desactivar el *Domain Name System* (DNS) en los dispositivos de laboratorio porque de esta manera, se evitará la espera del sistema de traducción de dominios ante un error de escritura de los comandos.

```
PE1MUROS(config)#line vty 0 15
PE1MUROS(config-line)#login local
PE1MUROS(config-line)#exec-timeout 30
PE1MUROS(config-line)#logging synchronous
PE1MUROS(config-line)#exit
```

k. Configurar la interfaz GigabitEthernet 0/0 con la dirección IP

```
PE1MUROS(config)# interface gigabitethernet 0/0
PE1MUROS(config-if)#description LINK TO PGOSSEAL
PE1MUROS(config-if)#ip address 192.168.1.1 255.255.255.0
```

Habilitar la interfaz

```
PE1MUROS(config-if)#no shutdown
```

Crear la interfaz *loopback* que se usará como identificador del equipo de red

```
PE1MUROS(config)# interface loopback 0
PE1MUROS(config-line)#ip address 1.1.1.1 255.255.255.255
```

l. Guardar la configuración en la NVRAM

```
PE1MUROS# copy running-config startup-config
```

4.2.1. CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO OSPF[7]

El protocolo de enrutamiento dinámico seleccionado es OSPF y se establecerá con el AS 27947 asignado a Telconet S.A. por el LACNIC. Las sesiones OSPF serán identificadas mediante los *router-id* configurados en cada dispositivo de la red con la dirección IP de la interfaz *loopback0.*

Las redes directamente conectadas que intervienen y que serán publicadas en el proceso de enrutamiento, siguen el formato: “network <dirección IP> <máscara wildcard> area 0”, donde: la máscara *wildcard* es la inversa binaria de la máscara normal, es decir, se cambian los bits 1L por 0L y viceversa; el área OSPF tiene el valor (0) en todos los routers configurados, a fin de indicar los dispositivos que compartirán la información de los estados de enlaces.

Los siguientes comandos deben configurarse solo en los dispositivos de la capa núcleo de la red de Telconet S.A., como son: los LER y los LSR.

a. Configurar OSPF

```
PE1MUROS(config)#router ospf 27947
PE1MUROS(config-router)#router-id 1.1.1.1
PE1MUROS(config-router)#network 192.168.1.0 0.0.0.255 area 0
PE1MUROS(config-router)#network 1.1.1.1 0.0.0.0 area 0
```

b. Verificar

```
PE1MUROS#show ip ospf neighbor
PE1MUROS#show ip route
```

4.2.2. CONFIGURACIÓN DE LAS VLAN EN LOS SWITCHES[7]

Las configuraciones de los switches se centran en establecer las VLAN, a fin de poder diferenciar los servicios ofertados y el tráfico de cada cliente. Los switches de la capa distribución serán configurados en la VLAN administrativa, mientras los switches de la capa de acceso tendrán soporte a varias VLAN, de acuerdo al número de clientes que manejen.

A continuación se presentan las configuraciones de las VLAN en el SW1COLON, de tal manera que sirva de guía para los restantes switches de la red.

a. Deshabilitar todas las interfaces como medida de seguridad y habilitar solo las requeridas

```
SW1COLON(config)#interface range fa0/1 – 48
SW1COLON(config-if)#shutdown
SW1COLON(config)#interface range gi0/1 – 4
SW1COLON(config-range)#shutdown
SW1COLON(config)#interface range fa0/1 - 3, fa0/10 - 13, fa0/20
- 23, fa0/30 – 33, g0/1
SW1COLON(config-range)#no shutdown
```

b. Determinar las interfaces troncales y definir las VLAN permitidas

```
SW1COLON(config)#interface range fa0/1 - 9, gi0/1
SW1COLON(config-if)#switchport trunk encapsulation dot1q
SW1COLON(config-if)#switchport mode trunk
SW1COLON(config-if)#switchport trunk native vlan 129
SW1COLON(config-if)#switchport trunk allowed vlan 11,22,129,100
```

c. Definir las VLAN y asignarlas con un nombre descriptivo

```
SW1COLON(config)#vlan 11
SW1COLON(config-vlan)#name CLIENTE
SW1COLON(config)#vlan 22
SW1COLON(config-vlan)#name INTERNET
SW1COLON(config)#vlan 129
SW1COLON(config-vlan)#name NATIVA/GESTION
SW1COLON(config)#vlan 100
SW1COLON(config-vlan)#name CLIENTE_VPNL2
```

d. Asignar una dirección IP para la administración del switch

```
SW1COLON(config)#interface vlan 129
SW1COLON(config-if)#ip address 10.2.41.2 255.255.255.0
SW1COLON(config-if)#no shutdown
```

e. Definir las interfaces de acceso con las VLAN respectivas

```
SW1COLON(config)#interface range fa0/10 -  19
SW1COLON(config-range)#switchport mode access
SW1COLON(config-range)#switchport access vlan 11
SW1COLON(config)#interface range fa0/20 - 29
SW1COLON(config-range)#switchport mode access
SW1COLON(config-range)#switchport access vlan 22
SW1COLON(config)#interface range fa0/10 -  19
SW1COLON(config-range)#switchport mode access
SW1COLON(config-range)#switchport access vlan 100
SW1COLON(config-range)#end
```

f. Configurar el *default gateway*

```
SW1COLON(config)#ip default-gateway 10.2.41.1
```

g. Verificar la correcta configuración

```
SW1COLON#show vlan
SW1COLON#show interface truck
```

4.2.3. CONFIGURACIÓN DE LA TECNOLOGÍA MPLS[1][3][4][15]

Para configurar MPLS en un dispositivo, es necesario primero habilitar *Cisco Express Forwarding* (CEF) y el protocolo *Label Distribution Protocol* (LDP). Los comandos mostrados a continuación deben ser configurados en los routers LER y LSR de la red MPLS.

a. Habilitar CEF

CEF mejora la conmutación de los paquetes a su destino en base a la información de la Tabla de información de envío FIB.

```
PE1MUROS(config)#ip cef
```

b. Habilitar LDP

LDP debe ser habilitado en el modo de configuración global y en cada interfaz MPLS.

En el modo de configuración global

```
PE1MUROS(config)#mpls label protocol ldp
```

En el modo de configuración específica

```
PE1MUROS(config-if)#mpls label protocol ldp
```

Definición del router-id de las sesiones LDP

```
PE1MUROS(config)#mpls ldp router-id loopback 0 force
```

Definición del rango de etiquetas a utilizar

```
PE1MUROS(config)#mpls label range 16 1000
```

c. Habilitar MPLS

En el modo de configuración específica de las interfaces

```
PE1MUROS(config-if)#mpls ip
```

d. Verificar la configuración de MPLS

```
PE1MUROS#show mpls forwarding-table
```

```
PE1MUROS#show mpls ldp bindings
PE1MUROS#show mpls ldp parameters
PE1MUROS#show mpls ldp neighbor
```

4.2.4. CONFIGURACIÓN DE MP-BGP[4][6]

Las sesiones MP-BGP deben establecerse solo entre los routers LER que desean comunicarse, como se indica a continuación:

a. Habilitar BGP y definir un vecino

El AS registrado por Telconet S.A. es 27947 y será utilizado para establecer la configuración del protocolo BGP.

```
PE1MUROS(config)#router bgp 27947
```
[40]

El identificador de la sesiones BGP de cada dispositivo será la *loopback0*

```
PE1MUROS(config-router)#bgp router-id 1.1.1.1
```

El comando "neighbor" se asocia con la dirección IP remota que puede ser la *loopback0* que identifica al router remoto. En una sesión iBGP el comando "remote-as" se establece con el AS propio del ISP, mientras en una sesión eBGP se utiliza el AS del ISP remoto.

```
PE1MUROS(config-router)#neighbor 5.5.5.5 remote-as 27947
```

b. Configurar las actualizaciones BGP

Los procesos BGP deben identificar una interfaz como fuente de las actualizaciones. Usualmente se estable una interfaz loopback debido a que siempre estará activa, y con ello, mantendrá la sesión BGP activa

```
PE1MUROS(config-router)#neighbor 5.5.5.5 update-source
loopback0
```

c. Activar la sesión VPNv4

Permite establecer los parámetros de las VPNv4, convirtiendo al protocolo BGP en MP-BGP.

```
PE1MUROS(config-router)#address-family vpnv4
```

[40] Para consultar el proveedor al que pertenece un determinado AS se puede acceder a la referencia: http://ipduh.com/ip/whois/as/

Después de activar la sesión es necesario definir como siguiente salto “next-hop-self” al vecino MPLS donde se originó la ruta, y habilitar el transporte de las comunidades: estándar y extendidas “both” en una sesión iBGP.

```
PE1MUROS(config-router-af)#neighbor 5.5.5.5 activate
PE1MUROS(config-router-af)#neighbor 5.5.5.5 next-hop-self
PE1MUROS(config-router-af)#neighbor 5.5.5.5 send-community both
```

d. Verificar la sesión MP-BGP

Los comandos que permiten ver si la sesión BGP está habilitada, son:

```
PE1MUROS#show ip bgp all summary
PE1MUROS#show ip bgp vpnv4 all summary
```

4.2.5. CONFIGURACIONES DE IPv6 EN ROUTER PE (6PE/6VPE)

En las secciones 4.2.5.1 y 4.2.5.2, se presentan los comandos de configuración para levantar el mecanismo 6PE y 6VPE respectivamente.

4.2.5.1. Configuración de 6PE[16]

Previa a la configuración de 6PE, es necesario que la red cuente con el protocolo de enrutamiento dinámico OSPF, CEF, el protocolo de distribución de etiquetas LDP y la tecnología MPLS.

A continuación se presentan los comandos para brindar servicios IPv6 en redes MPLS. Estos comandos deben ser configurados en los router LER que necesiten establecer comunicaciones IPv6.

a. Habilitar el enrutamiento IPv6

El siguiente comando debe ser configurado en los routers LER de la red IPv6

```
PE1MUROS(config)#ipv6 unicast-routing
```

b. Habilitar CEF en IPv6

Al igual que en IPv4, CEF trabaja con MPLS y también debe habilitarse para IPv6.

```
PE1MUROS(config)#ipv6 cef
```

c. Habilitar MP-BGP

Se establece una sesión iBGP con el PE remoto y se establecen las familias de direcciones en IPv4 e IPv6.

```
PE1MUROS(config)#router bgp 27947
PE1MUROS(config-router)#bgp router-id 1.1.1.1
PE1MUROS(config-router)#neig 5.5.5.5 remote-as 27947
PE1MUROS(config-router)#neig 5.5.5.5 update-source loopb 0
PE1MUROS(config-router)#neig 5.5.5.5 next-hop-self
PE1MUROS(config-router)#neig 5.5.5.5 version 4
PE1MUROS(config-router)#neig 5.5.5.5 description LINK-BGP TO
PE1GOSSEAL
PE1MUROS(config-router)#no bgp default ipv4-unicast
```

Definición de la familia de direcciones IPv6 con la redistribución de las redes conectadas y estáticas

```
PE1MUROS(config-router)#address-family ipv6
PE1MUROS(config-router-af)#no synchronization
PE1MUROS(config-router-af)#net 2001:29:2:41::0/64
PE1MUROS(config-router-af)#redistribute connected
PE1MUROS(config-router-af)#redistribute static
PE1MUROS(config-router-af)#neighbor 5.5.5.5 activate
PE1MUROS(config-router-af)#neighbor 5.5.5.5 send-label
```

Definición de la familia de direcciones IPv4 con la redistribución de las redes conectadas y estáticas

```
PE1MUROS(config-router)#address-family ipv4
PE1MUROS(config-router-af)#no synchronization
PE1MUROS(config-router-af)#neighbor 5.5.5.5 activate
PE1MUROS(config-router-af)#neighbor 5.5.5.5 next-hop-self
PE1MUROS(config-router-af)#redistribute connected
PE1MUROS(config-router-af)#redistribute static
PE1MUROS(config-router-af)#net 10.2.41.0 mask 255.255.255.0
PE1MUROS(config-router-af)#no auto-summary
PE1MUROS(config-router-af)#exit-address-family
```

d. Configurar las interfaces en el LER

```
PE1MUROS(config)#interface gi0/1
PE1MUROS(config-if)#description LINK TO SW1COLON
PE1MUROS(config-if)#no shutdown
PE1MUROS(config)#interface gi0/1.129
PE1MUROS(config-if)#description SUBINTERFACE TO NATIVA/GESTION
PE1MUROS(config-if)#encapsulation dot1Q 129 native
PE1MUROS(config-if)#ip address 10.2.41.1 255.255.255.0
PE1MUROS(config-if)#ipv6 add 2001:29:2:41::1/64
PE1MUROS(config-if)#ipv6 enable
```

e. Verificar la configuración

Para verificar la configuración correcta se emplean los siguientes comandos:

```
PE1MUROS#show ipv6 route
PE1MUROS#show bgp vpnv6 unicast all
```

4.2.5.2. Configuración de 6VPE[16][19][20]

6VPE es el mecanismo de transición mejor adaptado para las redes MPLS. El uso de VRF en la implementación de IPv6 permite brindar mayor seguridad y escalabilidad a la red. Los sitios que manejan IPv6 pueden trabajar simultáneamente con IPv4 gracias a la facilidad de BGP y MPLS para soportar múltiples protocolos.

Para crear una dirección IPv6 única, de manera similar a IPv4, se maneja el concepto del *Route Distinguisher* (RD) de 8 bytes y se lo agrega a la dirección IPv6 de 16 bytes para obtener una VPNv6 única de 24 bytes.

Previa a la utilización de los comandos listados a continuación, se debe tener configurado OSPF, CEF, LDP y MPLS.

a. Habilitar el enrutamiento IPv6

El siguiente comando se ubica en los routers que tengan soporte para IPv6.

```
PE1MUROS(config)#ipv6 unicast-routing
```

b. Habilitar CEF en IPv6

```
PE1MUROS(config)#ipv6 cef
```

c. Crear la Tabla VRF en IPv6

Se define el nombre de la VRF. Es sensible a mayúsculas y minúsculas

```
PE1MUROS(config)#vrf definition INTERNET
```

Se define el RD siguiendo el formato: ASTelconet:VLAN

```
PE1MUROS(config-vrf)#rd 27947:22
```

Se definen los RT siguiendo el formato: ASTelconet:VLAN

```
PE1MUROS(config-vrf)#route-target export 27947:22
PE1MUROS(config-vrf)#route-target import 27947:22
PE1MUROS(config-vrf)#address-family ipv4
PE1MUROS(config-vrf)#address-family ipv6
```

d. Definir la VRF para el transporte usando BGP

El AS registrado por Telconet S.A. es 27947 y será utilizado para establecer la configuración del protocolo BGP.

```
PE1MUROS(config)#router bgp 27947
```

Establecimiento de los parámetros de la VPNv6, convirtiendo al protocolo BGP en MP-BGP.

```
PE1MUROS(config-router)#address-family vpnv6
PE1MUROS(config-router-af)#neighbor 5.5.5.5 activate
PE1MUROS(config-router-af)#neighbor 5.5.5.5 send-community both
```

La redistribución de las direcciones IP se debe establecer mediante el comando “redistribute” y el tipo de interfaz que necesita ser distribuida, por ejemplo: conectadas, estáticas y/o dinámicas.

```
PE1MUROS(config-router)#address-family ipv6 vrf INTERNET
PE1MUROS(config-router-af)#redistribute connected
PE1MUROS(config-router-af)#redistribute static
PE1MUROS(config-router-af)#network 2001:22:22:22::0/64
```

e. Configurar la interfaz en el router LER

Para habilitar la VRF, se deben asignar el nombre y las direcciones IPv4 e IPv6 a la interfaz del router LER que se conecta con el CE, como se indica a continuación:

```
PE1MUROS(config)#interface gi0/1.22
PE1MUROS(config-subif)#description SUBINTERFACE TO VRF_INTERNET
PE1MUROS(config-subif)#encapsulation dot1q 22
PE1MUROS(config-subif)#vrf forwarding INTERNET
PE1MUROS(config-subif)#ipv6 address 2001:22:22:22::1/64
PE1MUROS(config-subif)#ip address 22.22.22.1 255.255.255.0
PE1MUROS(config-subif)#no shutdown
```

f. Configurar la interfaz en el router CE

En el CE se debe configurar la dirección IP, habilitar la interfaz y crear las rutas estáticas necesarias.

```
CE1COLON_CLIENTE(config)#interface fa0/1
CE1COLON_CLIENTE(config-if)#description LINK TO SW1COLON IPv6
CE1COLON_CLIENTE(config-if)#ip address 22.22.22.10
255.255.255.0
CE1COLON_CLIENTE(config-if)#ipv6 address 2001:22:22:22::10/64
CE1COLON_CLIENTE(config-if)#no shutdown
CE1COLON_CLIENTE(config-if)#exit
CE1COLON_CLIENTE(config)#ipv6 route 2001:44:44:44::0/64
2001:22:22:22::1
CE1COLON_CLIENTE(config)#  ip  route  44.44.44.0  255.255.255.0
22.22.22.1
```

g. Comprobar la VRF configurada

Los comandos para monitorear una VRF son:

```
PE1MUROS#show ipv6 route vrf INTERNET
PE1MUROS#show ipv6 route bgp
PE1MUROS#show bgp vpnv6 unicast vrf INTERNET 2001:22:22:22::1
```

Para comprobar la VRF existente se puede ejecutar el comando *ping*.

Entre los CE desde el CE remoto:

```
CE1PLAZATOROS_CLIENTE#ping 44.44.44.10
CE1PLAZATOROS_CLIENTE#ping ipv6 2001:44.44.44.10
```

Entre los PE desde el PE remoto:

```
PE1GOSSEAL#ping vrf INTERNET 44.44.44.1
PE1GOSSEAL#ping vrf INTERNET 2001:44:44:44:1
```

4.2.6. APLICACIONES DE MPLS

Las aplicaciones de MPLS que serán analizadas son:

- Redes Privadas Virtuales
- Calidad de Servicio
- Ingeniería de Tráfico

4.2.6.1. Configuraciones de VPN de MPLS

Las VPN de MPLS pueden ser de capa 2 y capa 3 como se indican a continuación:

Las VPN de MPLS de capa 2 (VPWS)

Los siguientes comandos deben ejecutarse en los routers LER desde los cuales, se van a establecer caminos de comunicación de capa 2:

a. Configurar VPWS local

La VPWS puede ser configurada en una interfaz o subinterfaz

```
PE1MUROS(config)#interface GigabitEthernet0/1.100
PE1MUROS(config-if)#description LINK TO SW1COLON VLAN L2
```

Al ser una VLAN se debe definir la encapsulación utilizada

```
PE1MUROS(config-if)#encapsulation dot1Q 100
```

Definición del par VPWS con el VC 100 y la encapsulación MPLS

```
PE1MUROS(config-if)#xconnect 5.5.5.5 100 encapsulation mpls
PE1MUROS(config-if)#no shutdown
```

b. Configurar VPWS remoto

```
PE1GOSSEAL(config)#interface GigabitEthernet0/1.100
PE1GOSSEAL(config-if)#description LINK TO SW1PLAZATOROS VLAN L2
PE1GOSSEAL(config-if)#description encapsulation dot1Q 100
PE1GOSSEAL(config-if)# xconnect 1.1.1.1 100 encapsulation mpls
PE1GOSSEAL(config-if)# no shutdown
```

c. Verificar las configuraciones

Los comandos para comprobar el funcionamiento de las VPWS son:

```
PE1GOSSEAL(config-if)# show mpls l2transport vc 100
PE1GOSSEAL(config-if)# show mpls l2transport vc 100 detail
```

Las VPN de MPLS de capa 3 en IPv4[6][12]

Las VRF (VPN de capa 3) deben ser configuradas en los routers LER entre los cuales se establece la comunicación de capa 3. Las VRF en IPv6 ya fueron expuestas en la sección 4.2.5.2 con el mecanismo 6VPE, es por ello que se enfocará en analizar las VRF en IPv4.

a. Crear la Tabla VRF

El nombre de la VRF es sensible a mayúsculas y minúsculas.

```
PE1MUROS(config)#ip vrf CLIENTE
```

b. Definir el *Route Distinguisher* (RD)

Si el RD no se configura, la Tabla VRF no dispondrá de su ID por lo que no funcionará correctamente.

```
PE1MUROS(config-vrf)#rd 27947:11
```

c. Definir los *Route Target* (RT)

Con los RT se definen las comunidades, sea que ingresan a la Tabla VRF (*import*) o se agregarán a la dirección IPv4 para ser exportadas (*export*). Se definen los mismos formatos que el RD.

```
PE1MUROS(config-vrf)#route-target export 27947:11
PE1MUROS(config-vrf)#route-target import 27947:11
```

O de manera resumida:

```
PE1MUROS(config-vrf)#route-target both 27947:11
```

En el PE remoto se debe definir el RT *import* y/o RT *export* según corresponda.

```
PE1GOSSEAL(config)#ip vrf CLIENTE
PE1GOSSEAL(config-vrf)#rd 27947:11
```

```
PE1GOSSEAL(config-vrf)#route-target import 27947:11
PE1GOSSEAL(config-vrf)#route-target export 27947:11
```

O de manera resumida:

```
PE1GOSSEAL(config-vrf)#route-target both 27947:11
```

d. Definir la VRF para el transporte con el protocolo BGP

La redistribución de las direcciones IP se debe establecer mediante el comando “redistribute” y el tipo de interfaz que necesita ser distribuida, por ejemplo: conectadas, estáticas y/o dinámicas.

```
PE1MUROS(config)#router bgp 27947
PE1MUROS(config-router)#address-family ipv4 vrf CLIENTE
PE1MUROS(config-router-af)#redistribute connected
PE1MUROS(config-router-af)#redistribute static
PE1MUROS(config-router-af)#networ 33.33.33.0 mask 255.255.255.0
```

e. Configurar la interfaz del router LER

Una interfaz solo puede pertenecer a una y sola una VRF, mientras una VRF puede abarcar varias interfaces. Para habilitar la VRF, se debe asignar el nombre y la dirección IP respectiva a la interfaz del router LER que se conecta con el CE, como se indica a continuación:

```
PE1MUROS(config)#interface gi0/1
PE1MUROS(config-if)#description SUBINTERFACE TO VRF_CLIENTE
PE1MUROS(config-if)#no shutdown
PE1MUROS(config-if)#interface gi0/1.11
PE1MUROS(config-subif)#ip vrf forwarding CLIENTE
PE1MUROS(config-subif)#ip address 11.11.11.1 255.255.255.0
```

f. Configurar la interfaz del router CE

En el CE se debe configurar la dirección IP, habilitar la interfaz y crear las rutas estáticas necesarias o levantar un protocolo de enrutamiento dinámico.

Enrutamiento estático PE-CE

Para este mecanismo se crea una ruta estática hacia la red destino o una ruta por defecto que apunte al *gateway*. En BGP no debe faltar el comando

"redistribute static", de lo contrario la ruta estática no será publicada en la tabla VRF.

```
CE1COLON_CLIENTE(config)#interface gi0/0
CE1COLON_CLIENTE(config-if)#ip address 11.11.11.10
255.255.255.0
CE1COLON_CLIENTE(config-if)#no shutdown
CE1COLON_CLIENTE(config-if)#exit
CE1COLON_CLIENTE(config)#ip route 33.33.33.0 255.255.255.0
11.11.11.1
```

O a su vez:

```
CE1COLON_CLIENTE(config)#ip route 0.0.0.0 0.0.0.0
11.11.11.1
```

Enrutamiento dinámico OSPF PE-CE

En este mecanismo se levanta el protocolo OSPF entre el CE y el LER:

```
CE1COLON_CLIENTE(config)#router ospf 1
CE1COLON_CLIENTE(config-router)# router-id 11.11.11.10
CE1COLON_CLIENTE(config-router)#network  11.11.11.0  0.0.0.255
area 0
```

En el PE se levanta una sesión OSPF por cada VRF y se redistribuye el protocolo BGP, como se indica a continuación:

```
PE1MUROS(config)#router ospf 1 vrf CLIENTE
PE1MUROS(config-router)#router-id 11.11.11.1
PE1MUROS(config-router)#network 11.11.11.0 0.0.0.255 area 0
PE1MUROS(config-router)#redistribute bgp 27947 subnets
PE1MUROS(config-router)#redistribute connected
```

En la familia de direcciones de la VRF se redistribuye OSPF:

```
PE1MUROS(config)#router bgp 27947
PE1MUROS(config-router)#address-family ipv4 vrf CLIENTE
PE1MUROS(config-router-af)#redistribute ospf 1 vrf CLIENTE
```

g. Verificar las configuraciones

Los comandos para monitorear una VRF son:

```
PE1MUROS#show ip route vrf CLIENTE
```

```
PE1MUROS#show ip bgp vpnv4 all summary
```

Para comprobar la VRF existente se puede ejecutar el comando “ping”

Entre los CE:

```
CE1PLAZATOROS_CLIENTE#ping 11.11.11.10
```

Entre los PE:

```
PE1GOSSEAL#ping vrf CLIENTE 11.11.11.1
```

4.2.6.2. Configuración de Calidad de Servicio[5][6][8][9][10][14][17]

Una de las Mejores Prácticas[41] de Cisco en lo referente a QoS, recomienda que la clasificación y el marcado del tráfico, se establezcan lo más cercano al origen en tanto sea posible. Como Telconet S.A. tiene dominio absoluto de los routers CE, es importante brindar Calidad de Servicio desde estos dispositivos.

Los paquetes que ingresan a la red MPLS deben ser marcados previamente sea por el teléfono IP, los equipos de vídeo conferencia, u otros mecanismos donde se confíe en el marcado del cliente o se descubran las aplicaciones de la red.

El concepto de marcado desde el cliente sale del alcance de este proyecto, por lo que se indicarán los comandos que permitan brindar tratamiento diferenciado en la nube MPLS, confiando en el tráfico marcado que envía el CE. Para mayor información, se recomienda revisar el mecanismo NBAR[42].

La configuración en los equipos CISCO será *Modular* QoS CLI (MQC) ya que define clases y políticas de QoS, como se indica a continuación en las secciones 1, 2 y 3.

1. Capa núcleo: routers LER[5]

Los routers LER son la puerta de entrada hacia la nube MPLS, por lo que deben asociar los campos DSCP (IP) y EXP (MPLS) de los paquetes, para poder

[41] Para mayor información se recomienda revisar [5], Volumen 2, Capítulo 9. pág 314 y 316.

[42] *Network Based Application Recognition* (NBAR) es el mecanismo usado por determinados routers y switches Cisco para reconocer, clasificar y marcar las aplicaciones que circulan por la red. Para mayor información se recomienda revisar la referencia [22].

reenviarlos al siguiente salto con el tratamiento diferencial que les corresponda según el PHB definido.

Las políticas que deben ser configuradas en los routers LER son:

Política para limitar la capacidad de tráfico

Una medida ligera de evitar la congestión, es sin duda, limitar la capacidad de tráfico de entrada de cada cliente, a través de la definición de políticas de entrada.

a. Definir la política para limitar el tráfico en 500Kbps

El tráfico que ingresa será asociado a la clase por defecto y por lo tanto, si se supera la capacidad de 500Kbps, la política descartará el tráfico en exceso controlando la capacidad configurada.

```
PE1MUROS(config)#policy-map LIMITADAR_TRAFICO_500kbps
PE1MUROS(config-pmap)#class class-default
```

Valor CIR en bps

```
PE1MUROS(config-pmap-c)#police cir 500000
```

Acciones de transmisión y dropeo a ejecutar

```
PE1MUROS(config-pmap-c-police)#conform-action transmit
PE1MUROS(config-pmap-c-police)#exceed-action drop
PE1MUROS(config-pmap-c-police)#violate-action drop
```

b. Definir la política en la interfaz

La asociación puede ser a una interfaz física o a subinterfaces configuradas.

```
PE1MUROS(config)#interface gi0/1
PE1MUROS(config-if)# service-polic in LIMITADAR_TRAFICO_500kbps
PE1MUROS(config)#interface gi0/1.11
PE1MUROS(config-subif)#service-pol in LIMITADAR_TRAFICO_500kbps
PE1MUROS(config)#interface gi0/1.22
PE1MUROS(config-subif)#service-pol in LIMITADAR_TRAFICO_500kbps
```

c. Verificar las configuraciones

Verificar la configuración de la política

```
PE1MUROS#show policy-map
```

Verificar la configuración de la clase

```
PE1MUROS#show class-map
```

Verificar la capacidad de tráfico de entrada y/o salida en la interfaz

```
PE1MUROS#show interface gi 0/1 | i rate
```

Encerar los registros de tráfico de las interfaces

```
PE1MUROS#clear counters
```

Además, para tener un análisis de tráfico en periodos de tiempo más continuos, se utilizan los siguientes comandos que permiten reconfigurar el intervalo de tiempo en segundos.

```
PE1MUROS(config)#interface range gi 0/0 - 1
PE1MUROS(config-if)#load-interval 30
```

Política para definir el mapa de correspondencias entre los campos DSCP y EXP del paquete

En vista de que los routers LER se encuentran en la periferia de la red MPLS, son los responsables de marcar el campo EXP en base al subcampo DSCP establecido.

a. Definir los mapas de clases

Los mapas de clases agrupan los paquetes que ingresan a la red en base a un campo determinado en la Tabla 3.5, como: el valor de DSCP y/o el IP *precedence*, para asignarles un tratamiento diferenciado.

Las clases pueden establecerse como: “match-any” o “match-all” (configurado por defecto) según se requiera. “Match-all” realiza siempre todas las sentencias detalladas en la clase; mientras que “match-any” asocia una de las sentencias especificadas, como se indica a continuación:

Se crea un “class-map” por cada clase definida que asocie los paquetes IP de la red que vengan marcados con el campo *ip precedence* 6 y 7.

```
PE1MUROS(config-cmap)#class-map match-any CLASE_ROUTING_IP
```

```
PE1MUROS(config-cmap)#descrip CLASE_ENRUTAMIENTO_IP
PE1MUROS(config-cmap)#match ip  precedence  6  7
```

El mapa de clases asocia los paquetes IP de la red que tengan marcados en el subcampo DSCP el valor EF

```
PE1MUROS(config)#class-map match-any CLASE_PLATINUM_IP
PE1MUROS(config-cmap)#descrip CLASE_PLATINUM_VOZ_IP
PE1MUROS(config-cmap)#match ip dscp EF
```

El mapa de clases asocia los paquetes IP de la red que tengan marcados en el subcampo DSCP el valor AF41

```
PE1MUROS(config)#class-map match-any CLASE_GOLD_IP
PE1MUROS(config-cmap)#descrip CLASE_GOLD_VIDEOCONFERENCIA_IP
PE1MUROS(config-cmap)#match ip dscp AF41
```

El mapa de clases asocia los paquetes IP de la red que tengan marcados en el subcampo DSCP el valor AF31

```
PE1MUROS(config)#class-map match-any CLASE_SILVER_IP
PE1MUROS(config-cmap)#descrip CLASE_SILVER_CORPORATIVOS_VIP_IP
PE1MUROS(config-cmap)#match ip dscp AF31
```

El mapa de clases asocia los paquetes IP de la red que tengan marcados en el subcampo DSCP el valor AF21

```
PE1MUROS(config)#class-map match-any CLASE_BRONZE_IP
PE1MUROS(config-cmap)#descrip CLASE_BRONZE_CORPORATIVOS_IP
PE1MUROS(config-cmap)#match ip dscp AF21
```

Para comprobar la configuración de los mapas de clases:

```
PE1MUROS#show class-map
```

b. Definir los mapas de políticas

Se establece el mapa de correspondencias entre los campos DSCP y EXP de los paquetes de entrada.

```
PE1MUROS(config)#policy-map POLITICA_IP_TO_MPLS_IN
```

La política referencia las clases definidas con el comando “class”

```
PE1MUROS(config-pmap)#Class CLASE_ROUTING_IP
```

Se marca con 6 el campo EXP de las etiquetas MPLS asociadas a la CLASE_ROUTING_IP

```
PE1MUROS(config-pmap-c)#set mpls experimental imposition 6
PE1MUROS(config-pmap)#class CLASE_PLATINUM_IP
```

Se marca con 5 el campo EXP de las etiquetas MPLS asociadas a la CLASE_PLATINUM_IP

```
PE1MUROS(config-pmap-c)#set mpls experimental imposition 5
PE1MUROS(config-pmap)#class CLASE_GOLD_IP
```

Se marca con 4 el campo EXP de las etiquetas MPLS asociadas a la CLASE_GOLD_IP

```
PE1MUROS(config-pmap-c)#set mpls experimental imposition 4
PE1MUROS(config-pmap)#class CLASE_SILVER_IP
```

Se marca con 3 el campo EXP de las etiquetas MPLS asociadas a la CLASE_SILVER_IP

```
PE1MUROS(config-pmap-c)#set mpls experimental imposition 3
PE1MUROS(config-pmap)#class CLASE_BRONZE_IP
```

Se marca con 2 el campo EXP de las etiquetas MPLS asociadas a la CLASE_BRONZE_IP

```
PE1MUROS(config-pmap-c)#set mpls experimental imposition 2
PE1MUROS(config-pmap)#class class-default
```

Se marca con 0 el campo EXP de las etiquetas MPLS asociadas a la clase_default

```
PE1MUROS(config-pmap-c)#set mpls experimental imposition 0
```

Para comprobar la configuración de los mapas de políticas:

```
PE1MUROS#show policy-map POLITICA_IP_TO_MPLS_IN
```

d. Definir la política en la interfaz

Se debe configurar la política a la entrada de las interfaces de los routers LER que se conectan con los clientes.

```
PE1MUROS(config)#interface gi0/1.11
PE1MUROS(config-if)#service-policy inp POLITICA_IP_TO_MPLS_IN
PE1MUROS(config)#interface gi0/1.22
```

```
PE1MUROS(config-if)#service-policy inp POLITICA_IP_TO_MPLS_IN
```

Para comprobar la configuración de los mapas de políticas en la interfaz:

```
PE1MUROS#show policy-map int gi0/1.11
PE1MUROS#show policy-map int gi0/1.22
```

Políticas para el manejo de la congestión en dirección a los clientes

Para manejar la congestión en los routers LER, se deben definir las políticas de salida en dirección a los clientes que establecen los PHB designados a cada Clase de Servicio, como se indican a continuación:

a. Definir los mapas de políticas[23]

Se utilizan las clases previamente definidas que asocian los paquetes IP y establecen los PHB asignados a cada una de ellas.

Mapa de políticas que define los PHB de cada clase de servicio en dirección al cliente

```
PE1MUROS(config)#policy-map POLITICA_IP_TO_CLIENTE_OUT
```

La clase CLASE_ROUTING_IP tiene el 5% de ancho de banda prioritario en la red

```
PE1MUROS(config-pmap)#class CLASE_ROUTING_IP
PE1MUROS(config-pmap-c)#priority percent 5
```

La clase CLASE_PLATINUM_IP tiene el 10% de ancho de banda prioritario en la red

```
PE1MUROS(config-pmap)#class CLASE_PLATINUM_IP
PE1MUROS(config-pmap-c)#priority percent 10
```

La clase CLASE_GOLD_IP tiene un ancho de banda garantizado del 15% y una cola limitada de 100 paquetes

```
PE1MUROS(config-pmap)#class CLASE_GOLD_IP
PE1MUROS(config-pmap-c)#bandwidth percent 15
PE1MUROS(config-pmap-c)#queue-limit 100  packets
```

La clase CLASE_SILVER_IP tiene un ancho de banda garantizado del 35% y una cola limitada de 100 paquetes

```
PE1MUROS(config-pmap)#class CLASE_SILVER_IP
PE1MUROS(config-pmap-c)#bandwidth percent 35
PE1MUROS(config-pmap-c)#queue-limit 100  packets
```

La clase CLASE_BRONZE_IP tiene un ancho de banda garantizado del 30%, una cola limitada de 100 paquetes y puede aumentar su capacidad hasta un 40% del ancho de banda total del enlace con el mecanismo *traffic shaping*

```
PE1MUROS(config-pmap)#class CLASE_BRONZE_IP
PE1MUROS(config-pmap-c)#bandwidth percent 30
PE1MUROS(config-pmap-c)#queue-limit 100 packets
PE1MUROS(config-pmap-c)#shape average percent 40
```

La clase por defecto no garantiza ningún tratamiento preferencial, utiliza el ancho de banda restante de la red con un umbral máximo del 50%, y además dispone del mecanismo de evasión de la congestión WRED para el descarte de los paquetes en base al valor DSCP configurado

```
PE1MUROS(config-pmap)#class class-default
PE1MUROS(config-pmap-c)#queue-limit 100 packets
PE1MUROS(config-pmap-c)#random-detect dscp-based
PE1MUROS(config-pmap-c)#shape average percent 50
```

Para comprobar la configuración de los mapas de políticas:

```
PE1MUROS(config)#show policy-map POLITICA_IP_TO_CLIENTE_OUT
```

b. Definir la política en la interfaz

Se debe configurar la política a la salida de las interfaces de los routers LER que se conectan con los clientes.

```
PE1MUROS(config)#int gi 0/1
PE1MUROS(config-if)#service-policy output
POLITICA_IP_TO_CLIENTE_OUT
```

Para comprobar la configuración de los mapas de políticas en la interfaz:

```
PE1MUROS#show policy-map int gi0/1
```

Políticas para el manejo de la congestión en dirección a la red MPLS

La política que permite controlar la congestión en las interfaces que se conectan con los routers LSR, define los parámetros de los PHB preestablecidos en la

Tabla 3.5, como son: las capacidades de ancho de banda garantizadas, las colas y los mecanismos de descarte, entre otros.

a. Definir los mapas de clases

Estas clases asocian los paquetes IP según el subcampo DSCP y las etiquetas MPLS con el campo EXP definido, ya que se encuentran en dirección a los dispositivos de la red MPLS.

El mapa de clases asocia los paquetes IP de la red que vienen marcados con el campo IP *precedence* 6 y 7, o las etiquetas MPLS que tengan marcados 6 y 7 en el campo EXP

```
PE1MUROS(config)#class-map match-any CLASE_ROUTING_MPLS
PE1MUROS(config-cmap)#description CLASE_ENRUTAMIENTO_MPLS
PE1MUROS(config-cmap)#Match ip  precedence  6  7
PE1MUROS(config-cmap)#Match mpls experimental topmost  6 7
```

El mapa de clases asocia las etiquetas MPLS que tengan el valor 5 marcado en el campo EXP

```
PE1MUROS(config)#class-map match-any CLASE_PLATINUM_MPLS
PE1MUROS(config-cmap)#description CLASE_PLATINUM_VOZ_MPLS
PE1MUROS(config-cmap)#match mpls experimental topmost  5
```

El mapa de clase asocia las etiquetas MPLS que tengan el valor 4 marcado en el campo EXP

```
PE1MUROS(config)#class-map match-any CLASE_GOLD_MPLS
PE1MUROS(config-cmap)#descrip CLASE_GOLD_VIDEOCONFERENCIA_MPLS
PE1MUROS(config-cmap)#match mpls experimental topmost  4
```

El mapa de clase asocia las etiquetas MPLS que tengan el valor 3 marcado en el campo EXP

```
PE1MUROS(config)#class-map match-any CLASE_SILVER_MPLS
PE1MUROS(config-cmap)#descri CLASE_SILVER_CORPORATIVOS_VIP_MPLS
PE1MUROS(config-cmap)#match mpls experimental topmost  3
```

El mapa de clase asocia las etiquetas MPLS que tengan el valor 2 marcado en el campo EXP

```
PE1MUROS(config)#class-map match-any CLASE_BRONZE_MPLS
PE1MUROS(config-cmap)#descriptio CLASE_BRONZE_CORPORATIVOS_MPLS
PE1MUROS(config-cmap)#match mpls experimental topmost  2
```

b. Definir los mapas de políticas

Se asocian los paquetes de las clases MPLS y establece los PHB determinados en la Tabla 3.5.

Mapa de política que define los PHB a cada clase de servicio

```
PE1MUROS(config)#policy-map POLITICA_MPLS_TO_MPLS_OUT
```

La clase CLASE_ROUTING_MPLS tiene el 5% de ancho de banda prioritario en la red

```
PE1MUROS(config-pmap)#class CLASE_ROUTING_MPLS
PE1MUROS(config-pmap-c)#priority percent 5
```

La clase CLASE_PLATINUM_MPLS tiene el 10% de ancho de banda prioritario en la red

```
PE1MUROS(config-pmap)#class CLASE_PLATINUM_MPLS
PE1MUROS(config-pmap-c)#priority percent 10
```

La clase CLASE_GOLD_MPLS tiene un ancho de banda garantizado del 15% y una cola limitada en 100 paquetes

```
PE1MUROS(config-pmap)#class CLASE_GOLD_MPLS
PE1MUROS(config-pmap-c)#bandwidth percent 15
PE1MUROS(config-pmap-c)#queue-limit 100  packets
```

La clase CLASE_SILVER_MPLS tiene un ancho de banda garantizado del 35% y una cola limitada en 100 paquetes

```
PE1MUROS(config-pmap)#class CLASE_SILVER_MPLS
PE1MUROS(config-pmap-c)#bandwidth percent 35
PE1MUROS(config-pmap-c)#queue-limit 100  packets
```

La clase CLASE_BRONZE_MPLS tiene un ancho de banda garantizado del 30%, una cola limitada en 100 paquetes y puede aumentar su capacidad hasta un 40% del ancho de banda total del enlace con el mecanismo *traffic shaping*

```
PE1MUROS(config-pmap)#class CLASE_BRONZE_MPLS
```

```
PE1MUROS(config-pmap-c)#bandwidth percent 30
PE1MUROS(config-pmap-c)#queue-limit 100 packets
PE1MUROS(config-pmap-c)#shape average percent 40
```

La clase por defecto no garantiza ningún tratamiento preferencial, utiliza el ancho de banda restante de la red con un umbral máximo del 50%; además dispone del mecanismo de evasión de la congestión WRED para el descarte de los paquetes en base al valor DSCP configurado

```
PE1MUROS(config-pmap)#class class-default
PE1MUROS(config-pmap-c)#queue-limit 100 packets
PE1MUROS(config-pmap-c)#random-detect dscp-based
PE1MUROS(config-pmap-c)#shape average percent 50
```

Para comprobar la configuración de los mapas de políticas:

```
PE1MUROS#show policy-map POLITICA_MPLS_TO_MPLS_OUT
```

c. Definir la política en la interfaz

Se debe configurar la política a la salida de las interfaces de los routers LER que se conectan con los routers LSR de la red MPLS.

```
PE1MUROS(config)#int gi 0/0
PE1MUROS(config-if)#service-policy output
POLITICA_MPLS_TO_MPLS_OUT
```

Para comprobar la configuración de los mapas de políticas en la interfaz:

```
PE1MUROS#show policy-map int gi0/0
```

2. Capa núcleo: routers LSR

Los routers LSR solo tienen interfaces MPLS es por ello que, se deben configurar las políticas de control de congestión a fin de establecer los PHB presentado en la Tabla 3.5.

a. Definir los mapas de clases

El mapa de clases asocia los paquetes IP de la red que vienen marcados con el campo *ip precedence* 6 y 7, o las etiquetas MPLS que tengan marcados 6 y

7 en el campo EXP. Esta clase define los paquetes IP debido a que en cualquier salto, se puede generar información de enrutamiento que viene marcada por defecto con IP *precedence* 6 y 7.

```
PGOSSEAL(config)#class-map match-any CLASE_ROUTING_MPLS
PGOSSEAL(config-cmap)#description CLASE_ENRUTAMIENTO_MPLS
PGOSSEAL(config-cmap)#Match ip  precedence  6  7
PGOSSEAL(config-cmap)#Match mpls experimental topmost  6 7
```

El mapa de clases asocia las etiquetas MPLS que tengan el valor 5 marcado en el campo EXP

```
PGOSSEAL(config)#class-map match-any CLASE_PLATINUM_MPLS
PGOSSEAL(config-cmap)#description CLASE_PLATINUM_VOZ_MPLS
PGOSSEAL(config-cmap)#match mpls experimental topmost  5
```

El mapa de clases asocia las etiquetas MPLS que tengan el valor 4 marcado en el campo EXP

```
PGOSSEAL(config)#class-map match-any CLASE_GOLD_MPLS
PGOSSEAL(config-cmap)#descrip CLASE_GOLD_VIDEOCONFERENCIA_MPLS
PGOSSEAL(config-cmap)#match mpls experimental topmost  4
```

El mapa de clases asocia las etiquetas MPLS que tengan el valor 3 marcado en el campo EXP

```
PE1MUROS(config)#class-map match-any CLASE_SILVER_MPLS
PGOSSEAL(config-cmap)#descri CLASE_SILVER_CORPORATIVOS_VIP_MPLS
PGOSSEAL(config-cmap)#match mpls experimental topmost  3
```

El mapa de clases asocia las etiquetas MPLS que tengan el valor 2 marcado en el campo EXP

```
PGOSSEAL(config)#class-map match-any CLASE_BRONZE_MPLS
PGOSSEAL(config-cmap)#descriptio CLASE_BRONZE_CORPORATIVOS_MPLS
PGOSSEAL(config-cmap)#match mpls experimental topmost  2
```

b. Definir los mapas de políticas

Se asocian los paquetes de las clases MPLS y establece los PHB definidos en la Tabla 3.5.

Mapa de política que define los PHB a cada clase de servicio

```
PGOSSEAL(config)#policy-map POLITICA_MPLS_TO_MPLS_OUT
```

La clase CLASE_ROUTING_MPLS tiene el 5% de ancho de banda prioritario en la red

```
PGOSSEAL(config-pmap)#class CLASE_ROUTING_MPLS
PGOSSEAL(config-pmap-c)#priority percent 5
```

La clase CLASE_PLATINUM_MPLS tiene el 10% de ancho de banda prioritario en la red

```
PGOSSEAL(config-pmap)#class CLASE_PLATINUM_MPLS
PGOSSEAL(config-pmap-c)#priority percent 10
```

La clase CLASE_GOLD_MPLS tiene un ancho de banda garantizado del 15% y una cola limitada de 100 paquetes

```
PGOSSEAL(config-pmap)#class CLASE_GOLD_MPLS
PGOSSEAL(config-pmap-c)#bandwidth percent 15
PGOSSEAL(config-pmap-c)#queue-limit 100  packets
```

La clase CLASE_SILVER_MPLS tiene un ancho de banda garantizado del 35% y una cola limitada de 100 paquetes

```
PGOSSEAL(config-pmap)#class CLASE_SILVER_MPLS
PGOSSEAL(config-pmap-c)#bandwidth percent 35
PGOSSEAL(config-pmap-c)#queue-limit 100  packets
```

La clase CLASE_BRONZE_MPLS tiene un ancho de banda garantizado del 30%, una cola limitada de 100 paquetes y puede aumentar su capacidad hasta un 40% del ancho de banda total del enlace con el mecanismo *traffic shaping*

```
PGOSSEAL(config-pmap)#class CLASE_BRONZE_MPLS
PGOSSEAL(config-pmap-c)#bandwidth percent 30
PGOSSEAL(config-pmap-c)#queue-limit 100 packets
PGOSSEAL(config-pmap-c)#shape average percent 40
```

La clase por defecto no garantiza ningún tratamiento preferencial, utiliza el ancho de banda restante de la red con un umbral máximo del 50%, y además dispone del mecanismo de evasión de la congestión WRED para el descarte de los paquetes en base al valor DSCP configurado

```
PGOSSEAL(config-pmap)#class class-default
PGOSSEAL(config-pmap-c)#queue-limit 100 packets
```

```
PGOSSEAL(config-pmap-c)#random-detect dscp-based
PGOSSEAL(config-pmap-c)#shape average percent 50
```

Para comprobar la configuración de los mapas de políticas:

```
PGOSSEAL#show policy-map POLITICA_MPLS_TO_MPLS_OUT
```

c. Definir la política en la interfaz

Se debe configurar la política a la salida de las interfaces de los routers LSR.

```
PGOSSEAL(config)#int gi 0/0
PGOSSEAL(config-if)#service-policy output
POLITICA_MPLS_TO_MPLS_OUT
```

Para comprobar la configuración de los mapas de políticas en la interfaz:

```
PGOSSEAL#show policy-map int gi0/0
```

3. Capa distribución y acceso[8]

Los equipos que pertenecen a estas capas, son los switches agregadores y los de acceso, que se encargan de enviar y recibir el tráfico de los clientes hacia la red MPLS y viceversa. En vista de que el tráfico ya fue marcado en los routers CE, estos switches deben tener configurado *Multi-Layer Switching* (MLS) y confiar en el marcado de los paquetes.

A continuación se indican los comandos necesarios para que los switches confíen en el marcaje preestablecido:

a. Habilitar QoS en el equipo

```
SW1COLON(config)#mls qos
```

Para verificar las configuraciones de MLS:

```
SW1COLON#show mls qos
```

b. Habilitar Qos en las interfaces

Se debe habilitar QoS en todas las interfaces del switch para que confíen en el valor DSCP marcado en los paquetes IP.

```
SW1COLON(config)#interface range fa0/1 - 48
SW1COLON(config-if)#mls qos trust dscp
SW1COLON(config)#interface range gi0/1 - 4
SW1COLON(config-if)#mls qos trust dscp
```

c. Configurar los parámetros de Qos para el control de la congestión de entrada

Los parámetros de QoS para el control de la congestión son aquellos que define el mecanismo SRR. El número de colas viene definido por el fabricante del dispositivo, es por ello que las configuración mostradas a continuación, son una guía para los restantes dispositivos. En la Tabla 3.7 se presentaron las colas de entrada y salida que soporta cada switch de la marca Cisco.

En la Tabla 4.1, se presentan los parámetros de QoS para el control de la congestión en las colas de entrada para un switch Cisco 3560.

CoS	PHB	COLA	UMBRAL	*BUFFER*	*BANDWIDTH*	UMBRAL	PQ
Routing	CS7, CS6	1	2	40%	30%	70%	30%
Platinum	EF	1	3			100%	-
Gold	AF41	1	1			50%	-
Silver	AF31	2	3	60%	70%	100%	-
Bronze	AF21	2	2			40%	-
Best-Effort	0	2	1			30%	-

Tabla 4.1 Parámetros de QoS para las colas de entrada

Establecer los valores DSCP para cada cola de entrada según los PHB de la Tabla 4.1

```
SW1COLON(config)#mls qos srr-queue input dscp-map queue 1
threshold 3 46
SW1COLON(config)#mls qos srr-queue input dscp-map queue 1
threshold 2 48 56
SW1COLON(config)#mls qos srr-queue input dscp-map queue 1
threshold 1 34
SW1COLON(config)#mls qos srr-queue input dscp-map queue 2
threshold 3 26
```

```
SW1COLON(config)#mls qos srr-queue input dscp-map queue 2
threshold 2 18
SW1COLON(config)#mls qos srr-queue input dscp-map queue 2
threshold 1 0
```

Establecer los porcentajes de los búferes de entrada: 40% para la cola 1 y 60% para la cola 2

```
SW1COLON(config)#mls qos srr-queue input buffers 40 60
```

Establecer los porcentajes de uso de los umbrales según la cola de entrada. El umbral 3 tiene por defecto el porcentaje del 100%, mientras que se deben configurar los restantes porcentajes.

```
SW1COLON(config)#mls qos srr-queue input threshold 1 70 50
SW1COLON(config)#mls qos srr-queue input threshold 2 30 40
```

Después de atender la cola prioritaria, la capacidad de ancho de banda se comparte entre las dos colas restantes, por lo que se configuran estos porcentajes

```
SW1COLON(config)#mls qos srr-queue input bandwidth 30 70
```

Se define a la cola 1 como la cola prioritaria y una capacidad garantizada del 30%

```
SW1COLON(config)#mls qos srr-queue input priority-queue 1
bandwidth 30
```

d. Establecer los parámetros de Qos para el control de la congestión de salida

En la Tabla 4.2, se presentan los parámetros de QoS para el control de la congestión en las colas de salida para un switch Cisco 3560.

CoS	PHB	COLA	UMBRAL	*BUFFER*	*BANDWIDTH*
Routing	CS7, CS6	1	2	30%	100%
Platinum	EF	1	3	35%	45%
Gold	AF41	2	1		
Silver	AF31	3	3	25%	35%
Bronze	AF21	3	2		
Best-Effort	0	4	1	10%	30%

Tabla 4.2 Parámetros de QoS para las colas de salida

Establecer los valores DSCP para cada cola de salida según los PHB de la Tabla 4.2

```
SW1COLON(config)#mls qos srr-queue output dscp-map queue 1
threshold 3 46 48 56
SW1COLON(config)#mls qos srr-queue output dscp-map queue 2
threshold 3 34
SW1COLON(config)#mls qos srr-queue output dscp-map queue 3
threshold 3 26
SW1COLON(config)#mls qos srr-queue output dscp-map queue 3
threshold 2 18
SW1COLON(config)#mls qos srr-queue output dscp-map queue 4
threshold 3 0
```

Establecer los porcentajes de los búferes de salida: 30% para la cola 1, 35% para la cola 2, 25% para la cola 3 y 10% para la cola 4

```
SW1COLON(config)#mls qos queue-set output 1 buffers 30 35 25 10
```

e. Establecer las capacidades de ancho de banda compartidas

Se deben especificar los porcentajes de ancho de banda que cada cola hará uso en las interfaces. Al definir la cola prioritaria, esta será atendida primero hasta quedar vacía, mientras las restantes colas deberán compartir la capacidad del enlace definiendo sus porcentajes, como se indica a continuación:

```
SW1COLON(config)#int range f0/1 – 48
```

Definición de la cola prioritaria

```
SW1COLON(config-if)#priority-queue out
```

Definición de los anchos de banda compartidos entre las colas

```
SW1COLON(config-if)#srr-queue bandwidth share 1 45 35 20
```

f. Verificar las configuraciones

Los comandos que permiten verificar la configuración de QoS en los switches son:

Para verificar que los valores DSCP fueron correctamente configurados en la cola respectiva

```
SW1COLON#sh mls qos maps dscp-input-q
```

Para verificar que las configuraciones de QoS fueron correctamente establecidas en las colas de salida

```
SW1COLON#sh mls qos queue-set 1
```

Para verificar las capacidades de ancho de banda en una interfaz determinada

```
SW1COLON#sh mls qos int gi 0/1 queueing
```

Para verificar que las configuraciones de QoS fueron correctamente establecidas en las colas de entrada

```
SW1COLON#sh mls qos input
```

4.2.6.3. Configuración de Ingeniería de Tráfico[18][10][13]

La Ingeniería de Tráfico (TE) tiene como objetivo la optimización de los recursos de la red y la capacidad para brindar redundancia de enlaces a través de la implementación de túneles MPLS TE. Los requerimientos previos a levantar TE son: OSPF, CEF, LDP y MPLS.

Creación de los túneles TE para balanceo de carga

La Ingeniería de Tráfico brinda balanceo de carga a través de la creación de túneles TE, como se indica a continuación:

a. Habilitar Ingeniería de Tráfico

Se debe habilitar tanto en la configuración global como en las interfaces de los equipos de la nube MPLS.

A nivel global:

```
PE1MUROS(config)# mpls traffic-eng tunnels
```

A nivel de interfaz:

```
PE1MUROS(config)# interface gi0/0
PE1MUROS(config-if)#mpls traffic-eng tunnels
```

b. Habilitar el protocolo de señalización RSVP

En las mismas interfaces donde se habilitó TE, se deben establecer los parámetros de ancho de banda para ser reservados mediante la Ingeniería de Tráfico.

```
PE1MUROS(config)# interface gi0/0
PE1MUROS(config-if)#ip rsvp bandwidth 1000 1000
```

El parámetro después del comando bandwidth indica el ancho de banda reservado en kbps, mientras que el segundo parámetro refleja el máximo ancho de banda reservado por flujo en kbps.

c. Crear las interfaces túneles TE

Los túneles TE se establecen entre los routers LER.

```
PE1MUROS(config)# interface tunnel1
```

Dirección IP origen sobre la cual se enviará el tráfico. Se recomienda utilizar una interfaz *loopback*:

```
PE1MUROS(config-if)#ip unnumbered loopback 0
```

Asignación del modo de operación del túnel: MPLS TE

```
PE1MUROS(config-if)#tunnel mode mpls traffic-eng
```

El destino del túnel TE se establece con la dirección IP del PE remoto.

```
PE1MUROS(config-if)#tunnel destination 5.5.5.5
```

Se anuncia el túnel en el protocolo IGP (OSPF) y se habilita el envío de tráfico

```
PE1MUROS(config-if)#tunnel mpls traffic-eng autoroute announce
```

Se especifica la cantidad de ancho de banda reservado para el túnel TE en el LSP

```
PE1MUROS(config-if)#tunnel mpls traffic-eng bandwidth 1204
```

Se establece la prioridad del túnel TE en un LSP. Los valores permitidos van de 0 a 7, donde 0 es la prioridad más alta y 7 la menor. El primer campo indica el valor de prioridad del túnel, y el segundo, aunque es opcional, indica el valor de prioridad de otro LSP precedente y de menor prioridad.

```
PE1MUROS(config-if)#tunnel mpls traffic-eng priority 7 7
```

El camino que seguirá el túnel puede ser: dinámico o explícito. En la selección explícita, se crea el camino indicando cada salto hasta el destino:

```
PE1MUROS(config)#interface tunnel1
```

```
PE1MUROS(config-if)#tunnel mpls traffic-eng path-option 1
explicit name TUNEL_UIO_TO_PE1GOSSEAL
```

El LSP se construye especificando los siguientes saltos por el administrador de red.

```
PE1MUROS(config)#ip explicit-path name TUNEL_UIO_TO_PE1GOSSEAL
enable
```

El comando “next-address” indica salto a salto, las direcciones IP a través de las cuales se alcanza el destino.

```
PE1MUROS(config-ip-expl-path)#next-address 2.2.2.2
PE1MUROS(config-ip-expl-path)#next-address 4.4.4.4
PE1MUROS(config-ip-expl-path)#next-address 5.5.5.5
```

Si la selección es dinámica, se construye el trayecto en base a los protocolos IGP y CSPF configurados de la siguiente manera:

```
PE1MUROS(config)#interface tunnel2
PE1MUROS(config-if)#tunnel mpls traffic-eng path-option 1
dynamic
```

El valor 1 indica la importancia del túnel frente a otras configuraciones.

d. Habilitar TE en el protocolo IGP: OSPF

Para que el protocolo IGP pueda soportar Ingeniería de Tráfico, se agregan los siguientes comandos a la configuración anterior de OSPF:

```
PE1MUROS(config)#router ospf 27947
```

Se asocia *loopback*0 como identificador del router en la sesión TE:

```
PE1MUROS(config-if)#mpls traffic-eng router-id loopback 0
```

Habilitar TE en el área 0

```
PE1MUROS(config-if)#mpls traffic-eng area 0
```

e. Verificar las configuraciones

```
PE1MUROS#show ip rsvp interfaz gi1/0
PE1MUROS#show mpls traffic-engineering tunnels tunnel 1
PE1MUROS#show mpls traffic-engineering tunnels brief
PE1MUROS#show ip interface tunnel1
```

De la misma manera que los túneles 1 y 2, los túneles 3 y 4 deben configurarse pero en sentido contrario.

Redundancia de enlaces con túneles TE

Con la Ingeniería de Tráfico, se pueden proteger enlaces de la red mediante *Fast Re-Route*, que permite levantar túneles TE de respaldo frente a los problemas en las interfaces protegidas.

a. Habilitar *Fast Re-Route*

Fast Re-Route permite proteger los enlaces de la red, reenrutando el tráfico del túnel principal por un túnel de respaldo preconfigurado. Se configurará el túnel 10 como respaldo del túnel 1.

```
PEGOSSEAL(config)# interface tunnel10
PEGOSSEAL(config-if)#ip unnumbered Loopback 0
PEGOSSEAL(config-if)# tunnel destination 5.5.5.5
PEGOSSEAL(config-if)#tunnel mode mpls traffic-eng
PEGOSSEAL(config-if)#tunnel mpls traffic-eng autoroute
announce
PEGOSSEAL(config-if)#tunnel mpls traffic-eng bandwidth 100
PEGOSSEAL(config-if)#tunnel mpls traffic-eng priority 2 2
PEGOSSEAL(config-if)# tunnel mpls traffic-eng path-option 1
explicit name BACKUP_TUNEL_UIO_TO_PE1GOSSEAL
```

b. Definir la ruta explícita

```
PEGOSSEAL(config)# ip explicit-path name
BACKUP_TUNEL_UIO_TO_PE1GOSSEAL
PEGOSSEAL(config-ip-expl-path)#next-address 3.3.3.3
PEGOSSEAL(config-ip-expl-path)#next-address 4.4.4.4
```

c. Configurar el túnel principal

En las configuraciones del túnel principal se debe agregar una sentencia de respaldo.

```
PE1MUROS(config)#interface tunnel 1
PE1MUROS(config-if)#tunnel mpls traffic-eng fast-reroute
```

d. Designar la Interfaz protegida

Se debe establecer la interfaz del router que activará el túnel de respaldo cuando se encuentre en estado *down.*

```
PE1GOSSEAL(config)#interface gi0/1
PE1GOSSEAL(config-if)#mpls traffic-eng backup-path Tunnel 10
```

e. Verificar la configuración

```
PE1GOSSEAL #show mpls traffic-engineering fast-reroute database
PE1GOSSEAL #show mpls traffic-engineering fast-reroute database
details
```

Para comprobar se ejecuta un comando *ping* continuo y se desconecta la interfaz protegida para ver que el re-enrutamiento por el túnel secundario es inmediato y la pérdida de paquetes es mínima.

```
PE1MUROS# ping 5.5.5.5 repeat 3000
```

De la misma manera que los túneles 1 y 10, los túneles 3 y 30 deben configurarse pero en sentido contrario.

4.2.7. CONFIGURACIÓN DE SEGURIDAD EN IPv6

La configuración se basará en tres de las Mejores Prácticas de Seguridad que recomienda Cisco Systems, Inc.; como son: las VLAN, las Listas de Control de Acceso en IPv6 y la gestión mediante acceso remoto seguro.

4.2.7.1. VLAN

En la sección 4.2.2 se presentaron los comandos para configurar VLAN en un switch teniendo una dirección IP de gestión en IPv4. Para configurar una dirección IPv6 de gestión se deben incluir algunos comandos adicionales como se indican a continuación:

a. Habilitar la plantilla de doble pila

```
SW1COLON(config)#sdm prefer dual-ipv4-and-ipv6 default
SW1COLON#reload
```

b. Habilitar el soporte para IPv6 en el switch

```
SW1COLON(config)#ipv6 unicast-routing
```

c. Asignar la IP de administración del switch

```
SW1COLON(config)#interface vlan 129
SW1COLON(config-if)#ipv6 enable
SW1COLON(config-if)#ipv6 add 2001:29:2:41::2/64
SW1COLON(config-if)#no shutdown
```

d. Configurar el default gateway

```
SW1COLON(config)#ipv6 route ::0/0 2001:29:2:41::1
```

e. Verificar la configuración

```
SW1COLON#show vlan
SW1COLON#show interface truck
```

f. Configurar las subinterfaces en el router

Se creará la interfaz gi 0/1.2 como *dual stack* y que maneje la VLAN 129 como nativa.

```
PE1MUROS(config)#interface gi0/1
PE1MUROS(config-if)#description SUBINTERFACE TO VRF_CLIENTE
PE1MUROS(config-if)#no shutdown
PE1MUROS(config)#int gi0/1.11
PE1MUROS(config-if)#encapsulation dot1q 11
PE1MUROS(config-if)#ip vrf forwarding CLIENTE
PE1MUROS(config-if)#ip address 11.11.11.1 255.255.255.0
PE1MUROS(config)#interface gi0/1.22
PE1MUROS(config-if)#encapsulation dot1q 22
PE1MUROS(config-if)#vrf forwarding INTERNET
PE1MUROS(config-if)#ipv6 address 2001:22:22:22::1/64
PE1MUROS(config-if)#ip add 22.22.22.1 255.255.255.0
PE1MUROS(config-if)#interface GigabitEthernet0/1.129
PE1MUROS(config-if)#encapsulation dot1Q 129 native
PE1MUROS(config-if)#ip address 10.2.41.1 255.255.255.0
PE1MUROS(config-if)#ipv6 add 2001:29:2:41::1/64
PE1MUROS(config-if)#ipv6 enable
```

4.2.7.2. Listas de Control de Acceso (ACL) en IPv6

Las ACL permiten brindar seguridad a la redes al permitir y/o denegar el tráfico de entrada o salida. Las configuraciones en IPv6 son similares a IPv4, aunque solo se pueden establecer ACL nombradas extendidas.

A continuación se muestran las configuraciones de las ACL en IPv4 e IPv6:

a. Definir las ACL en IPv4

Se permite el tráfico HTTP, HTTPS, FTP Y TFTP para determinados hosts y redes en IPv4.

```
PE1MUROS(config)#ip access-list extended ACLGESTION_MPLS
PE1MUROS(config-ext-nacl)#permit tcp 10.2.41.0 0.0.0.255 any eq
www
PE1MUROS(config-ext-nacl)#deny tcp any any eq www
PE1MUROS(config-ext-nacl)#permit tcp 10.2.41.0 0.0.0.255 any eq
443
PE1MUROS(config-ext-nacl)#deny tcp any any eq 443
PE1MUROS(config-ext-nacl)#permit tcp any host 10.2.41.11 eq ftp
PE1MUROS(config-ext-nacl)#deny tcp any any eq ftp
PE1MUROS(config-ext-nacl)#permit  tcp  any  host  10.2.41.11  eq
ftp-data
PE1MUROS(config-ext-nacl)#deny tcp any any eq ftp-data
PE1MUROS(config-ext-nacl)#permit  udp  any  host  10.2.41.11  eq
tftp
PE1MUROS(config-ext-nacl)#deny udp any any eq tftp
PE1MUROS(config-ext-nacl)#permit ip any any
PE1MUROS(config-ext-nacl)#deny ip any any
```

b. Definir las ACL en IPv6

Se permite el tráfico HTTP, HTTPS, FTP y TFTP para determinados hosts y redes en IPv6.

```
PE1MUROS(config)#ipv6 access-list ACLV6GESTION_MPLS
PE1MUROS(config-ipv6-acl)#permit tcp 2001:29:2:41::0/64 any eq
www
PE1MUROS(config-ipv6-acl)#deny tcp any any eq www
```

```
PE1MUROS(config-ipv6-acl)#permit tcp 2001:29:2:41::0/64 any eq
443
PE1MUROS(config-ipv6-acl)#deny tcp any any eq 443
PE1MUROS(config-ipv6-acl)#permit tcp any host 2001:29:2:41::11
eq ftp
PE1MUROS(config-ipv6-acl)#deny tcp any any eq ftp
PE1MUROS(config-ipv6-acl)#permit tcp any host 2001:29:2:41::11
eq ftp-data
PE1MUROS(config-ipv6-acl)#deny tcp any any eq ftp-data
PE1MUROS(config-ipv6-acl)#permit udp any host 2001:29:2:41::11
eq tftp
PE1MUROS(config-ipv6-acl)#deny udp any any eq tftp
PE1MUROS(config-ipv6-acl)#permit ipv6 any any
PE1MUROS(config-ipv6-acl)#deny ipv6 any any
```

c. Asignar las ACL a la interfaz

La asignación de las ACL puede ser de entrada (*in*) o salida (*out*) tanto para IPv4 como para IPv6, aunque se diferencian por los comandos utilizados; siendo “Access-group” para IPv4 y “Traffic-filter” para IPv6.

```
PE1MUROS(config)#int  gi0/0
PE1MUROS(config-if)#ip access-group ACLGESTION_MPLS in
PE1MUROS(config-if)#ipv6 traffic-filter ACLV6GESTION_MPLS in
PE1MUROS(config)#int  gi0/1.129
PE1MUROS(config-if)#ip access-group ACLGESTION_MPLS in
PE1MUROS(config-if)#ipv6 traffic-filter ACLV6GESTION_MPLS in
```

d. Verificar las configuraciones

```
PE1MUROS#show access-list
PE1MUROS#show ipv4 access-list
PE1MUROS#show ipv6 access-list
```

4.2.7.3. Gestión de acceso remoto seguro

La gestión de acceso remoto seguro se establece mediante el protocolo SSH (puerto 22). La siguiente configuración debe estar especificada en todos los dispositivos de la red de Telconet S.A.: routers y switches.

a. Definir el dominio de Telconet S.A.

```
PE1MUROS(config)#ip domain-name telconet.ec
```

b. Habilitar el cifrado RSA

```
PE1MUROS(config)#crypto key generate rsa general-keys modulus
1024
```

c. Especificar la versión del protocolo SSH

```
PE1MUROS(config)#ip ssh version 2
```

d. Especificar el tiempo de la sesión SSH abierta sin actividad (en segundos)

```
PE1MUROS(config)#ip ssh time-out 30
```

e. Especificar el Número máximo de reintentos de autenticación

```
PE1MUROS(config)#ip ssh authentication-retries 1
```

f. Definir las ACL en IPv4

Las redes que se deben especificar en la ACL son aquellas que se van a permitir o denegar en las sesiones SSH.

```
PE1MUROS(config)#access-list 1 permit 192.168.1.0 0.0.0.15
PE1MUROS(config)#access-list 1 permit 192.168.1.16 0.0.0.15
PE1MUROS(config)#access-list 1 permit 10.2.41.11 0.0.0.0
PE1MUROS(config)#access-list 1 permit 10.2.52.11 0.0.0.0
PE1MUROS(config)#access-list 1 permit 1.1.1.1 0.0.0.0
PE1MUROS(config)#access-list 1 permit 2.2.2.2 0.0.0.0
PE1MUROS(config)#access-list 1 permit 3.3.3.3 0.0.0.0
PE1MUROS(config)#access-list 1 permit 4.4.4.4 0.0.0.0
PE1MUROS(config)#access-list 1 permit 5.5.5.5 0.0.0.0
PE1MUROS(config)#access-list 1 deny any
```

g. Definir las ACL en IPv6

```
PE1MUROS(config)#ipv6 access-list ACLV6GESTION_SSH
PE1MUROS(config-ipv6-acl)#permit ipv6 2001:29:2:41::0/64 any
PE1MUROS(config-ipv6-acl)#permit ipv6 2001:29:2:52::0/64 any
PE1MUROS(config-ipv6-acl)#deny ipv6 any any
```

h. Asociar las líneas VTY con SSH y las ACL

A los routers de la nube MPLS solo se podrá acceder mediante SSH como medida de seguridad. En los switches de las capas distribución y acceso, se accederá mediante SSH y/o *telnet*; mientras en los routers CE, las ACL serán diferentes ya que dependerán del cliente.

```
PE1MUROS(config)#line vty 5 15
```

Asociar las ACL a a las líneas vty como entrada

```
PE1MUROS(config-if)#access-class 1 in
PE1MUROS(config-if)#ipv6 access-class ACLV6GESTION_SSH in
```

Configurar la gestión remota en SSH y/o *Telnet*

```
PE1MUROS(config-if)# transport input ssh
PE1MUROS(config-if)# transport output telnet ssh
```

i. Verificar las configuraciones

```
PE1GOSSEAL#ssh -l test -v 2 10.2.41.1
PE1GOSSEAL#ssh -l test -v 2 2001:29:2:41::1
PE1GOSSEAL#ssh -l test -vrf CLIENTE -v 2 11.11.11.1
PE1GOSSEAL#telnet 10.2.41.1
PE1GOSSEAL#telnet 2001:29:2:41::1
PE1GOSSEAL#telnet 11.11.11.1 /vrf CLIENTE
PE1GOSSEAL#telnet 2001:22:22:22::1 /vrf INTERNET
```

4.3. PROTOTIPO DE LA RED DISEÑADA

La implementación del prototipo de la red MPLS diseñada tiene por objetivo probar las configuraciones presentadas en la sección 4.2 y obtener resultados que demuestren el soporte a IPv6 de una red MPLS/IPv4 empleando las Mejores Prácticas de Seguridad.

El prototipo estará conformado por 9 dispositivos: 2 routers LER que hacen las funciones de PE1MUROS y PE1GOSSEAL, 3 routers LSR como PGOSSEAL, PDATACENTER y PGYE, 2 switches de acceso como SW1COLON y SW1PLAZATOROS, y 2 routers CE como CE1COLON_CLIENTE y CE1PLAZATOROS_CLIENTE.

Se han considerado tres routers LSR en el prototipo a fin de tener enlaces alternos que permitan comprobar las funcionalidades de la Ingeniería de Tráfico. El PGYE simula la red de la matriz Guayaquil, para ofrecer un camino redundante al tráfico de la red de Quito.

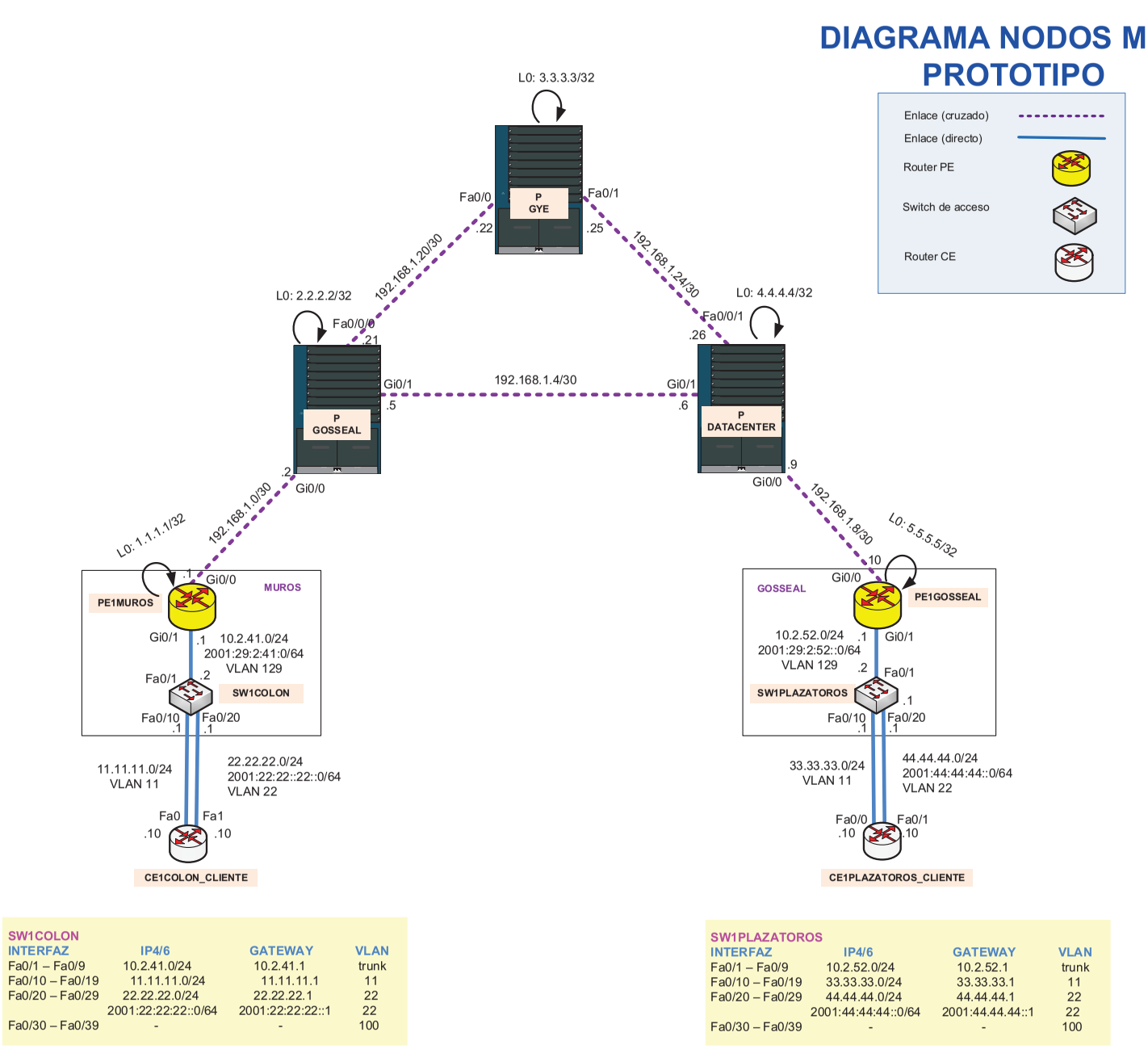
La capa distribución no estará representada por ningún dispositivo en el presente prototipo, ya que sus configuraciones serán prácticamente las mismas que los switches de la capa acceso; en todo caso, se implementarán los dispositivos: SW1COLON y SW1PLAZATOROS que simularán las funcionalidades de la red en capa 2, especialmente en lo referente a las configuraciones de Calidad de Servicio.

Se configurarán 4 VLAN: la VLAN 11 que simulará un cliente con servicios en IPv4, la VLAN 22 que será como un cliente con servicios en IPv4 e IPv6, la VLAN 129 como nativa y administrativa, y finalmente, la VLAN 100 que hará referencia a un cliente con servicios de transporte de capa 2 (VPWS).

En el ANEXO F se presentan las características técnicas de hardware y software de los equipos utilizados en el prototipo; mientras los comandos de configuración de cada dispositivo, se encuentran detallados en el ANEXO G.

En la Figura 4.1 se presenta la topología física del prototipo de la red MPLS con soporte para IPv6 de Telconet S.A.-Quito, detallando: la información del tipo y número de las interfaces, las conexiones, el direccionamiento IP utilizado, la definición de las VLAN y el rango de interfaces en los switches, entre otras características.

En la Tabla 4.3 se muestra el direccionamiento de cada dispositivo de la red del prototipo, detallando: los tipos y número de interfaces, las direcciones IP, el *gateway* y las VLAN utilizadas en cada dispositivo de la red del prototipo.



SW1COLON

INTERFAZ	IP4/6	GATEWAY	VLAN
Fa0/1 – Fa0/9	10.2.41.0/24	10.2.41.1	trunk
Fa0/10 – Fa0/19	11.11.11.0/24	11.11.11.1	11
Fa0/20 – Fa0/29	22.22.22.0/24	22.22.22.1	22
	2001:22:22:22::0/64	2001:22:22:22::1	22
Fa0/30 – Fa0/39	-	-	100

SW1PLAZATOROS

INTERFAZ	IP4/6	GATEWAY	VLAN
Fa0/1 – Fa0/9	10.2.52.0/24	10.2.52.1	trunk
Fa0/10 – Fa0/19	33.33.33.0/24	33.33.33.1	11
Fa0/20 – Fa0/29	44.44.44.0/24	44.44.44.1	22
	2001:44:44:44::0/64	2001:44.44.44::1	22
Fa0/30 – Fa0/39	-	-	100

Figura 4.1 Prototipo de la red MPLS con soporte para IPv6 de Telconet S.A.-UIO

DIRECCIONAMIENTO DE LA RED				
DISPOSITIVO	**INTERFAZ**	**DIRECCIÓN IP**	***GATEWAY***	**VLAN**
PGOSSEAL	G0/0	192.168.1.2/30	-	-
	G0/1	192.168.1.5/30	-	-
	Fa0/0/0	192.168.1.21/30	-	129
	Loopback 0	2.2.2.2/32	-	-
PDATACENTER	G0/0	192.168.1.9/30	-	-
	G0/1	192.168.1.6/30	-	-
	Fa0/0/1	192.168.1.26/30	-	129
	Loopback 0	4.4.4.4/32	-	-
PGYE	Fa0/0	192.168.1.22/30	-	-
	Fa0/1	192.168.1.25/30	-	-
	Loopback 0	3.3.3.3/32	-	-
PE1MUROS	G0/0	192.168.1.1/30	-	-
	G0/1.11	11.11.11.1/24	-	11
	G0/1.22	22.22.22.1/24	-	22
		2001:22:22:22::1/64		
	G0/1.129	10.2.41.1/24	-	129
		2001:29:2:41::1/64		
	Loopback 0	1.1.1.1/32	-	-
PE1GOSSEAL	G0/0	192.168.1.10/30	-	-
	G0/1.11	33.33.33.1/24	-	11
	G0/1.22	44.44.44.1/24	-	22
		2001:44.44.44::1/64		
	G0/1.129	10.2.52.1/24	-	129
		2001:29:2:52::1/64		
	Loopback 0	5.5.5.5/32	-	-
SW1COLON	Gi0/1-G0/4	-	-	*trunk*
	Fa0/0-Fa0/9	-	-	*trunk*
	Fa0/9-Fa0/19	-	-	11
	Fa0/20-Fa0/29	-	-	22
	Fa0/30-Fa0/39	-	-	100
	VLAN 129	10.2.41.2/24	10.2.41.1	*native*
		2001:29:2:41::2/64	2001:29:2:41::1/64	
SW1PLAZATOROS	Gi0/1-G0/4	-	-	*trunk*
	Fa0/0-Fa0/9	-	-	*trunk*
	Fa0/9-Fa0/19	-	-	11
	Fa0/20-Fa0/29	-	-	22
	Fa0/30-Fa0/39	-	-	100
	VLAN 129	10.2.52.2/24	10.2.52.1	*native*
		2001:29:2:52::2/64	2001:29:2:52::1/64	
CE1COLON_ CLIENTE	Fa0	11.11.11.10/24	11.11.11.1	-
	Fa1	22.22.22.10/24	10.2.43.1	-

		2001:22:22:22::10/64	2001:22:22:22::1	
CE1PLAZATOROS_ CLIENTE	Fa0/0	33.33.33.10/24	33.33.33.1	-
	Fa0/1	44.44.44.10/24	44.44.44.1	-
		2001:44:44:44::10/64	2001:44:44:44::1	

Tabla 4.3 Direccionamiento del prototipo

4.3.1. CONFIGURACIÓN BÁSICA DE LOS DISPOSITIVOS DE RED

En la Figura 4.2 se indica el acceso al PE1MUROS, a través de la línea de consola con autenticación usuario y contraseña, una vez configurados los comandos de la sección 4.2. Además, se muestra el mensaje del día de acceso restringido.

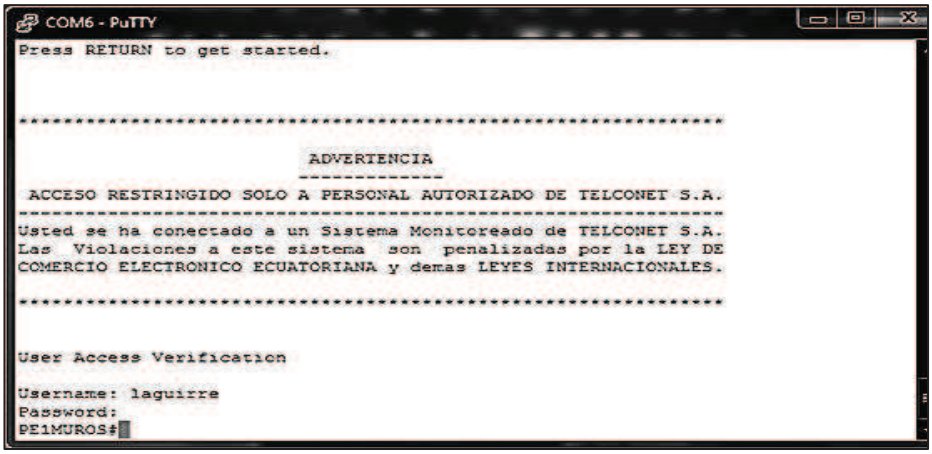


Figura 4.2 Acceso al dispositivo mediante nombre de usuario y contraseña

El comando “show ip interface brief” mostrado en la Figura 4.3 permite desplegar en forma resumida, el estado de las interfaces a fin de comprobar la configuración de las mismas.

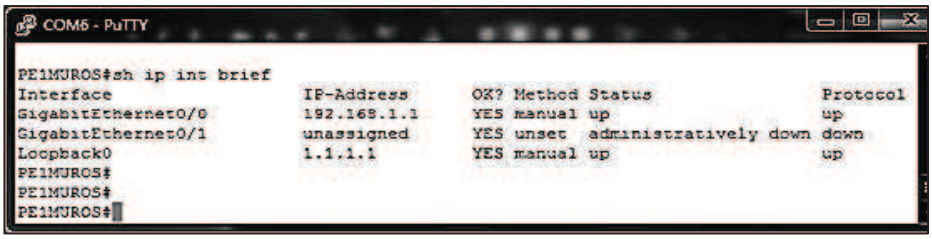


Figura 4.3 Verificación resumida del estado de las interfaces

Para comprobar que la configuración de las interfaces es correcta, se tiene el comando “show ip route” que indica el estado actual de la tabla de enrutamiento del dispositivo, como se indica en la Figura 4.4 para el router PE1MUROS.

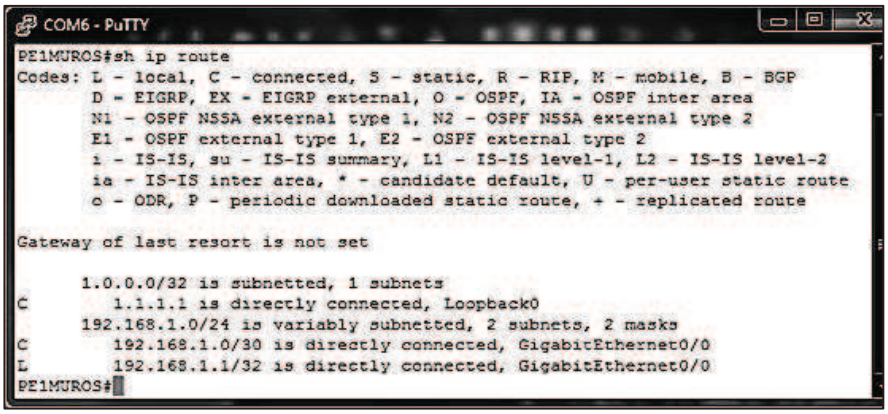


Figura 4.4 Verificación de la tabla de enrutamiento

4.3.2. CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO OSPF[7]

En la Figura 4.5 se indica cómo la red converge al recibir los estados de los enlaces OSPF de los dispositivos configurados en el área 0. La tabla de enrutamiento del PE1MUROS ahora, no solo indica en el comando “show ip route” las redes directamente conectadas sino también, las redes aprendidas por OSPF.

Figura 4.5 Verificación de la tabla de enrutamiento con OSPF

En la Figura 4.6 se muestran los vecinos establecidos con el PE1MUROS, a través de las sesiones OSPF levantadas.

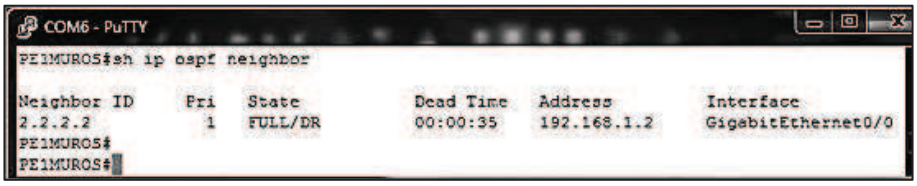


Figura 4.6 Verificación de los vecinos OSPF establecidos

4.3.3. CONFIGURACIÓN DE LAS VLAN EN LOS SWITCHES

En la Figura 4.7 se muestra la asignación de las interfaces a las VLAN configuradas.

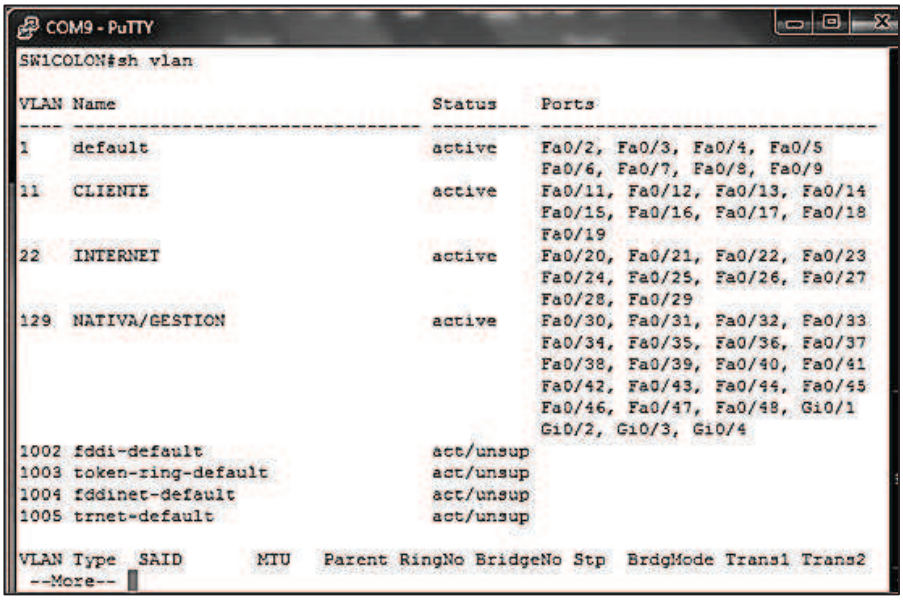


Figura 4.7 Verificación de las interfaces asociadas a cada VLAN

La configuración de las interfaces troncales se puede verificar con el comando “show interface trunk” como se muestra en la Figura 4.8, donde la interfaz Fa0/1 es la única interfaz habilitada como troncal y permite solo las VLAN: 11, 22 y 129. La VLAN 129 es la VLAN configurada como nativa.

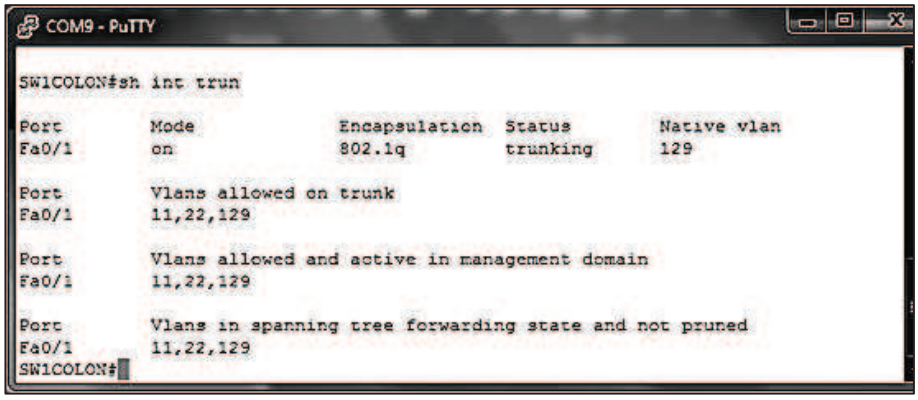


Figura 4.8 Verificación de las interfaces troncales

4.3.4. CONFIGURACIÓN DE LA TECNOLOGÍA MPLS

Para comprobar que la tecnología MPLS está trabajando correctamente, se pueden verificar los siguientes comandos:

PE1MUROS#show mpls forwarding-table
PE1MUROS#show mpls ldp bindings
PE1MUROS#show mpls ldp parameters
PE1MUROS#show mpls ldp neighbor

El Figura 4.9 se indica la tabla LFIB de MPLS, donde se especifican las etiquetas, las direcciones IP y las interfaces del siguiente salto.

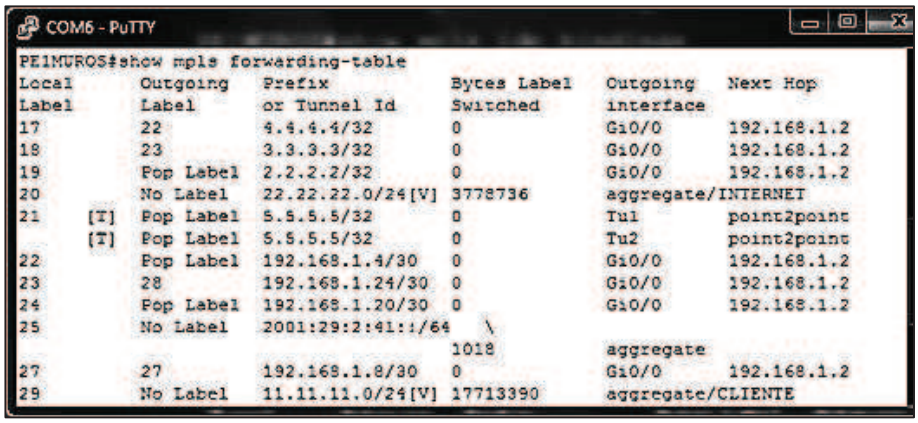


Figura 4.9 Verificación de la tabla LFIB

En la Figura 4.10 se muestran los parámetros del protocolo LDP, como los intervalos de tiempo y la versión.

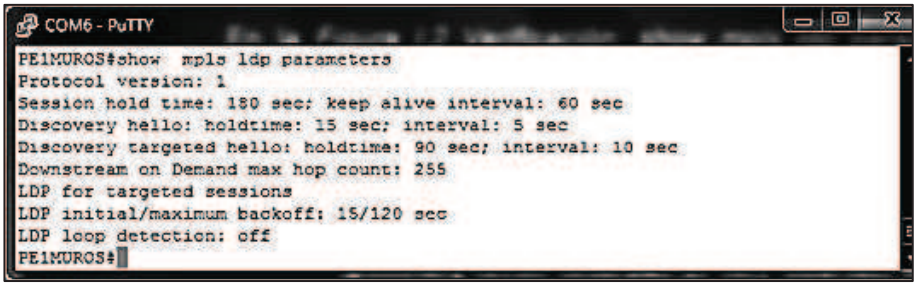


Figura 4.10 Verificación de los parámetros LDP

En la Figura 4.11 se indica la tabla FIB, donde se detalla toda la distribución de etiquetas.

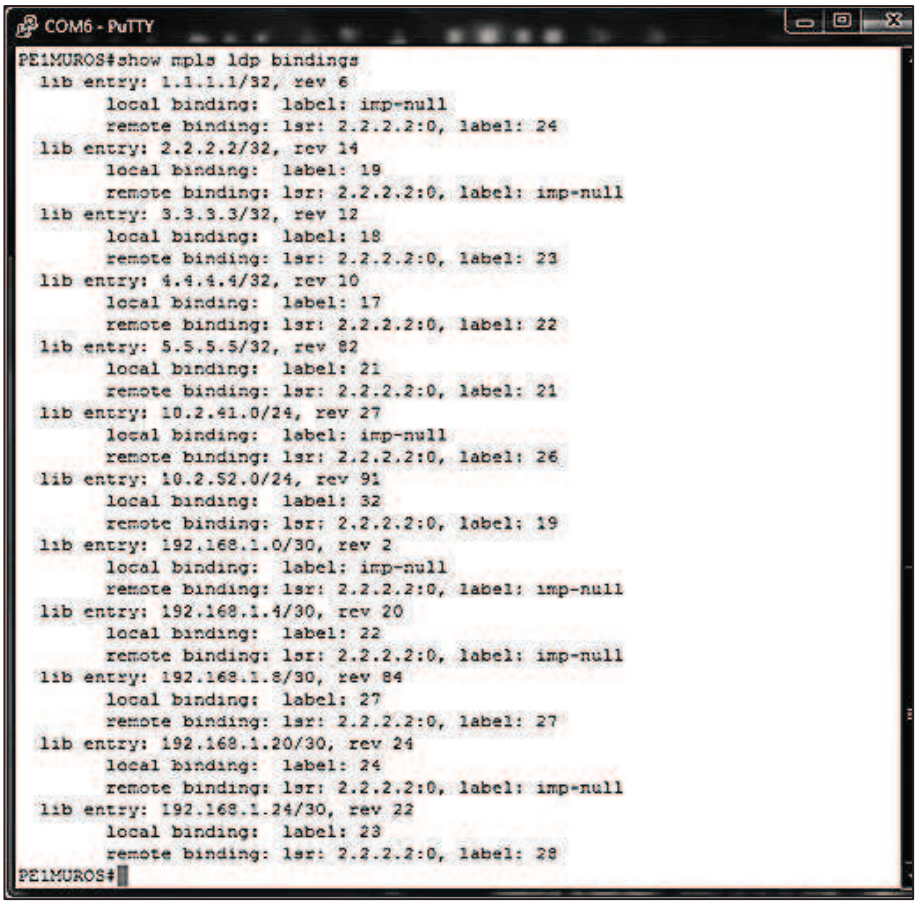


Figura 4.11 Verificación de la tabla FIB

En la Figura 4.12 se detallan los vecinos establecidos en las sesiones LDP.

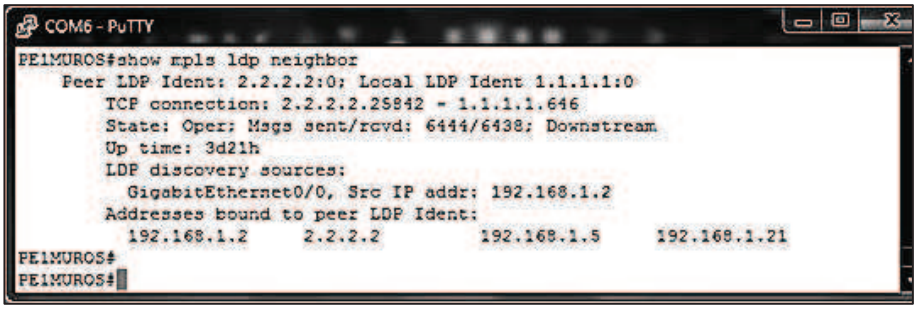


Figura 4.12 Verificación de los vecinos LDP

4.3.5. CONFIGURACIÓN DE MP-BGP

Para la verificación de las sesiones BGP establecidas se tiene el comando "show ip bgp all summary", como se indica en la Figura 4.13.

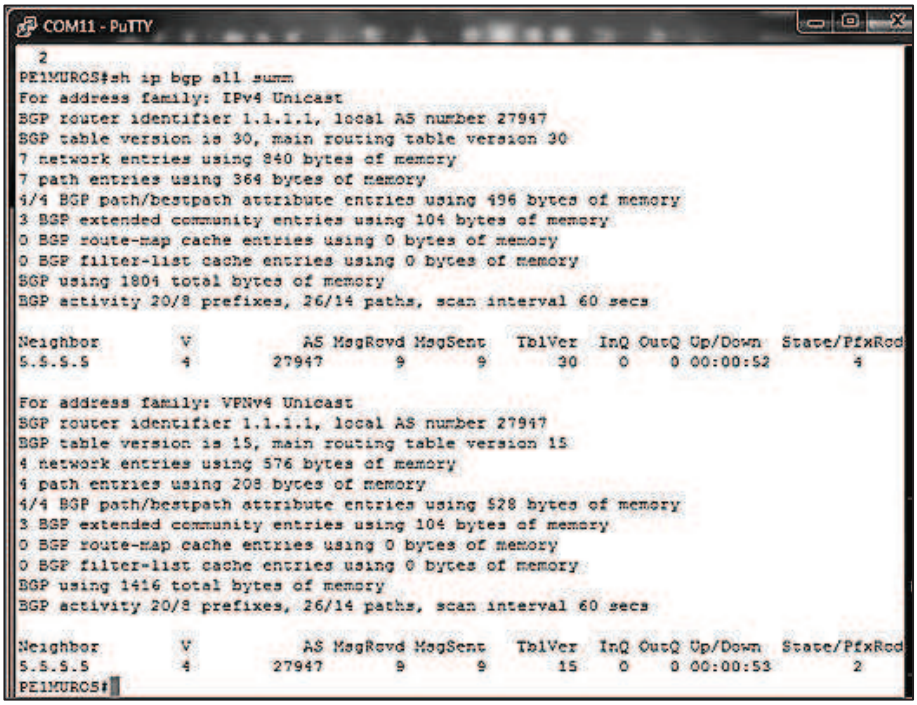


Figura 4.13 Verificación de las sesiones BGP establecidas

Para verificar que el protocolo BGP se convierte en MP-BGP, se tiene el comando "show ip bgp vpnv4 all summary", que indica las sesiones MP-BGP establecidas, como se indica en la Figura 4.14.

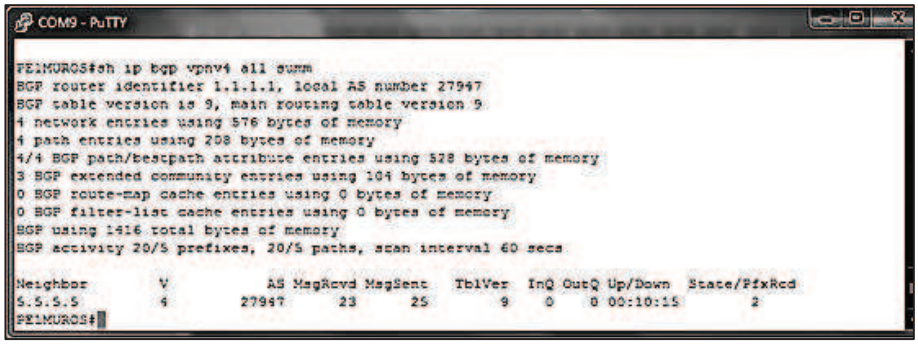


Figura 4.14 Verificación de las sesiones MP-BGP establecidas

4.3.6. CONFIGURACIONES DE IPv6 EN ROUTERS PE (6PE/6VPE)

4.3.6.1. Configuración de 6PE[16]

Para verificar que las sesiones se establecieron en el PE remoto, se deben aprender las direcciones IPv6 del mismo en la tabla de enrutamiento de IPv6, como se indica en la Figura 4.15.

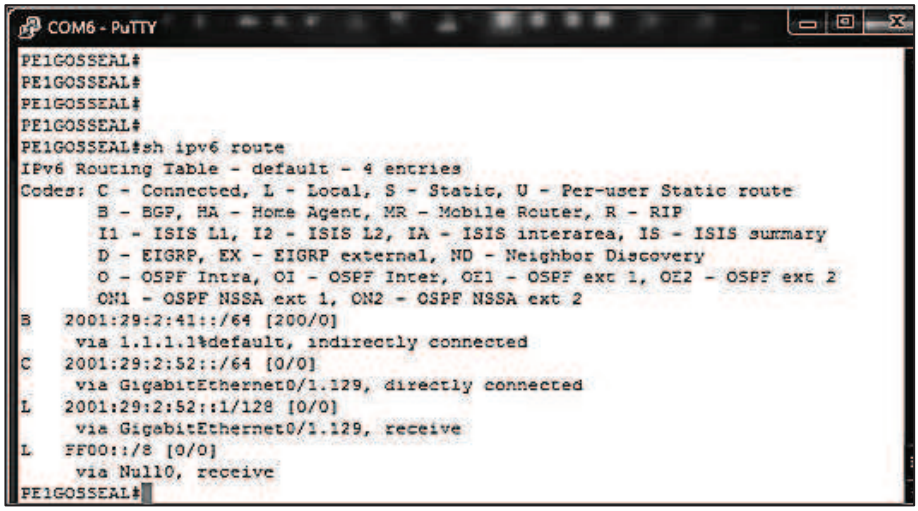


Figura 4.15 Verificación de la tabla de enrutamiento de IPv6

El resultado esperado es poder alcanzar al PE remoto a través de su dirección en IPv6, logrando comprobar que la sesión IPv6 está activa. Se tiene el comando “ping” con el cual se puede definir el estado de la conexión con la interfaz remota, como se indica en la Figura 4.16.

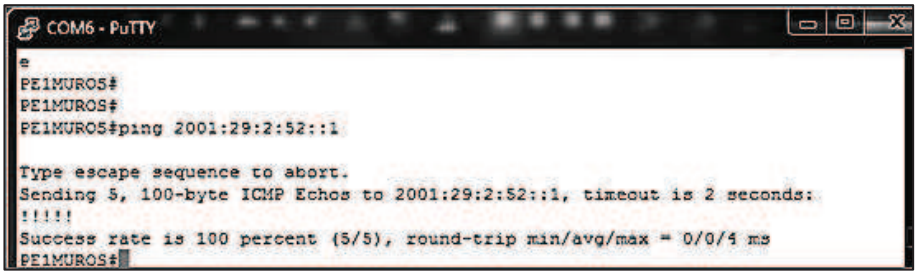


Figura 4.16 Verificación del estado de la conexión remota con PE1GOSSEAL

De la misma manera, se establece un comando "ping" con el PE1MUROS en el Figura 4.17.

Figura 4.17 Verificación del estado de la conexión remota con PE1MUROS

4.3.6.2. Configuración de 6VPE[16][19][20]

Para verificar que la sesión está activada hay que revisar que las redes estén publicadas en la tabla de enrutamiento de la VRF INTERNET, como se indica en la Figura 4.18.

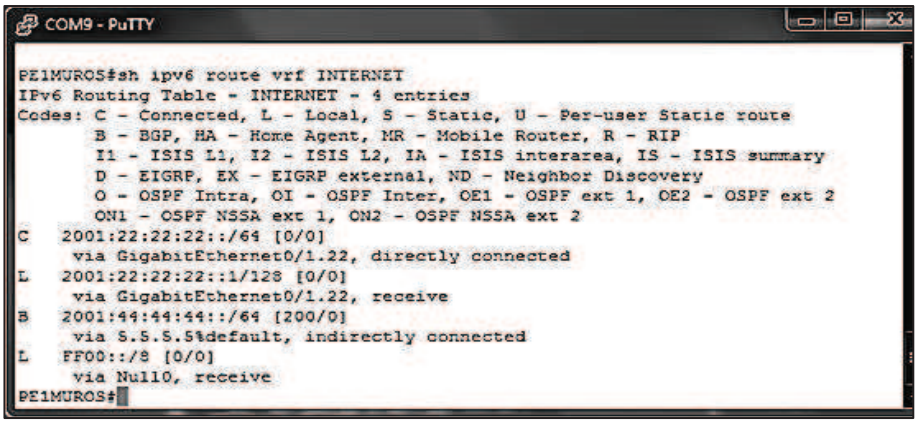


Figura 4.18 Verificación de la tabla de enrutamiento de la VRF INTERNET

Para comprobar que la sesión MP-BGP de la VRF INTERNET está activa, se tiene el comando “show bgp vpnv6 unicast vrf INTERNET”, como se muestra en la Figura 4.19.

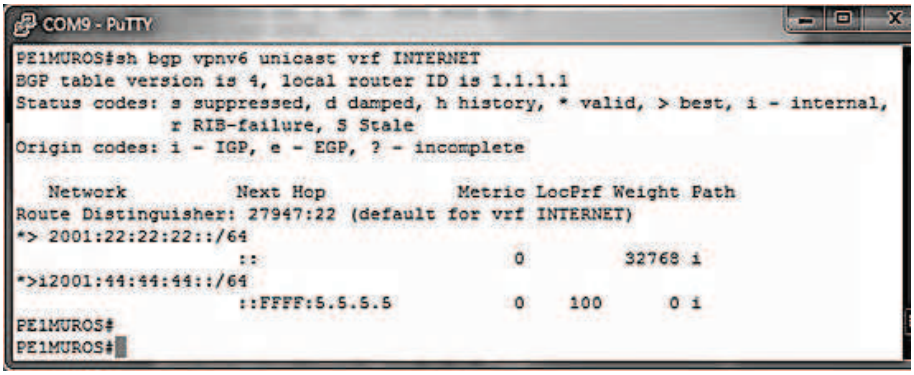


Figura 4.19 Verificación de la sesión MP-BGP IPv6 activada

El resultado esperado es alcanzar mediante el comando “ping” exitoso, la red de la VRF remota en IPv6, como se indica en Figura 4.20. El comando “ping” debe ir acompañado del nombre de la VRF y de la dirección IPv6. La conectividad es exitosa desde el PE1MUROS hacia las interfaces IPv6 de los LER y CE remotos.

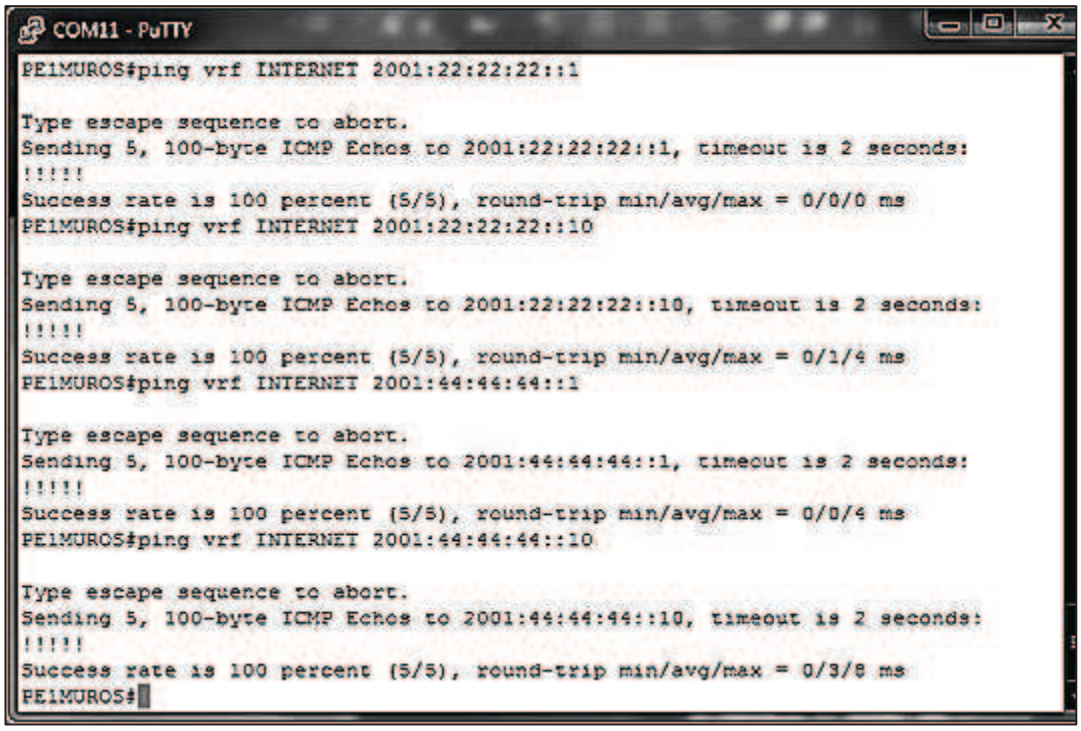


Figura 4.20 Comando “ping” a la red del cliente en IPv6 desde el PE1MUROS

Para revisar el estado de las interfaces en IPv6 de manera resumida, se tiene el comando “show ipv6 interface brief”, como se indica en la Figura 4.21.

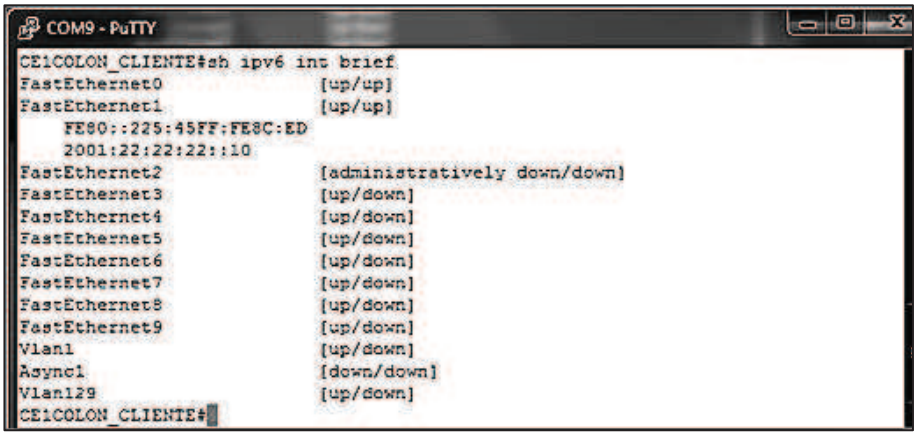


Figura 4.21 Verificación del estado resumido de las interfaces en IPv6

En el CE también se puede revisar la tabla de enrutamiento en IPv6 con el comando “show ipv6 route”, como se indica en la Figura 4.22.

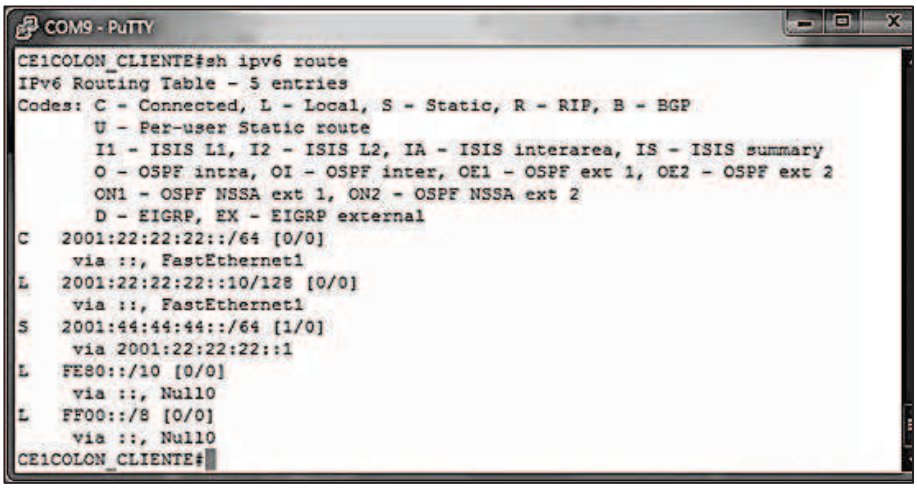


Figura 4.22 Verificación de la tabla de enrutamiento en IPv6

En la Figura 4.23, se indica el comando “ping” exitoso desde el router CE hacia las direcciones IPv6 de los routers LER y CE remotos.

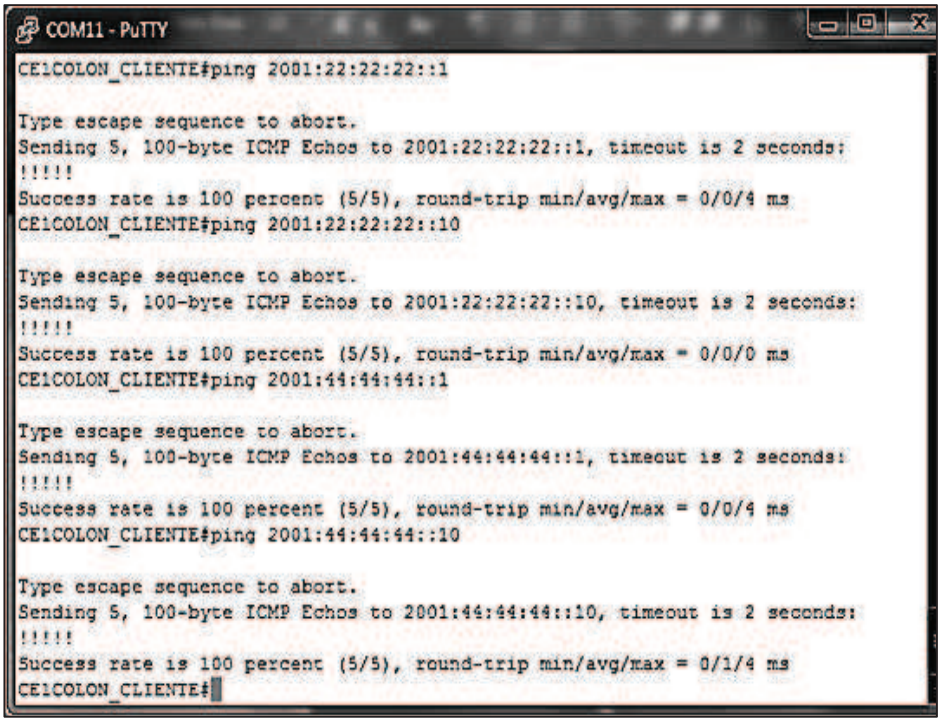


Figura 4.23 Comando “ping” a la red del cliente en IPv6 desde el CE

4.3.7. APLICACIONES DE MPLS

Las aplicaciones de MPLS que serán analizadas son:

- Redes Privadas Virtuales
- Calidad de Servicio
- Ingeniería de Tráfico

4.3.7.1. Configuraciones de las VPN de MPLS

Las VPN de MPLS pueden ser de capa 2 y capa 3 como se indican a continuación en las secciones 1 y 2.

1. Las VPN de MPLS de capa 2 (VPWS)

Para comprobar que la VPN de capa 2 está habilitada, se tiene el comando “show mpls l2transport vc 100” mostrado en la Figura 4.24, que presenta información de la dirección IP destino, el VC y el estado de la VPN.

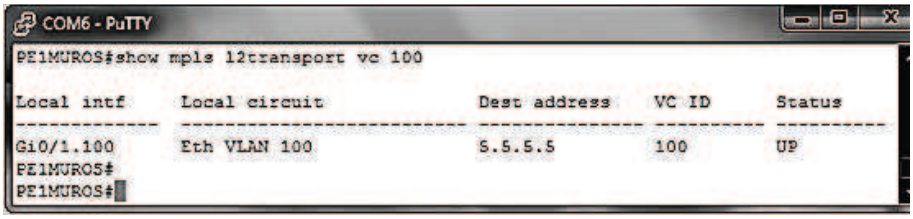


Figura 4.24 Verificación del estado de la VPN de capa 2

En la Figura 4.25 se muestra de manera detallada el estado de la VPN de capa 2 con el VC 100.

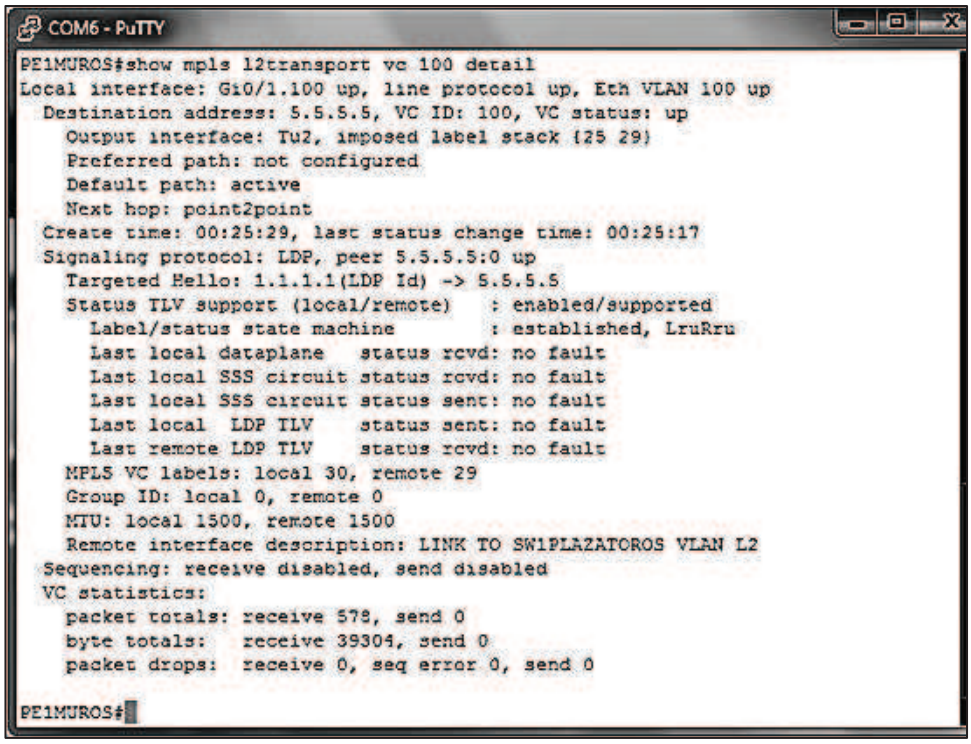


Figura 4.25 Verificación detallada del estado de la VPN de capa 2

En la Figura 4.26 se muestra el diagrama de la red con los dispositivos del cliente para establecer la VPN de capa 2. Debido a que el enrutamiento de las VPN de capa 2 está a cargo de los clientes, se deben configurar las interfaces de los dispositivos CE en una misma red de tal manera que simulen el transporte en capa 2. La redes utilizadas serán la 192.168.0.0/24 y 2001:29:192:168::0/64, a fin de que se compruebe que el proveedor solo se encarga del transporte de los paquetes y no presenta problemas de sobrelapamiento de redes, ya que la subred escogida es la misma que la utilizada en el enlace PE1MUROS-PGOSSEAL.

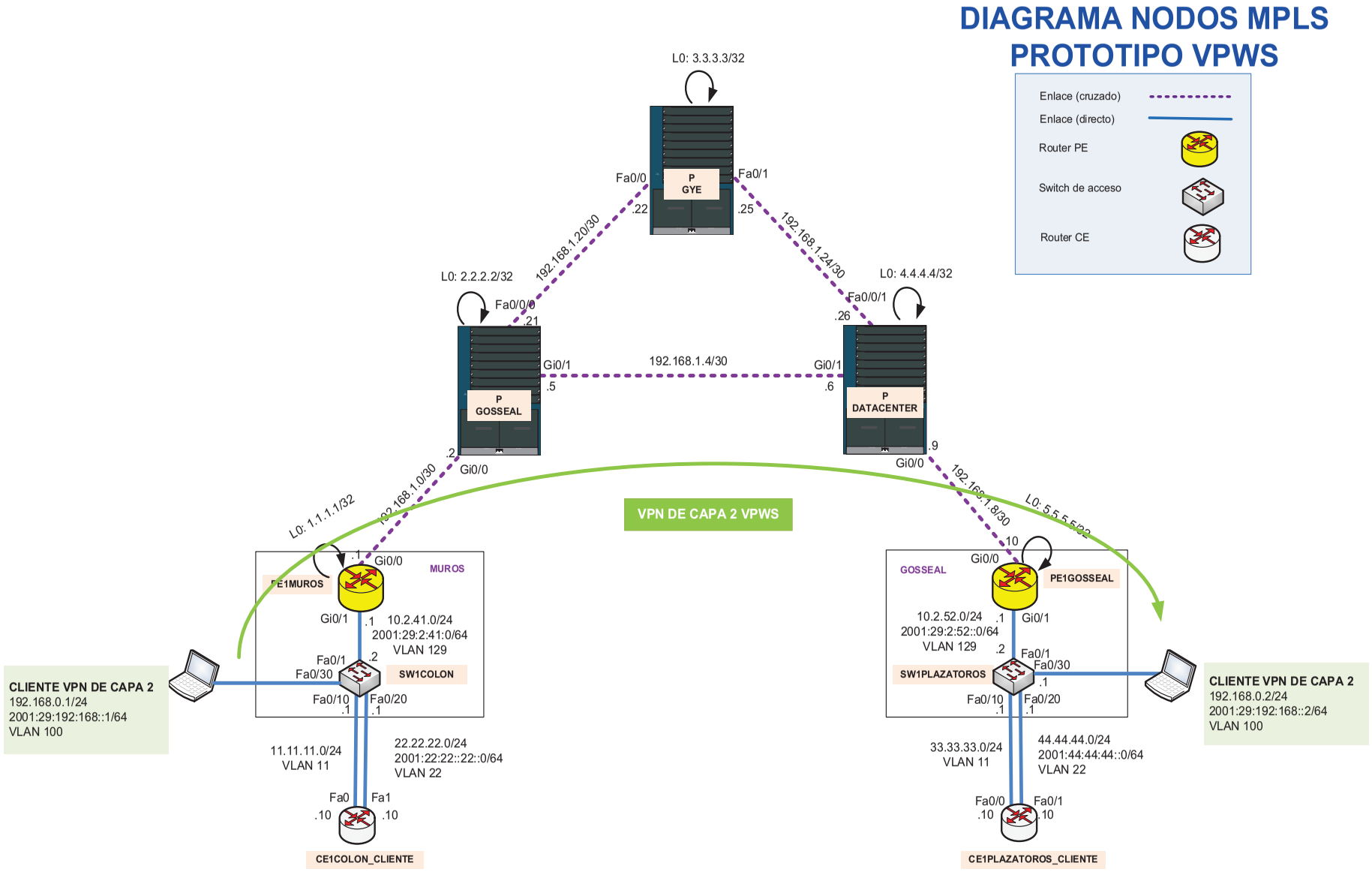


Figura 4.26 Prototipo de la red con las VPN de capa 2

Para comprobar la VPN de capa 2, se tiene el comando “ping” como se muestra en la Figura 4.27, donde se tiene conectividad hacia la PC remota.

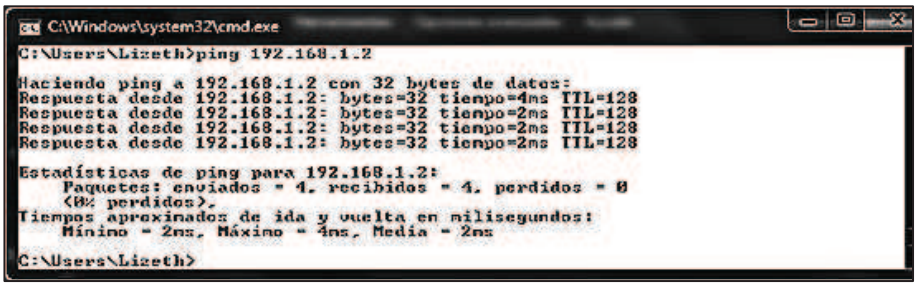


Figura 4.27 Verificación de la conectividad hacia la PC remota

En la Figura 4.28 se tiene el resultado del comando “ipconfig /all” en las PC, donde se muestra mayor detalle de las interfaces configuradas como la dirección física MAC del dispositivo.

Figura 4.28 Verificación de las direcciones físicas MAC en las P_CCOLON

Teniendo a conocimiento las direcciones físicas MAC de las PC, en los switches se puede realizar el comando “show mac address-table” en la Figura 4.29, para verificar que el dispositivo ha aprendido en su Tabla MAC, las direcciones físicas de las PC en la VLAN 100, como son: 00-1B-28-CD-11-31 y 00-1E-68-E0-A1-7D.

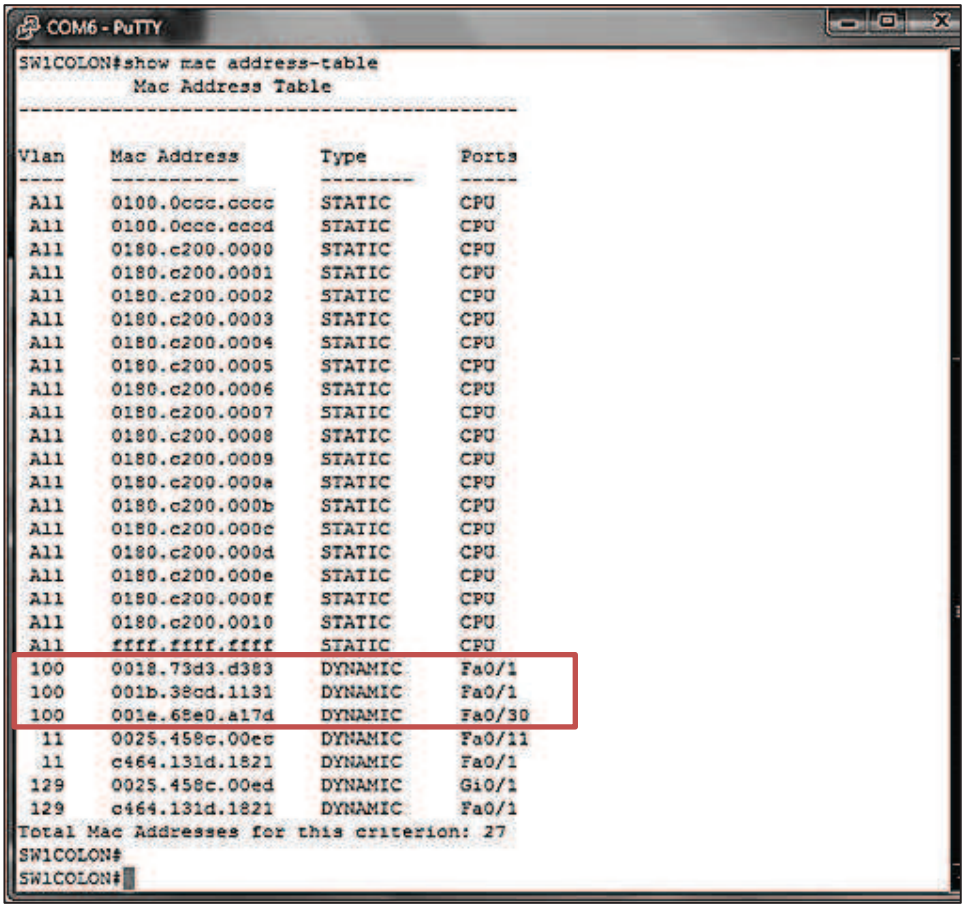


Figura 4.29 Verificación de la Tabla MAC

2. Las VPN de MPLS de capa 3 en IPv4[6][12]

En la Figura 4.30 se puede ver la tabla de enrutamiento de la VRF CLIENTE independiente de la tabla de enrutamiento global.

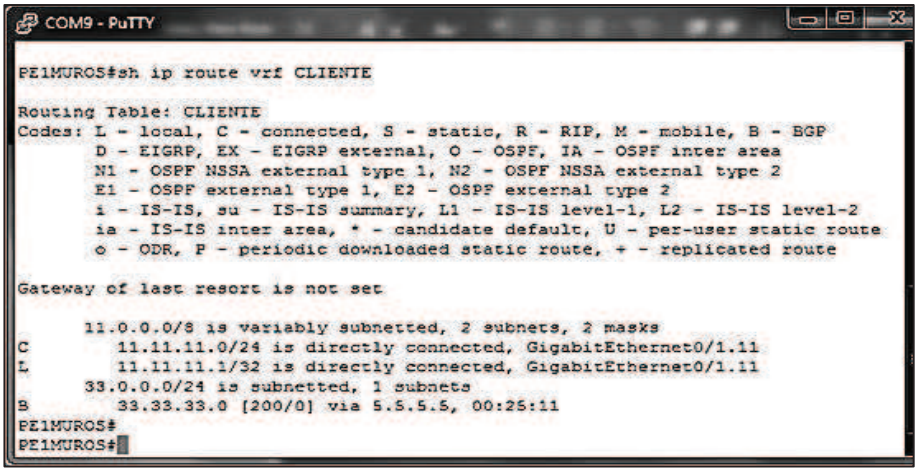


Figura 4.30 Verificación tabla de enrutamiento de la VRF CLIENTE

Para comprobar que la sesión MP-BGP está activa se tiene el comando “show ip bgp vpnv4 all summary”, donde se presenta información de los parámetros de tiempo, la versión, etc; como se muestra en la Figura 4.31.

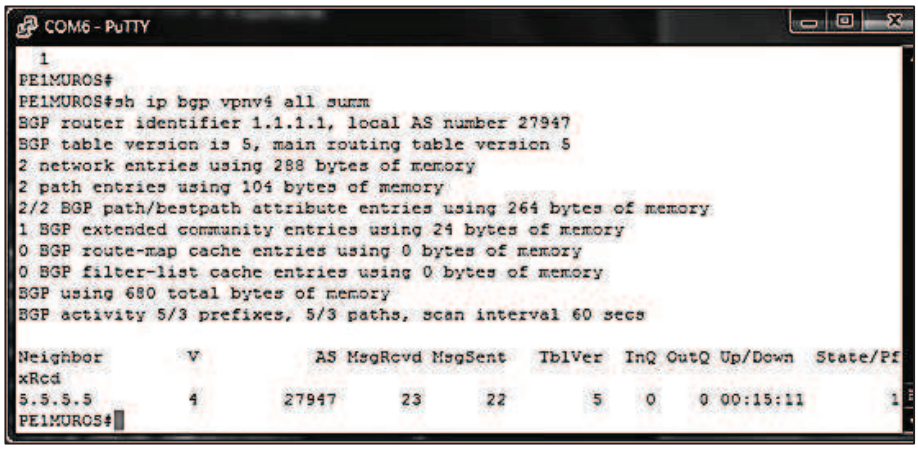


Figura 4.31 Verificación de la sesión vpnv4

Enrutamiento Estático PE-CE

Una vez configuradas las interfaces, se puede comprobar la conectividad a la red de la VRF CLIENTE mediante el comando “ping”, como se indica en la Figura 4.32.

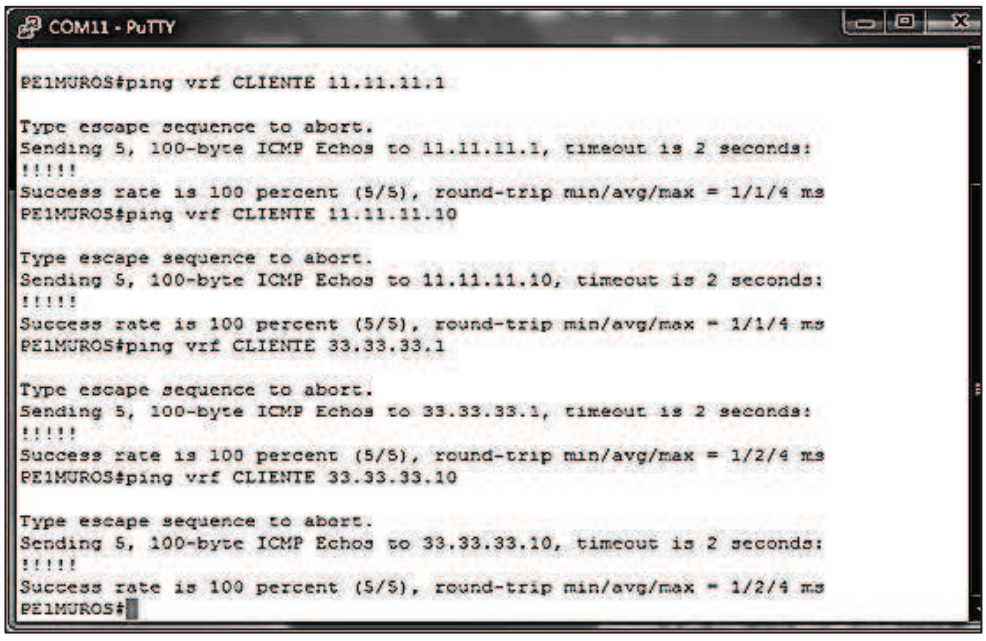


Figura 4.32 Comando “ping” a la red del CLIENTE desde el PE1MUROS

Enrutamiento Dinámico OSPF PE-CE

Como resultado de la configuración de la VPN de capa 3, se espera tener un comando “ping” exitoso, a la red del cliente publicada en la tabla de enrutamiento de la VRF en el PE, como se indica en la Figura 4.33.

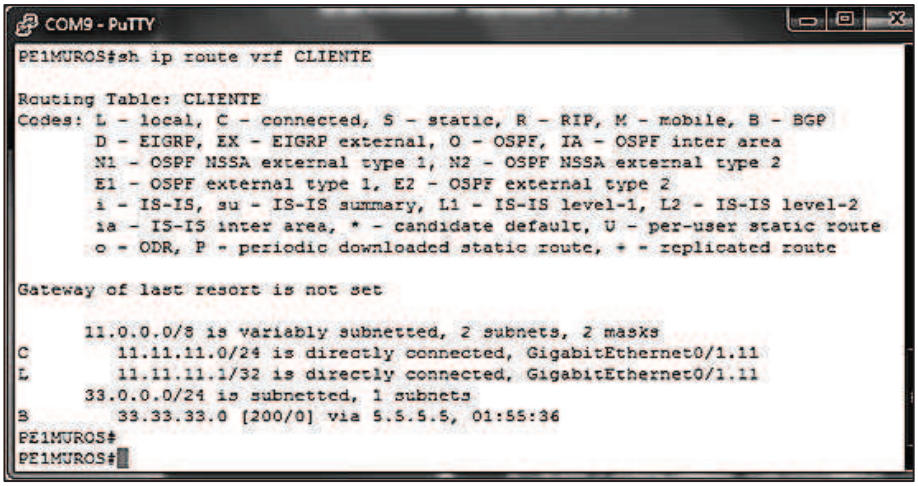


Figura 4.33 Verificación de la tabla de enrutamiento de la VRF CLIENTE

En la Figura 4.34, se tendrán los comandos “ping” exitosos hacia la red del cliente.

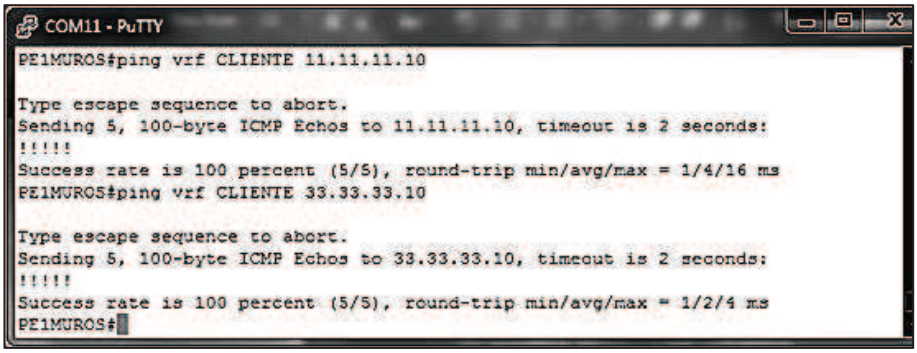


Figura 4.34 Comando “ping” a la red del CLIENTE desde el PE1MUROS

3. Las VPN de MPLS de capa 3 de doble pila[6][12]

Se espera como resultado, tener conectividad mediante el comando “ping” hacia las redes en IPv4 e IPv6 de la VRF en los dispositivos remotos, como se indica en la Figura 4.35.

Figura 4.35 Verificación de la conectividad desde el PE1MUROS

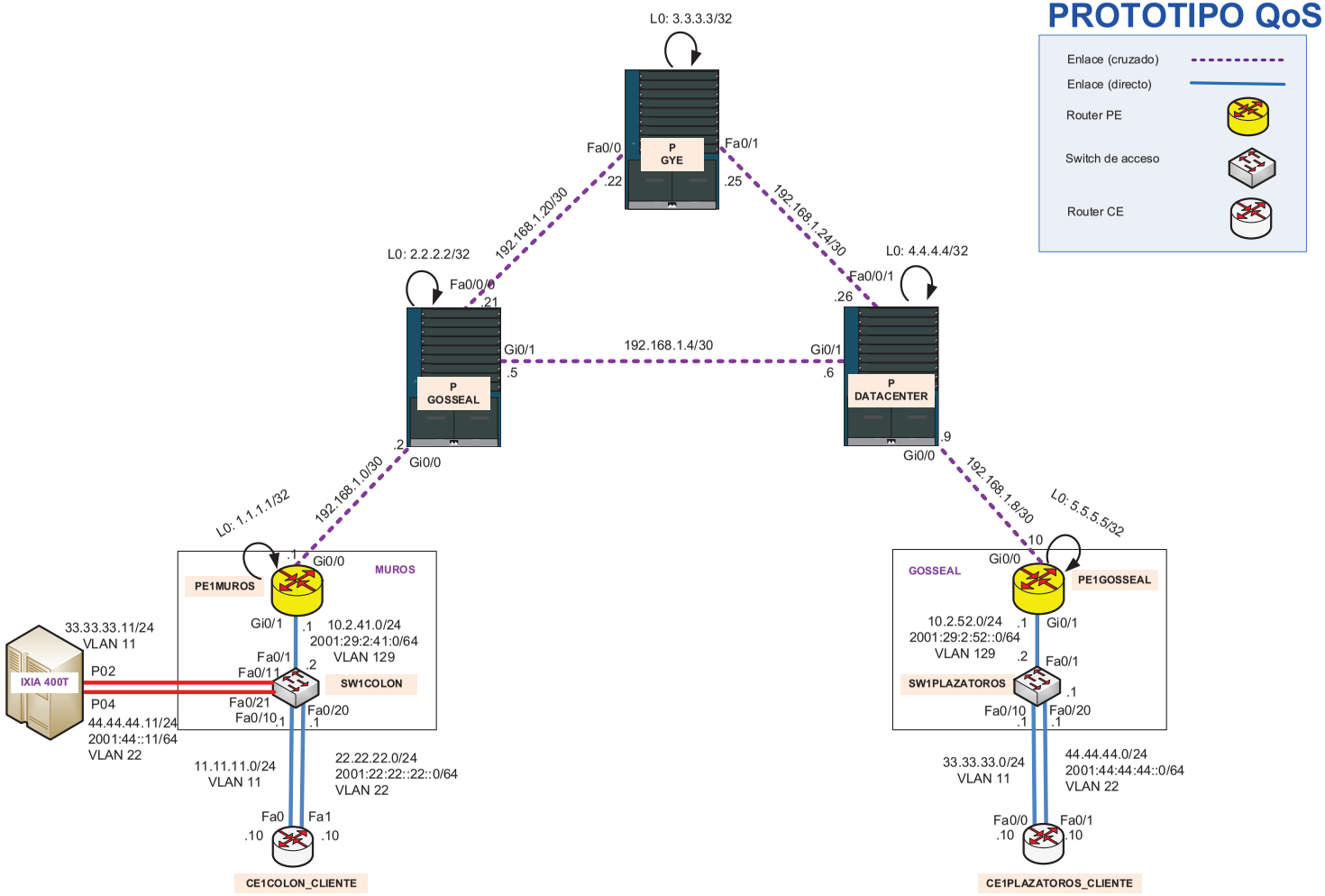
4.3.7.2. Configuración de Calidad de Servicio[9][10]

La implementación de Calidad de Servicio en el presente prototipo, se centra en configurar la nube MPLS y los switches de acceso que deben confiar en los paquetes previamente marcados en el CE.

Las configuraciones de QoS se realizarán para un dispositivo en particular de las capas del modelo jerárquico. Las diferencias se verán reflejadas en el número, tipo de interfaces y direcciones IP, según la Tabla 4.3.

La Calidad de Servicio solo se puede comprobar cuando en la red se tienen enlaces saturados, es por ello que se va a conectar el generador de tráfico IXIA 400T[11] a la red, como se detalla en la Figura 4.36.

La manera de acceder al escritorio remoto del generador de tráfico IXIA 400T y las configuraciones establecidas, se detallan en el ANEXO H.



SW1COLON

INTERFAZ	IP4/6	GATEWAY	VLAN
Fa0/1 – Fa0/9	10.2.41.0/24	10.2.41.1	trunk
Fa0/10 – Fa0/19	11.11.11.0/24	11.11.11.1	11
Fa0/20 – Fa0/29	22.22.22.0/24	22.22.22.1	22
	2001:22:22:22::0/64	2001:22:22:22::1	22
Fa0/30 – Fa0/39	-	-	100

SW1PLAZATOROS

INTERFAZ	IP4/6	GATEWAY	VLAN
Fa0/1 – Fa0/9	10.2.52.0/24	10.2.52.1	trunk
Fa0/10 – Fa0/19	33.33.33.0/24	33.33.33.1	11
Fa0/20 – Fa0/29	44.44.44.0/24	44.44.44.1	22
	2001:44:44:44::0/64	2001:44.44.44::1	22
Fa0/30 – Fa0/39	-	-	100

Figura 4.36 Prototipo de la red con QoS

1. Capa núcleo: los routers LER y LSR[5]

Para tener un análisis de tráfico en periodos de tiempo más cortos, se utiliza el comando “load-interval” que permite reconfigurar el intervalo de tiempo en segundos, como se indica en la Figura 4.37.

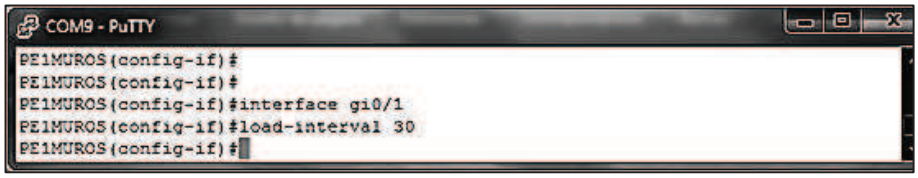


Figura 4.37 Verificación de la conectividad desde el CE1COLON

Para comprobar la política limitadora de tráfico, el generador debe estar configurado para transmitir 2 Mbps; proceso que se detalla en el ANEXO H Figuras H.20-28. Entonces, se puede observar en la interfaz gi0/1, un total de 2 Mbps de tráfico de entrada, como se detalla en la Figura 4.38.

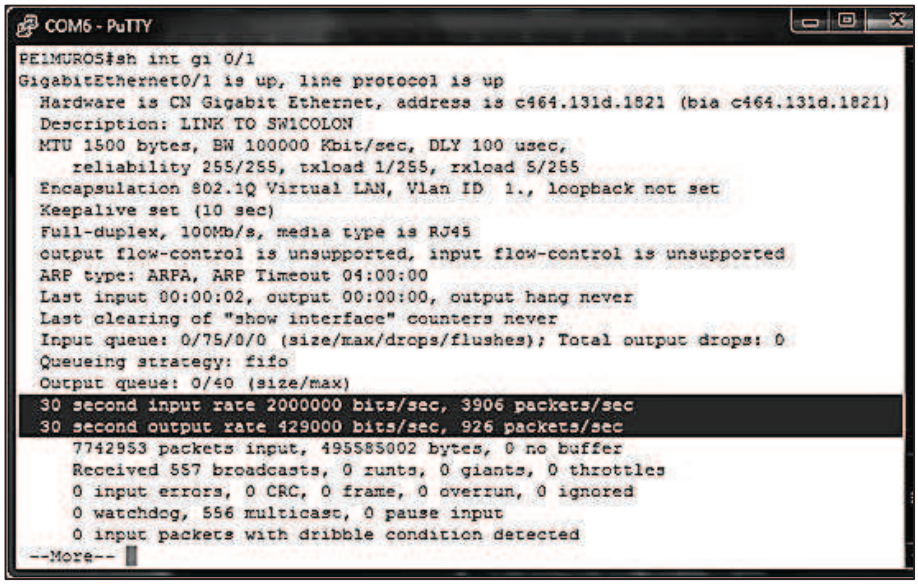


Figura 4.38 Verificación de la velocidad de tráfico de entrada de 2 Mbps

Para verificar que se ha configurado la política, se tiene el comando “show policy-map”, donde se detallan todos los parámetros configurados de la política, como se indica en la Figura 4.39.

Figura 4.39 Verificación de la configuración de la política

En la Figura 4.40 se muestra el comando “show class-map” para verificar la configuración de las clases.

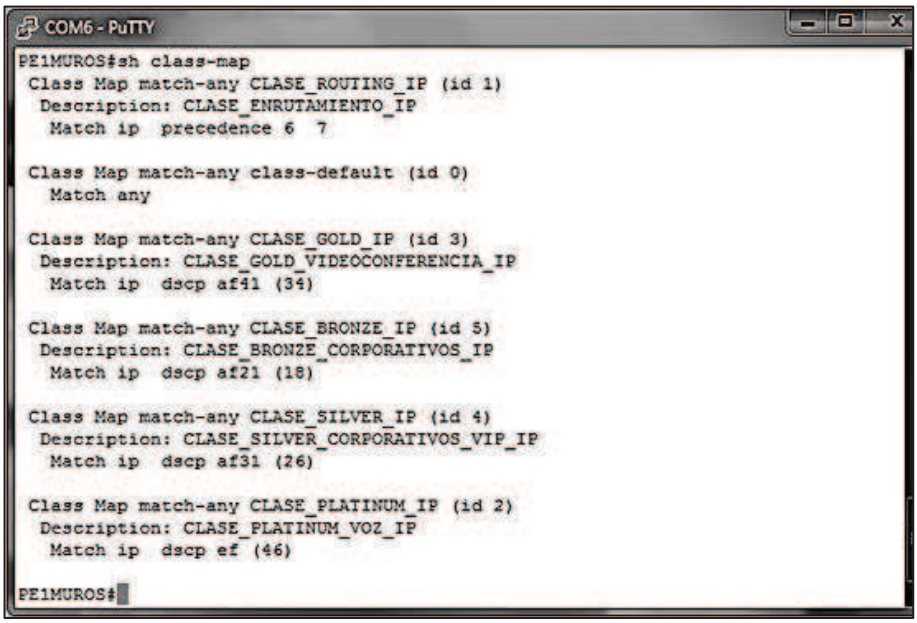


Figura 4.40 Verificación de la configuración de las clases

Una vez aplicada la política en la interfaz, y generando mayor tráfico con el IXIA 400T que el valor configurado, se observará que los paquetes excedidos serán descartados ante la presencia de saturación. En la Figura 4.41 se indica el resultado del comando “show policy-map int gi0/1”, donde se detalla el descarte de los paquetes.

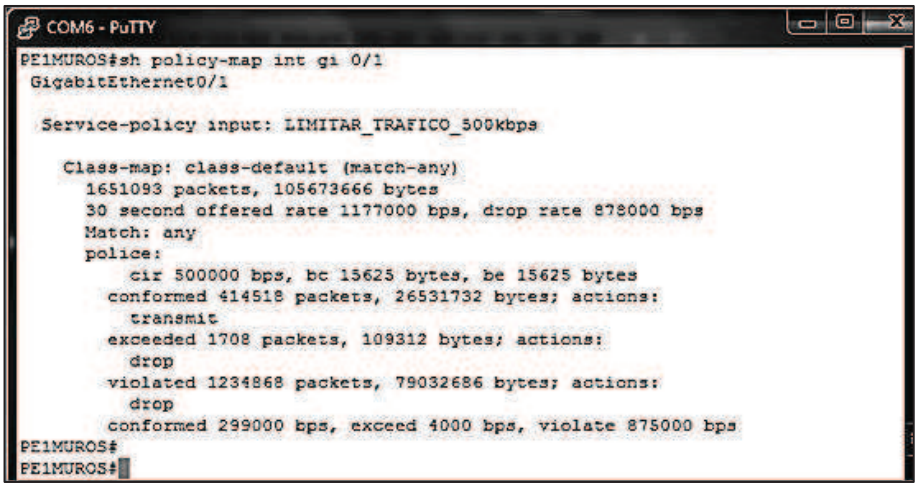


Figura 4.41 Verificación de los paquetes descartados

Para verificar los parámetros configurados en las políticas de una determinada interfaz, se tiene el comando “show policy-map int gi 0/0” como se muestra en la Figura 4.42.

Figura 4.42 Verificación de los parámetros de la política de la interfaz gi0/0

2. Capa distribución y acceso

Para comprobar que MPS está habilitado en el switch, se tiene el comando “show mls qos”, como se indica en la Figura 4.43.

Figura 4.43 Verificación de la configuración de MLS

Para verificar que los parámetros de las colas de entrada fueron correctamente, se tiene el comando “show mls qos input-queue”, como se indica en la Figura 4.44.

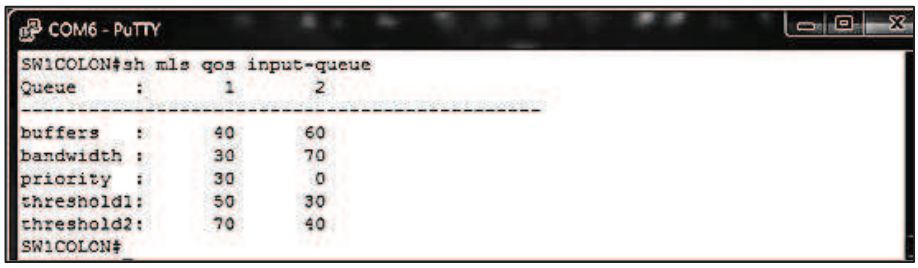


Figura 4.44 Verificación de los parámetros de las colas de entrada

Para verificar que los parámetros de las colas de salida fueron correctamente, se tiene el comando “show mls qos queue-set 1”, como se indica en la Figura 4.45.

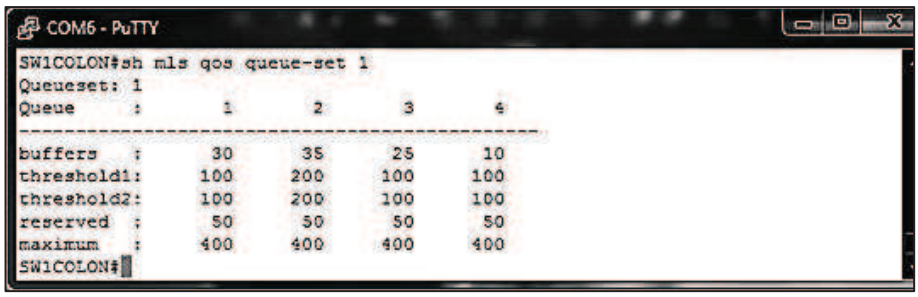


Figura 4.45 Verificación de los parámetros de las colas de salida

3. Resultados obtenidos de QoS en IPv4

En la Figura 4.46, se indica la política de entrada configurada en la subinterfaz gi0/1.11, donde se agrupa el tráfico en las cinco diferentes CoS para definir el mapa de correspondencias DSCP-EXP.

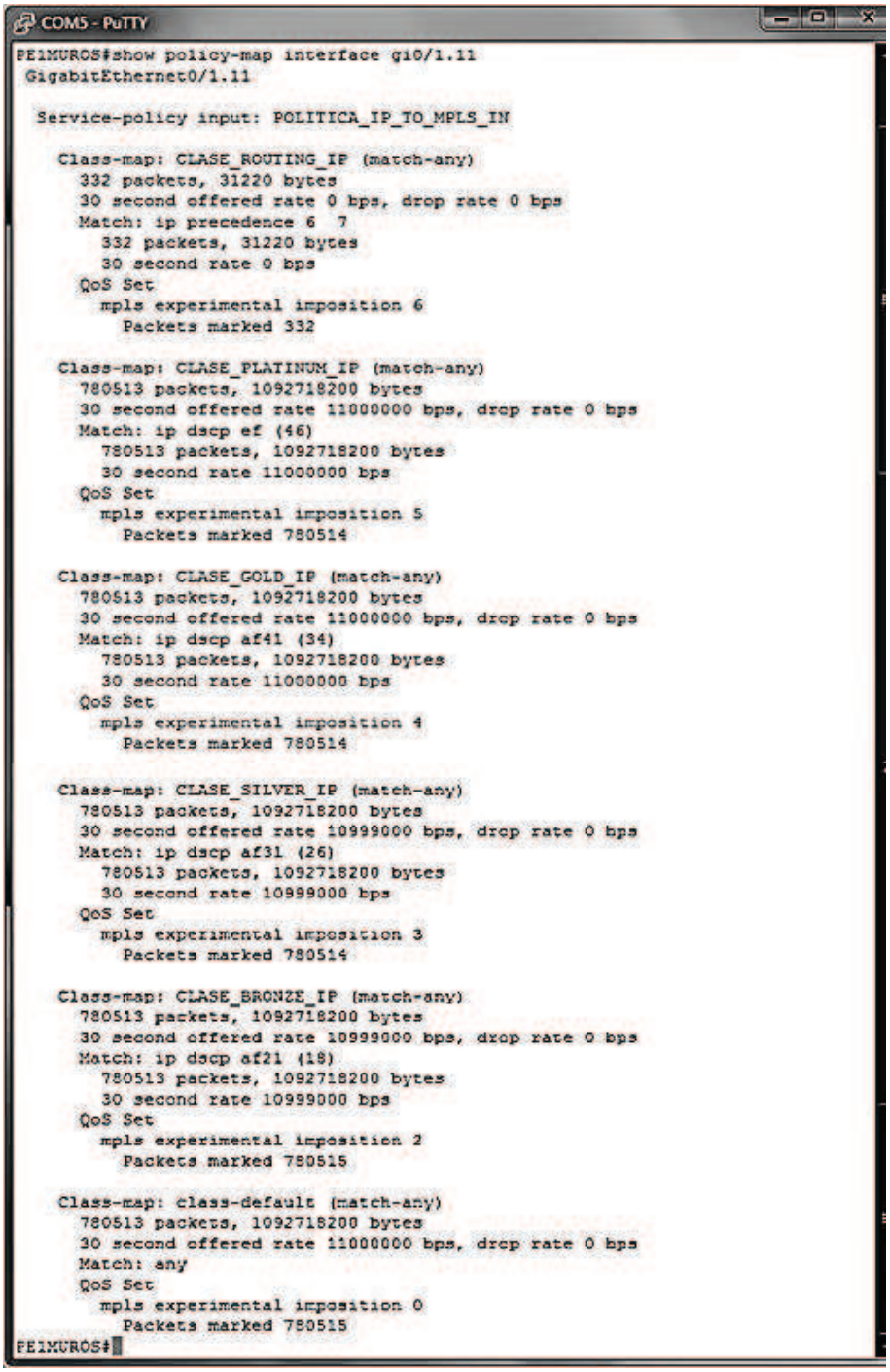


Figura 4.46 Verificación de la política de entrada en la gi0/1.11

En la Figura 4.47, se indica el resultado del comando “ping” desde el cliente CE1COLON hasta la red del CE1PLAZATOROS. El comando “ping” no tiene un trato preferencial en la red, es por ello que durante la saturación del enlace se tiene 3 paquetes perdidos de 5.

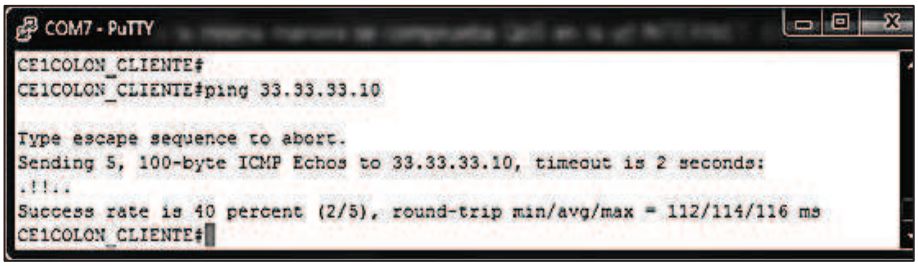


Figura 4.47 Verificación del comando “ping” con saturación

Por el contrario, desde el PE1MUROS se realizará el comando “ping” extendido marcado con 184 en el campo *Type of Service,* hacia la red del router CE1PLAZATOROS, como se muestra en la Figura 4.48.

Figura 4.48 Verificación del tráfico de llegada al router CE

4. Resultados obtenidos de QoS en *Dual Stack*

En la Figura 4.49, se indica la política de entrada configurada en la subinterfaz gi0/1.22, donde se agrupa el tráfico en las cinco diferentes CoS para definir el mapa de correspondencias DSCP-EXP.

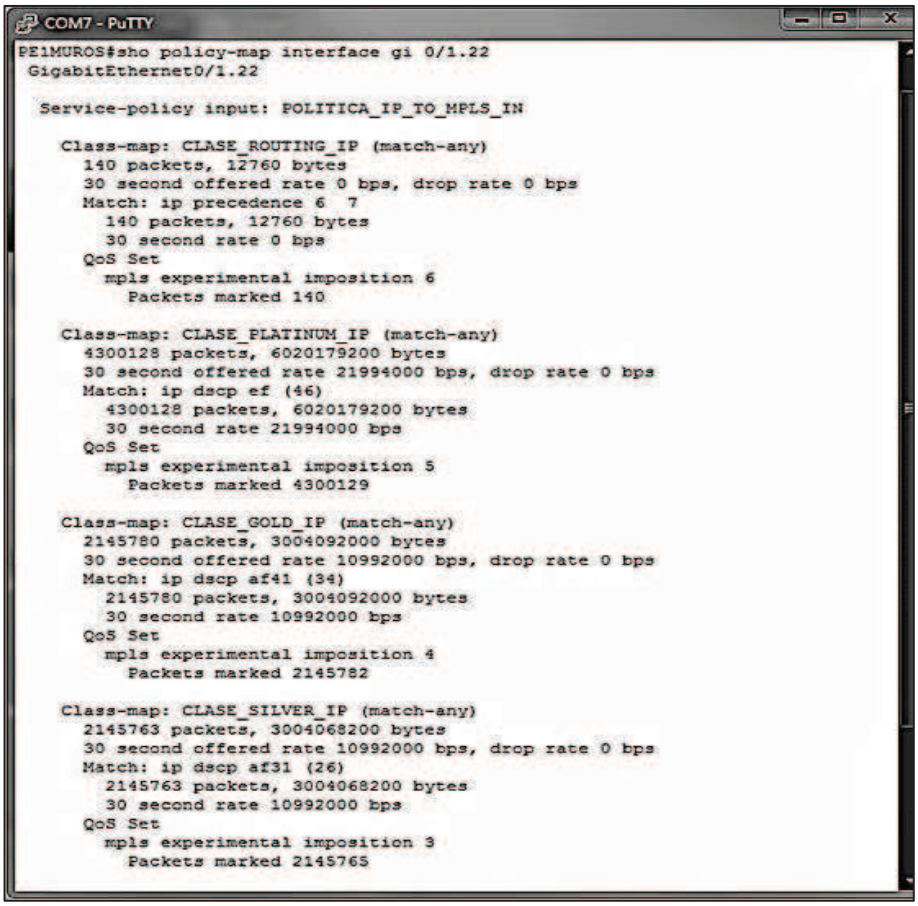


Figura 4.49 Verificación de la política de entrada en la gi0/1.22

Desde el CE1COLON, se realizará el comando “ping” extendido marcado con 184 en el campo *Type of Service,* hacia la red del router CE1PLAZATOROS en IPv4, como se muestra en la Figura 4.50.

Figura 4.50 Verificación del comando “ping” en IPv4 y ToS en 184

Por el contrario, desde el CE1COLON se realizará el comando “ping” extendido marcado con 184 en el campo *Type of Service,* hacia la red del router CE1PLAZATOROS en IPv6, como se muestra en la Figura 4.51.

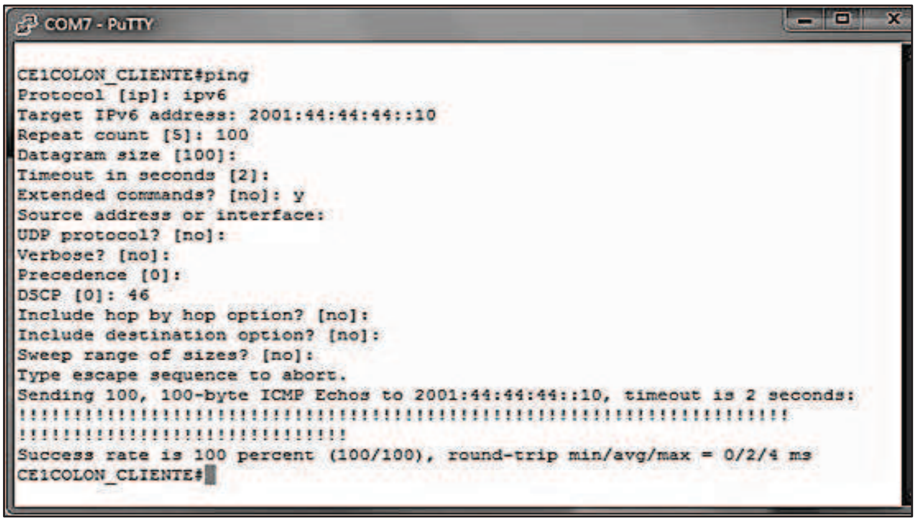


Figura 4.51 Verificación del comando “ping” en IPv6 y ToS en 184

4.3.7.3. Configuración de Ingeniería de Tráfico

La configuración de Ingeniería de Tráfico se centra en la creación de túneles TE para brindar balanceo de carga y redundancia de enlaces. Los requerimientos previos a levantar TE son: OSPF, CEF, LDP y MPLS.

Creación de los túneles TE para balanceo de carga

En la Figura 4.52 se indica el prototipo de configuración para balanceo de carga en la red. Se crearán 4 túneles, de los cuales los túneles 1 y 2 serán en sentido PE1MUROS-PE1GOSSEAL, y los túneles 3 y 4, en sentido PE1GOSSEAL-PE1MUROS.

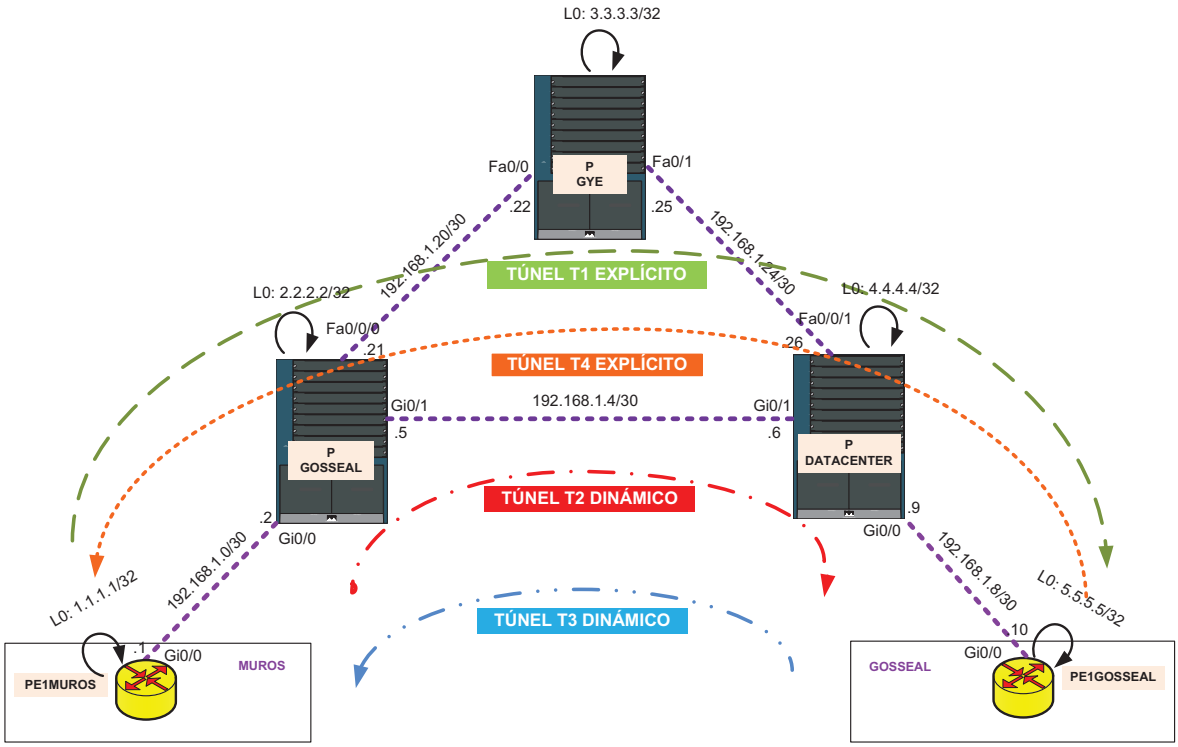


Figura 4.52 Prototipo de la red con TE - balanceo de carga

Para comprobar que se ha reservado la capacidad de ancho de banda con RSVP, se utiliza el comando “show ip rsvp interface gi 0/0”, como se indica en la Figura 4.53.

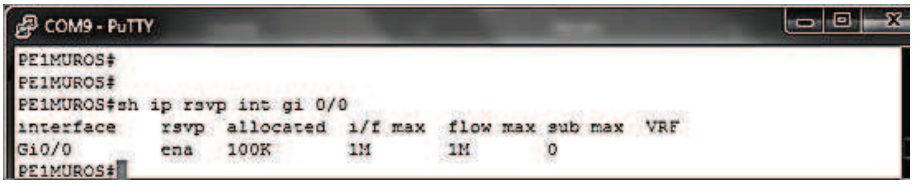


Figura 4.53 Verificación de RSVP

Para obtener información más detallada de la configuración del túnel 1, se tiene el comando “show mpls traffic-eng tunnel t1”, como se muestra en la Figura 4.54.

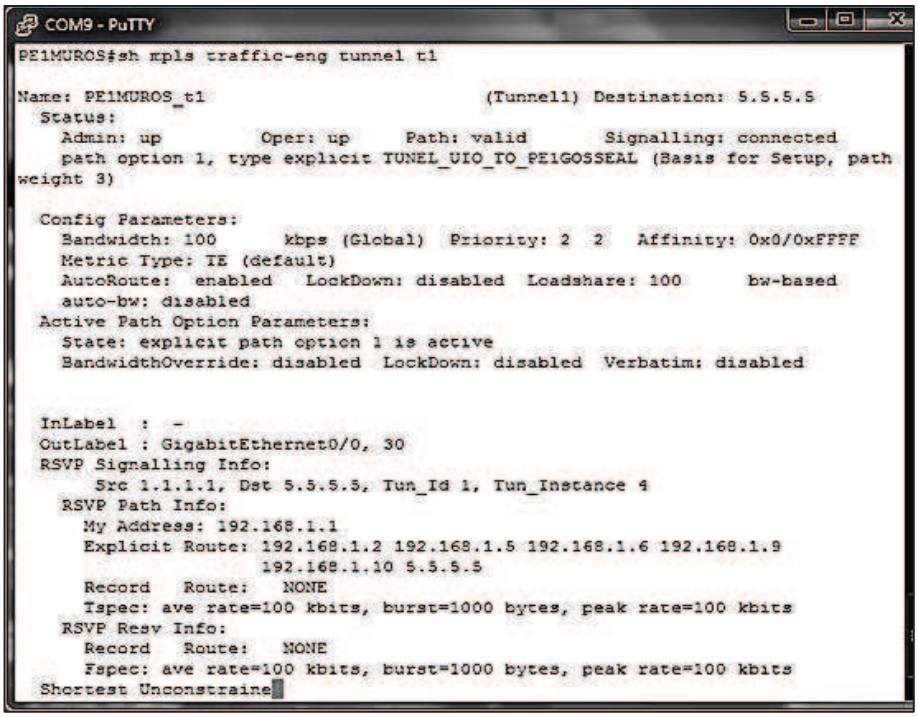


Figura 4.54 Verificación detallada de las configuraciones del túnel 1

Resultados obtenidos de la configuración de Ingeniería de Tráfico - balanceo de carga

En la Figura 4.55 se puede ver que para alcanzar la loopback 5.5.5.5 se observa que ahora se tienen dos caminos, como son: el túnel 1 y túnel 2.

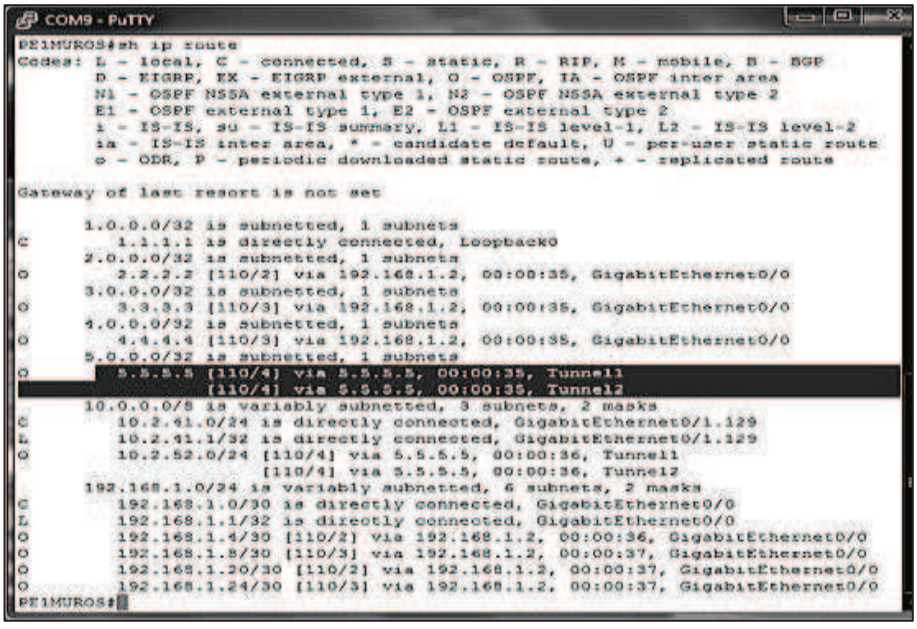


Figura 4.55 Verificación de la tabla de enrutamiento

Para mayor detalle en el comando “show ip route 5.5.5.5”, se observa el balanceo asimétrico (1:2) en la Figura 4.56, ya que el ancho de banda reservado en cada túnel es diferente. El Túnel 1 reserva 100kbps, mientras el túnel 2, 200kbps.

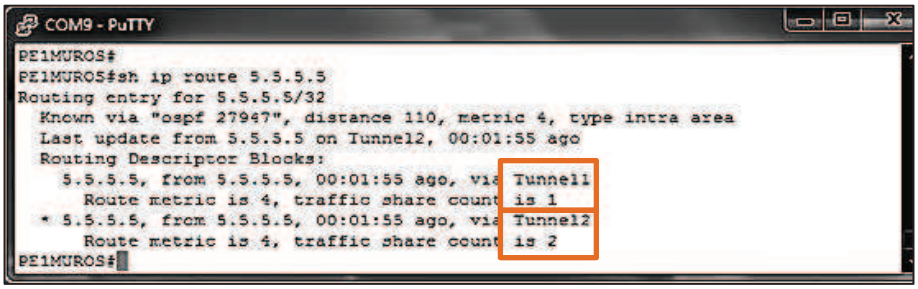


Figura 4.56 Verificación del balanceo de carga asimétrico

Ahora el balanceo es simétrico (1:1), donde el túnel 1 y 2 comparten el tráfico en proporciones iguales, como se indica en la Figura 4.57.

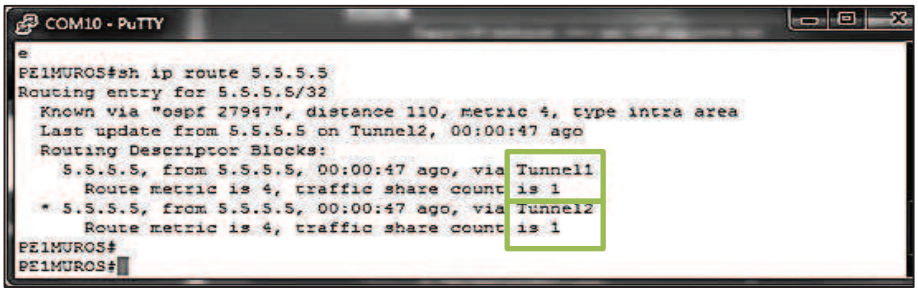


Figura 4.57 Verificación del balanceo de carga asimétrico

Para verificar que los túneles TE están en estado activo, se tiene el comando “show mpls traffic-eng tunnels brief”, como se indica en la Figura 4.58.

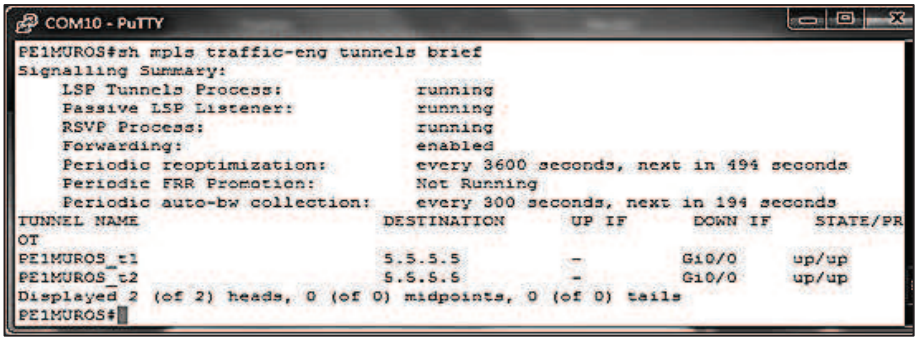


Figura 4.58 Verificación del estado de los túneles

Redundancia de enlaces con túneles TE

La Ingeniería de Tráfico mediante el comando *Fast Re-Route,* permite brindar redundancia de enlaces, a través de la creación de túneles de respaldo. La interfaz protegida debe ser definida y configurada para reenrutar el tráfico en el menor tiempo posible.

En la Figura 4.59 se indica el diagrama para brindar redundancia del enlace PGOSSEAL-PDATACENTER.

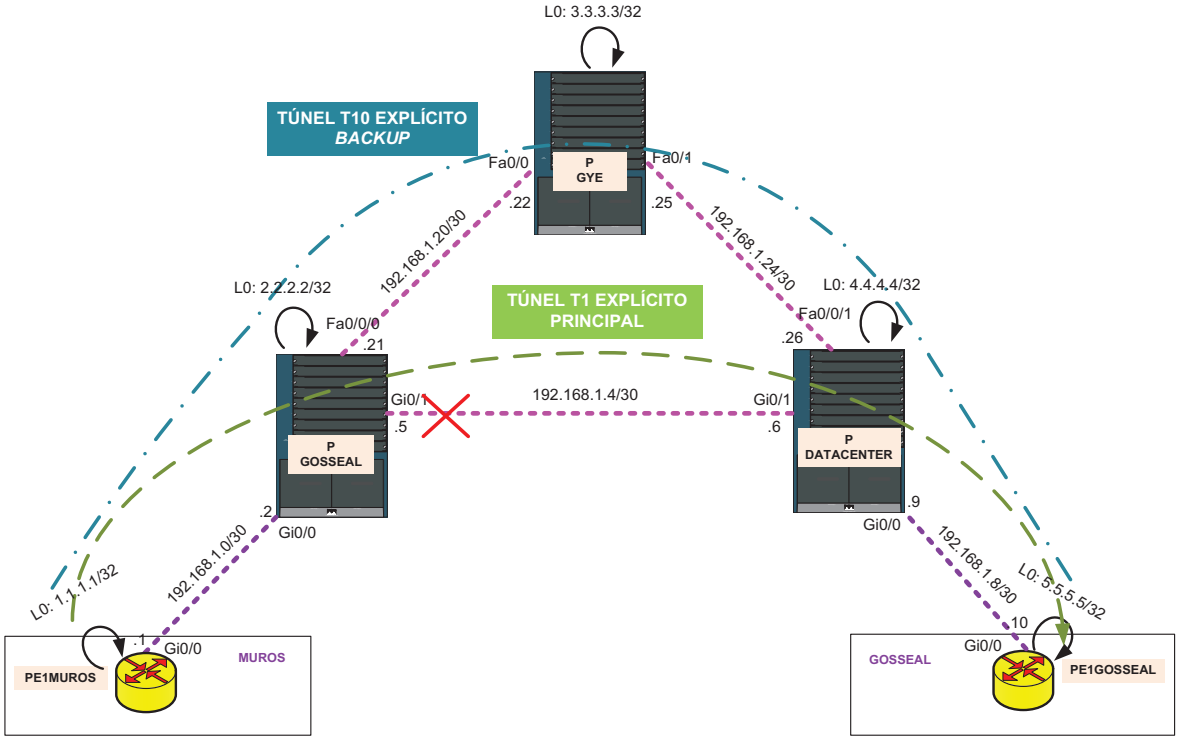


Figura 4.59 Prototipo de la red con TE – redundancia de enlaces túneles 1 y 10

Para verificar la configuración de *Fast Re-Route* en el túnel, se utiliza el comando de la Figura 4.60.

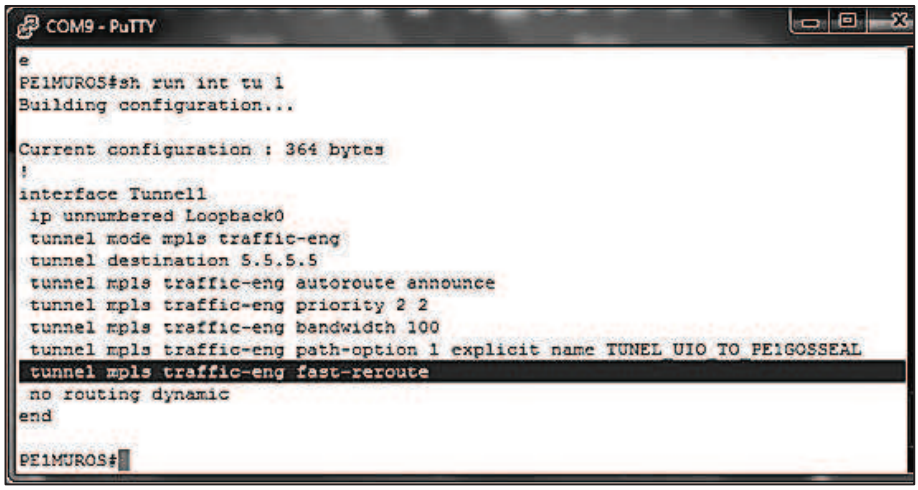


Figura 4.60 Verificación de la configuración de *Fast Re-Route*

Resultados obtenidos de la configuración de Ingeniería de Tráfico – redundancia de enlaces

El resultado esperado es que cuando la interfaz gi0/1 del PGOSSEAL cambie de estado a *down,* no exista gran pérdida de paquetes ya que el tráfico se reenrutará por el túnel de respaldo.

Para verificar el estado de los túneles TE, se utiliza el comando “show mpls traffic-eng tunnels brief”, mostrado en la Figura 4.61.

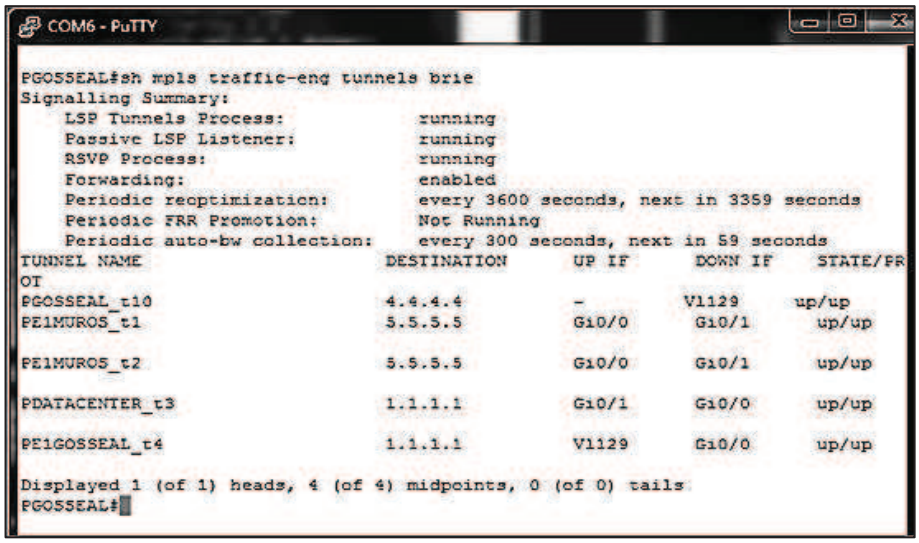


Figura 4.61 Verificación de los estados de los túneles creados

En la Figura 4.62 se observa que el túnel 10 está en estado listo de protección a la interfaz gi0/1 del PGOSSEAL.

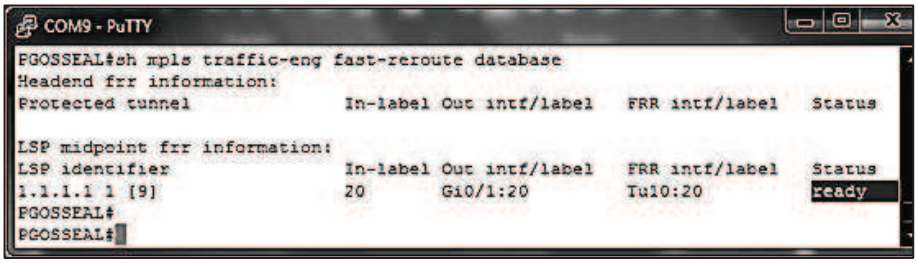


Figura 4.62 Verificación del estado listo de la interfaz gi0/1 con el túnel 10

Para comprobar el funcionamiento de *Fast Re-Route,* se va a realizar un comando "ping" continuo de 2500 paquetes como se indica en la Figura 4.63; para durante este tiempo, desconectar la interfaz protegida gi0/1 del PGOSSEAL y analizar el número de paquetes perdidos, así como la activación del túnel 10 de respaldo.

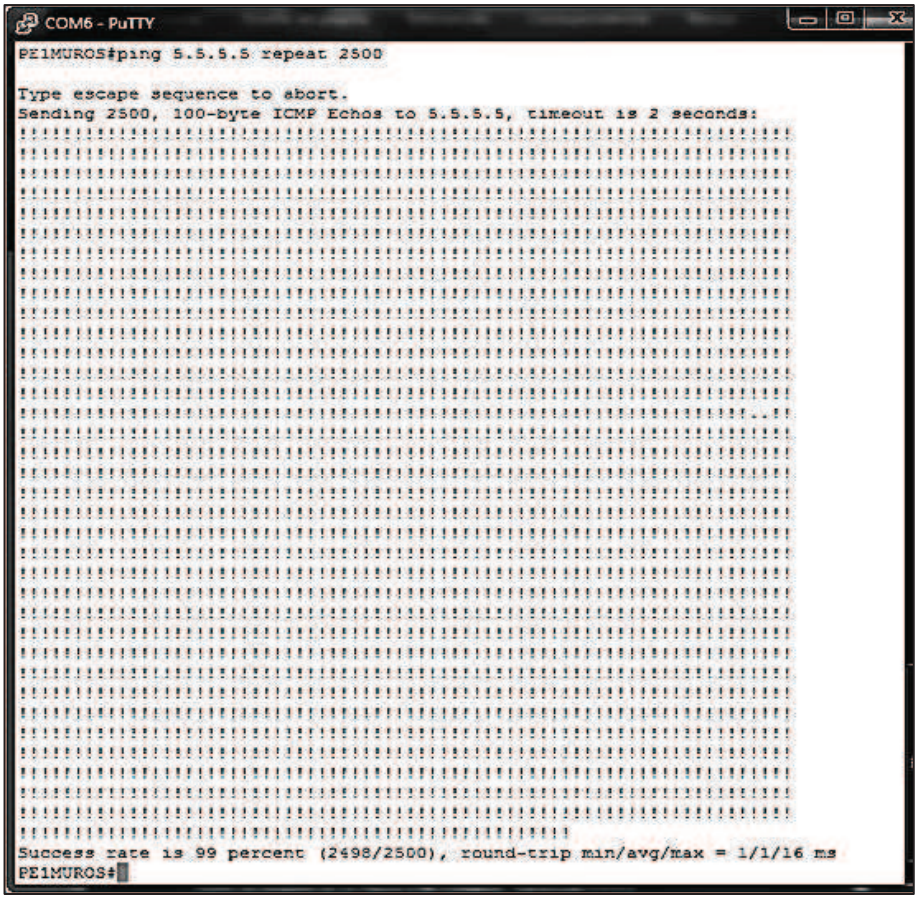


Figura 4.63 Comando "ping" continuo 2500

Según el comando “show mpls traffic-eng fast-reroute database” de la Figura 4.64, se observa que el túnel 10 ha cambiado de estado de listo a activo.

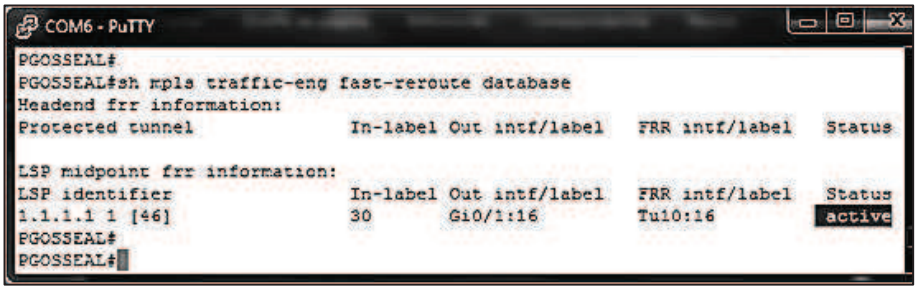


Figura 4.64 Verificación del estado del túnel de respaldo en activo

Configuración de los Túneles 3 y 30 Respaldo

Para proteger la interfaz gi0/1 del PDATACENTER, se deben realizar las mismas configuraciones y pruebas para los túneles 3 y 30 respaldo, como se indica en la Figura 4.65.

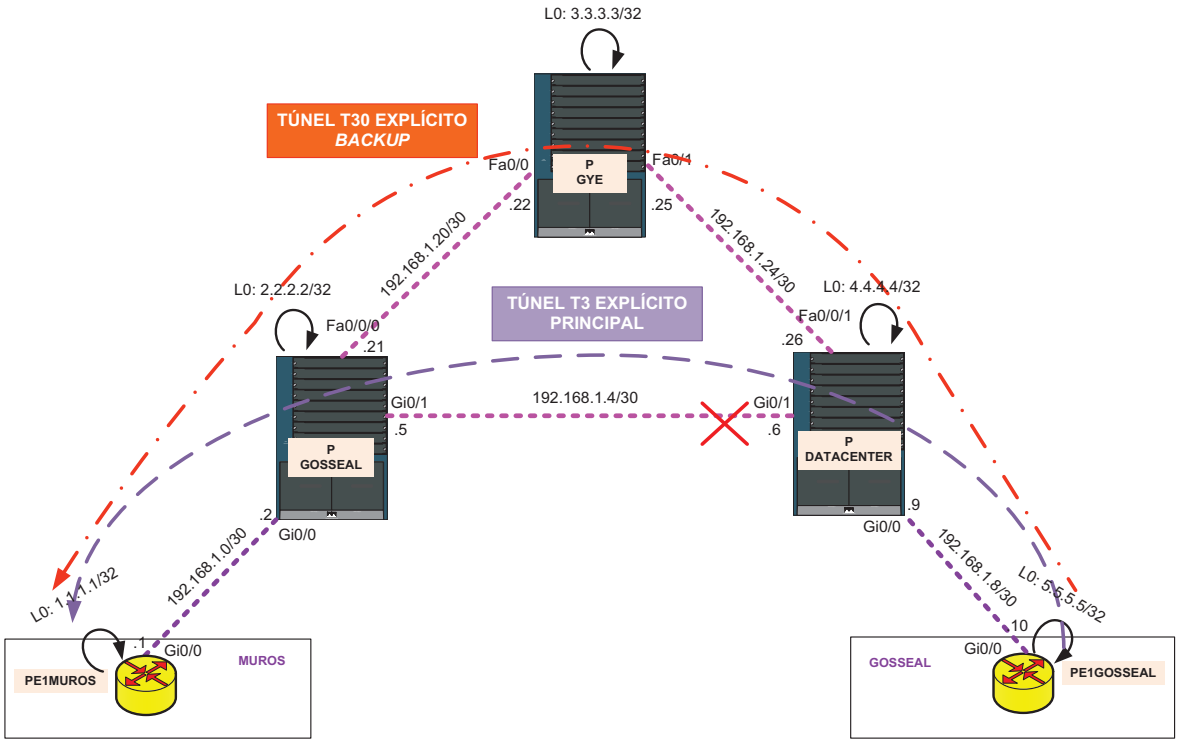


Figura 4.65 Prototipo de la red con TE – redundancia de enlaces túneles 3 y 30

En la Figura 4.66 se verifican los estados activos de los túneles 3 y 30.

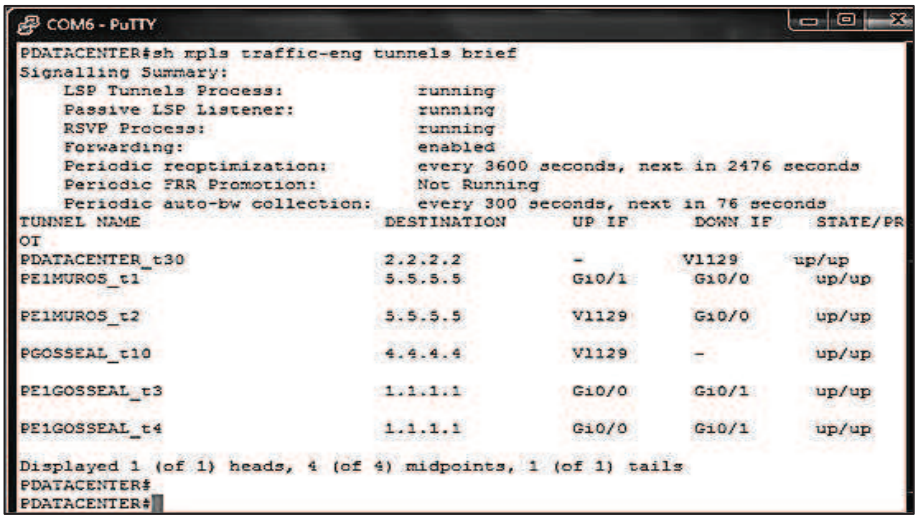


Figura 4.66 Verificación del estado del túnel 3

De la misma manera que con los túneles 1 y 10, la pérdida de los paquetes con los túneles 3 y 30 respaldo, son mínimos como se muestra en la Figura 4.67.

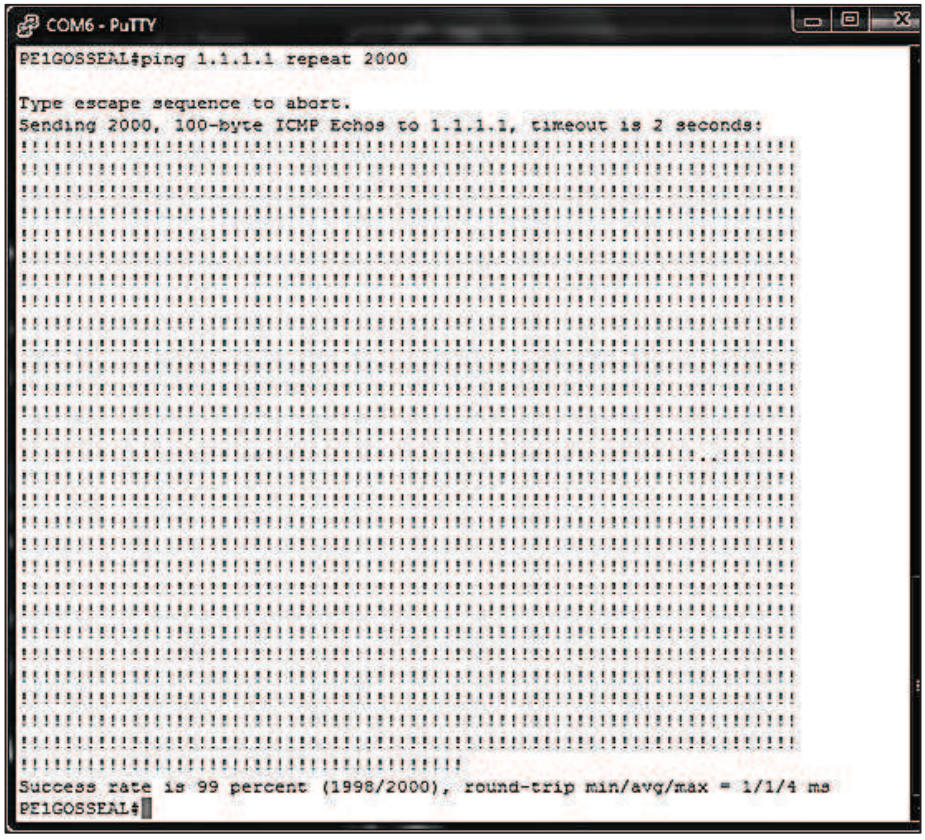


Figura 4.67 Comando “ping” continuo hacia 1.1.1.1

4.3.8. CONFIGURACIÓN DE SEGURIDAD EN IPv6

Las Mejores Prácticas de Seguridad que serán analizadas son:

- VLAN
- Listas de Control de Acceso en IPv6
- Gestión mediante acceso remoto seguro.

En el ANEXO I se indican las configuraciones y pruebas a detalle de las Mejores Prácticas de Seguridad en IPv6 analizadas para el presente prototipo.

4.3.8.1. VLAN

En la Figura 4.68 se muestra el comando “sdm prefer dual-ipv4-and-ipv6 default” para habilitar la plantilla de doble pila en los switches 3560. Luego, es necesario reiniciar el dispositivo de tal manera que la plantilla tenga efecto.

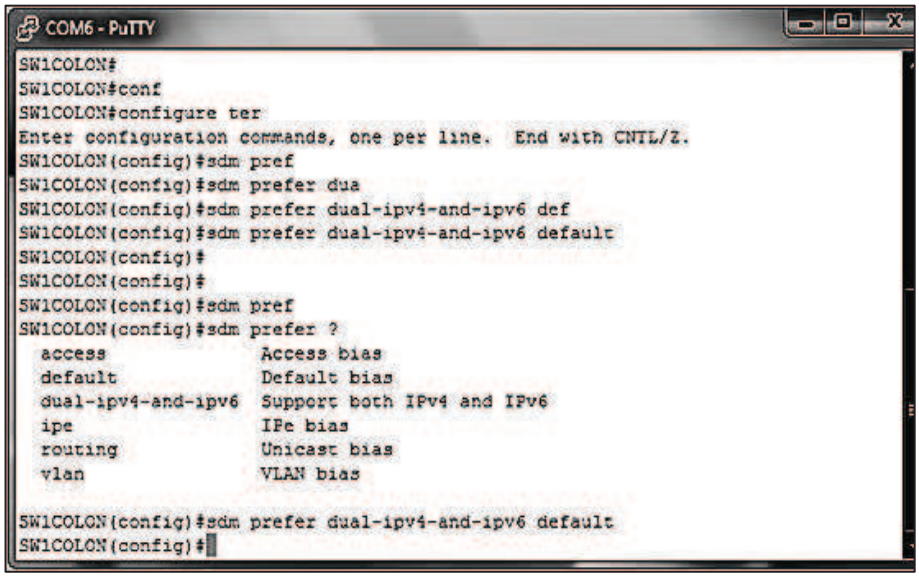


Figura 4.68 Habilitar la plantilla de doble pila

4.3.8.2. Listas de Control de Acceso (ACL) en IPv6

En la Figura 4.69 se indica el resultado del comando ”show access-lists” que sirve verificar las configuraciones de las ACL en el dispositivo.

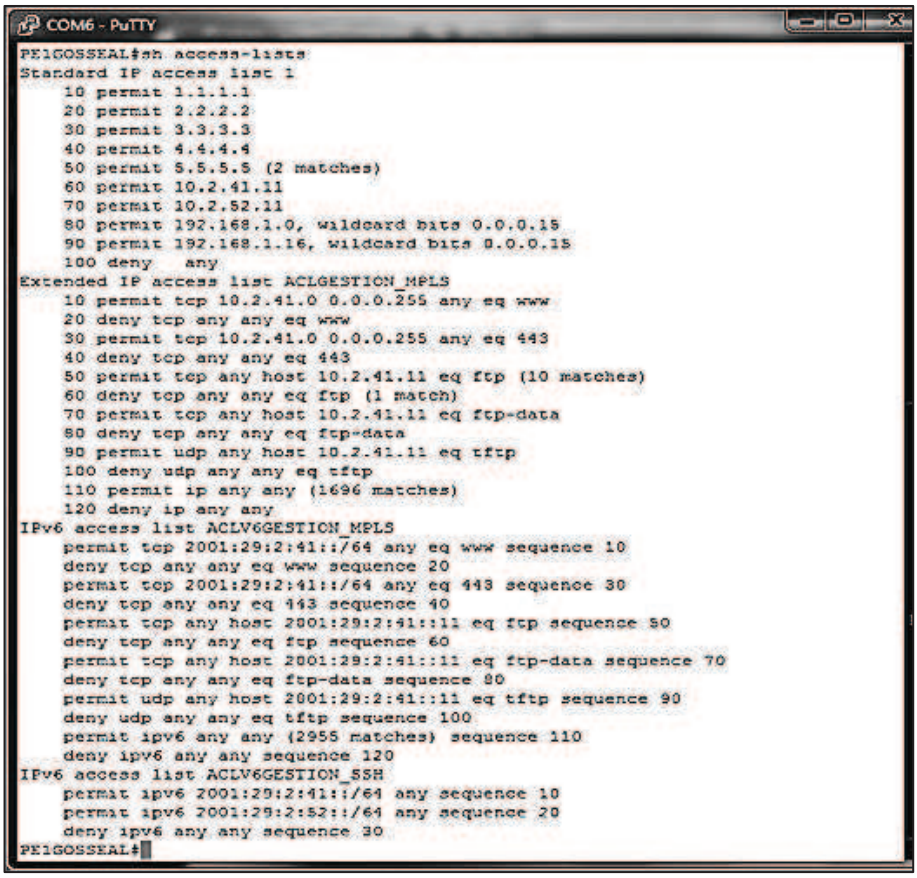


Figura 4.69 Verificación de la configuración de las ACL

4.3.8.3. Gestión de acceso remoto seguro

En la Figura 4.70 se indica el resultado del comando “show access-lists” para verificar las configuraciones de las ACL.

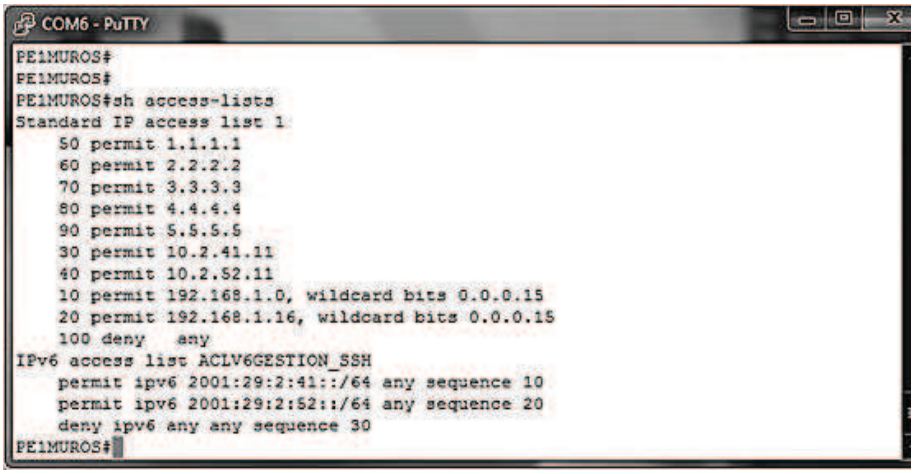


Figura 4.70 Verificación de las ACL configuradas

En la Figura 4.71 se indica el resultado del comando “show run | b login” para verificar las configuraciones de las líneas consola, auxiliar y VTY.

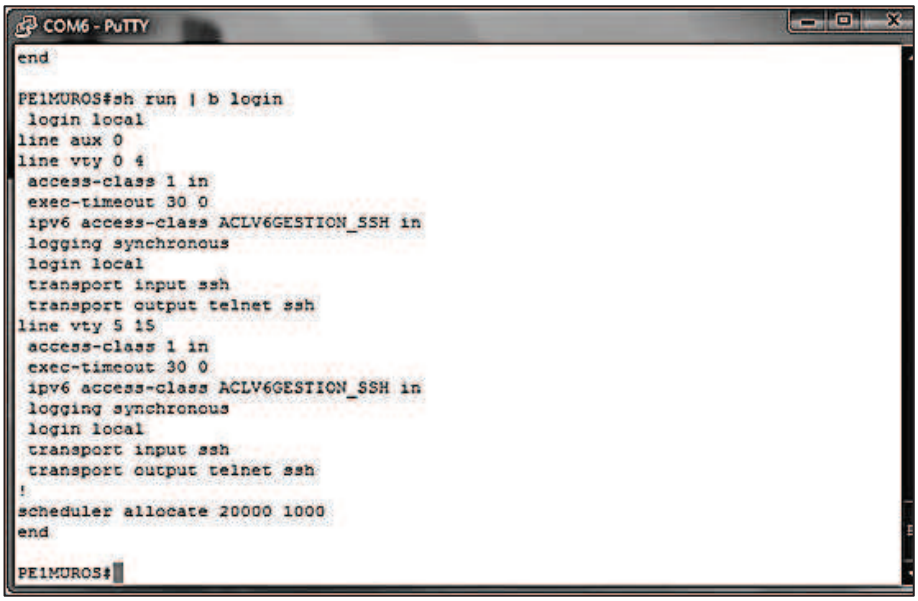


Figura 4.71 Verificación de las configuraciones de las líneas VTY

En la Figura 4.72 se indican las configuraciones de SSH en los switches de la red del prototipo.

Figura 4.72 Verificación de la gestión remota

REFERENCIAS BIBLIOGRÁFICAS
CAPÍTULO 4

LIBROS Y MANUALES

[1] VIVEK, Alwayn. “Advanced MPLS Design and Implementation”. Cisco-Press. Estados Unidos de América. Septiembre, 2001.

[2] ANÓNIMO. “Aspectos Básicos de Networking - CCNA 1”. Academia de red Cisco. Módulo uno. Cuarta edición. Capítulo 8. Madrid, España. 2007-2008.

[3] DE GHEIN, Luc CCIE. “MPLS Fundamentals”. Cisco Press. No. 1897. ISBN: 1-58705-197-4. Indianapolis, Estados Unidos de América. Noviembre, 2006.

[4] ALMEIDA ARCOS, Andrés. “Arquitectura de Redes MPLS”. Academia de Certificaciones Internacionales en Redes y Tecnologías de Información ACIERTE-EPN. Quito, Ecuador. Junio, 2011.

[5] ANÓNIMO, “Implementing Cisco Quality of Service”. Student Guide Cisco Systems, Inc. Versión 2.2 volúmenes 1 y 2. 2006.

[6] ALMEIDA ARCOS, Andrés. “BGP y Calidad de Servicio en Redes Convergentes”. Academia de Certificaciones Internacionales en Redes y Tecnologías de Información ACIERTE-EPN. Quito, Ecuador. Noviembre, 2011

[7] ANÓNIMO. “Conceptos y Protocolos de Enrutamiento - CCNA 2”. Academia de red Cisco. Módulo dos. Cuarta edición. Capítulos 4 y 5. Madrid, España. 2007-2008.

PROYECTOS DE TITULACIÓN

[8] NIETO PORRAS, Luisana Bertilda, “Diseño y Configuración de Calidad de Servicio en la Tecnología MPLS para un Proveedor de Servicios de CE1COLON_CLIENTE”. EPN. Mayo, 2010.

[9] MARCHÁN MERINO, Julia Soledad, YÁNEZ QUINTANA, Daniel Alfonso. "Estudio y Diseño para la Migración de una Red Gigabit Ethernet de datos de una Empresa Portadora de Servicios a la Tecnología MPLS (Multiprotocol Label Switching)". Abril, 2008.

[10] HIDALGO LLUMIQUINGA, Carlos Luis, LAGUAPILLO MUÑOZ, David Alejandro. "Diseño e Implementación de una Laboratorio que permita emular y probar servicios IP y MPLS de la red de Backbone CISCO de la Corporación de Telecomunicaciones CNT". Noviembre, 2011.

DIRECCIONES ELECTRÓNICAS

[11] ANÓNIMO. "IXIA 400T". IXIA Enabling a Converged World. March 1998-2012. http://www.ixiacom.com/products/display?skey=ch_400t

[12] ANÓNIMO. "MPLS Virtual Private Networks (VPNs)". Cisco IOS Software Releases 12.2 T. Cisco Systems.
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftvpn13.html

[13] ANÓNIMO. "MPLS Traffic Engineering". Cisco IOS Software Releases 12.2 S. Cisco Systems.
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/TE_1208S.html

[14] ANÓNIMO. "Configuring Quality of Service for MPLS Traffic". Cisco 10000 Series Router Calidad de Servicio: Guía de Configuración. Cisco Systems.
http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/qos/10qmpls.html

[15] ANÓNIMO. "MPLS Label Distribution Protocol" Cisco IOS Software Releases 12.2 T. Cisco Systems.
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ft_ldp7t.html

[16] ANÓNIMO. "Configuring IP Version 6". Cisco 10000 Series Router Calidad de Servicio: Guía de Configuración. Cisco Systems.

http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/broadband/ipv6.html

[17] ANÓNIMO. “Mls Qos (global configuration mode) Through Mpls Experimental”. Cisco IOS Software Releases 12.2 S. Cisco Systems. http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_m2.html

[18] ANÓNIMO. “MPLS Basic Traffic Enrineering Using OSPF Configuration Example”. Cisco IOS Software Releases 12.2 S. Cisco Systems. http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a0080093fd0.shtml

[19] ANÓNIMO. “6VPE: IPv6 over MPLS VPN”. Cisco IOS Software Releases 12.2 S. Cisco Systems. https://sites.google.com/site/amitsciscozone/home/important-tips/mpls-wiki/6vpe-ipv6-over-mpls-vpn

[20] ANÓNIMO. “Implementing IPv6 over MPLS”. Cisco IOS Software Releases 12.2 S. Cisco Systems. http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-over_mpls.html

[21] ANÓNIMO. “Passwords and Privileges Commands”. Cisco IOS Software Releases 12.2. Cisco Systems. http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/srfpass.html

[22] ANÓNIMO. “Network Based Application Recognition (NBAR)”. Cisco IOS Software. Cisco Systems, Inc. http://www.cisco.com/en/US/products/ps6616/products_ios_protocol_group_home.html

[23] ANÓNIMO. “Commands: queue-limit – random-detect precedence”. Cisco IOS Software Releases 12.2. Cisco Systems. http://www.cisco.com/en/US/docs/ios/12_2/qos/command/reference/qrfcmd7.html#wp1053418

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- MPLS es una tecnología que ofrece nuevas aplicaciones, flexibilidad, escalabilidad, rapidez en la conmutación y sobre todo bajo costo, es por ello que Telconet S.A. y muchos proveedores nacionales han adoptado esta tecnología con el fin de mejorar su infraestructura de red y cumplir con las exigencias de los clientes en lo referente a Calidad de Servicio.

- En el análisis de la situación actual de la red de Telconet S.A.-Quito, se pudo constatar que muchos de los dispositivos no tienen soporte a IPv6, es por ello que fue necesario actualizar el IOS y/o migrar el equipo a uno más robusto. Para los routers 7206VXR que disponían de la versión de IOS 12.2(33)SRD5, fue suficiente con la actualización de la versión de IOS a 15.0(1)M7; mas para los switches 3550, el enrutamiento IPv6 no fue soportado por el hardware del dispositivo, entonces se cotizaron dispositivos más robusto que tengan soporte a las plantillas de doble pila como los switches 3560.

- Se concluye que el crecimiento de los clientes nuevos de Telconet S.A.-Quito durante los tres primeros años de análisis (2007, 2008 y 2009) ha sido positivo, variando de 236 a 430 y 515 respectivamente. En el 2010 aunque se tienen nuevos clientes, la cantidad es menor que en el 2009 con 450 clientes. Mientras para el 2011, el crecimiento supera los años anteriores y se estabiliza con 534 clientes. Las razones de este incremento reducido en el año 2010 son dos: primero, el proveedor no estuvo ofertaron nuevos servicios durante este periodo; y segundo, no se disponía de tanta cobertura como en el 2011 cuando se empezó a migrar su infraestructura de red a fibra óptica y a

la tecnología MPLS en su *backbone.* Sin embargo en los próximos cinco años (2012-2017), no se espera un crecimiento exponencial de clientes debido a que el mercado de Quito prácticamente está copado, es por ello que la regresión logarítmica resultó como la tendencia más acertada para el análisis del número de clientes, reflejando el crecimiento significativo en los primeros años (2007-2009) y constante en los siguientes (2010-2017).

- Se concluye que el número de clientes no refleja el crecimiento de una empresa, debido a que se pueden tener pocos clientes que facturen grandes cantidades de dinero, o cientos de ellos con facturas pequeñas. Por lo cual además del número de clientes, se analizaron las ventas facturas del proveedor para tener valores más cercanos a la realidad, teniendo un crecimiento del 27,13% anual en las ventas facturadas de los servicios que se ofertan en la actualidad como Internet dedicado y Transmisión de datos; y los que se esperan ofertar como el *Data Center*.

- Se concluye que el mejor mecanismo para determinar los requerimientos del rediseño, es obteniendo las capacidades de tráfico reales que circulan por la red mediante las gráficas de tráfico obtenidas con la herramienta Cacti, a fin de no sobredimensionar los enlaces ni los equipos. La peor situación es cuando todos los clientes trabajen a su máxima capacidad contratada, pero no es recomendable diseñar en base a este análisis porque los costos de cada Mbps resultan mayores, al requerir enlaces y equipos más robustos. Por el contrario, en el primer caso ya se considera la peor situación de la red cuando se analizan los valores máximos y no los promedios de las gráficas, obteniendo mejores costos que van acorde al uso real de la infraestructura de red del proveedor.

- Las VPN son las ventajas más notables de MPLS, son escalables y no ameritan la creación de túneles o el cifrado de la información para brindar privacidad. Las VPN de capa 2 permiten brindar un mecanismo de transporte

transparente a la red del cliente, mientras las VPN de capa 3 mantienen tablas de enrutamiento diferentes de la tabla de enrutamiento global, permitiendo optimizar el envío de paquetes al disminuir los tiempos de procesamiento en las búsquedas.

- Se determina que se deben configurar solo las políticas de QoS necesarias en los dispositivos, de lo contrario el procesamiento de los mismos se verá seriamente afectado. En el prototipo se definieron las políticas de salida en los routers LSR, y dos políticas de entrada y salida para los routers LER.

- El generador IXIA 400T puede transmitir una gran cantidad de tráfico pero se limitará su capacidad por el medio físico establecido para conectar el IXIA a la red. En los enlaces de cobre utilizados para el prototipo, se tuvo como máxima capacidad de transmisión a 76,1Mbps.

- La Ingeniería de Tráfico es la aplicación de MPLS para la optimización del uso de los recursos ya que brinda un uso eficiente de las velocidades de transmisión; evita zonas sobre y sub-utilizadas; minimiza el retardo, el jitter y la pérdida de paquetes; y permite tener caminos alternos en caso de fallas en la red.

- El balanceo de carga con Ingeniería de Tráfico puede establecerse de manera simétrica o asimétrica dependiendo de la velocidad configurada en el túnel TE con el comando “tunnel mpls traffic-eng bandwidth 1204”. En los túneles simétricos las velocidades son iguales en los dos túneles; mientras en los asimétricos, un túnel transportará los paquetes a mayor velocidad que el otro.

- Se concluye que existen dos maneras de manipular los túneles TE, de forma dinámica y explícita. Los túneles dinámicos se establecen en base al IGP configurado; mientras en los túneles explícitos, el administrador de red debe

definir los saltos del trayecto del paquete. Cuando se protege una interfaz, la mejor forma de establecer un túnel TE es explícitamente porque queda a la flexibilidad de decisión del administrador e implica menor tiempo de conmutación al tener el camino preestablecido, ya que el IGP no necesita recalcular el trayecto del túnel de respaldo.

- Se concluye que en IPv6 no se pueden crear las ACL numeradas ni las extendidas. La configuración de las ACL en IPv6 se establecen como nombradas y extendidas, definiendo la dirección IP origen y destino en cada una de las entradas.

- Se concluye que las VLAN al estar definidas en la capa 2 del modelo ISO/OSI, transmiten tramas por lo que los paquetes IPv4 e IPv6, no serán diferenciados en la transmisión. Sin embargo, si se desea configurar la VLAN administrativa con una dirección IPv6, se debe habilitar el enrutamiento IPv6 en el switch mediante la plantilla de doble pila soportada a partir de la serie 3560.

5.2. RECOMENDACIONES

- Se recomienda utilizar protocolos estandarizados porque aunque hoy una empresa domine el mercado, no se garantiza que en los próximos años, esta siga siendo tan competente como en la actualidad. Un protocolo propietario no brinda la misma flexibilidad que un protocolo estandarizado, debido a que no tiene el respaldo de una institución como la IETF que garantice el avance continuo del mismo. La competencia será siempre un factor importante para estabilizar el mercado, es por ello que pueden surgir otras empresas con ideas innovadoras y desplazar a los protocolos propietarios actuales, pero un protocolo estandarizado siempre estará respaldado por las institución de estandarización.

- Cuando se va a rediseñar una red es importante analizar el tiempo para el cual, se dimensionan los enlaces y los dispositivos, debido a que las tecnologías de la información están en constante desarrollo. Considerando que los dispositivos de telecomunicaciones tiene una vida comercialmente útil de 3 años, es recomendable dimensionar las redes a 3 o 5 años como máximo.

- No se recomienda migrar toda la infraestructura de red de un ISP a IPv6 porque tanto en Ecuador como en el mundo, esta migración será progresiva en tiempo y costos. Los mecanismos de transición son la mejor opción para tener soporte a IPv6 al menor costo.

- En lo referente a Calidad de Servicio, es importante analizar el lugar donde se van a marcar los paquetes para ingresar a la red MPLS y recibir un tratamiento diferenciado. El lugar de selección debe ser completamente administrado por el personal del proveedor debido a que, si el cliente tiene conocimiento de redes, puede manipular el marcaje de los paquetes y provocar congestión en la red.

- Se recomienda rediseñar la red en base al modelo jerárquico de tres capas: núcleo, distribución y acceso ya que se definirán funciones específicas para cada una. De la misma manera, la administración y solución de los problemas de la red serán más óptimos al estar claramente diferenciados entre una capa y otra.

- Para el rediseño de los routers LER, no es tan recomendado ubicar un equipo redundante ya que se tendrá un incremento sustancial en los costos. Se aconseja en todo caso, colocar de dispositivos con doble memoria RSP y módulos de interfaces adicionales, a fin de brindar redundancia en el procesador y en las interfaces.

- Se recomienda utilizar mecanismo NBAR para diferenciar, clasificar y marcar las aplicaciones utilizadas por los clientes a fin de garantizar la Calidad de Servicio de extremo a extremo.

- Se recomienda definir no más de 3 o 4 clases de tráfico en una red MPLS debido a que la clasificación y asignación de políticas incrementará el procesamiento de los dispositivos. No se incluyen las clases de enrutamiento y por defecto ya que estas serán necesarias siempre en la definición de las políticas de QoS.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS Y MANUALES

[1] VIVEK, Alwayn. “Advanced MPLS Design and Implementation”. Cisco-Press. Estados Unidos de América. Septiembre, 2001.

[2] HIDALGO LASCANO, Pablo William. Folleto “Redes de Área Extendida”. Escuela Politécnica Nacional. Quito, Ecuador. Marzo, 2011.

[3] ALMEIDA ARCOS, Andrés. “Arquitectura de Redes MPLS”. Academia de Certificaciones Internacionales en Redes y Tecnologías de Información ACIERTE-EPN. Quito, Ecuador. Junio, 2011.

[4] TANENBAUM, Andrew S. “Redes de Computadoras”. Cuarta Edición. PRETICE HALL. Vrije Universiteit. México. 2003.

[5] STALLINGS, William. “Comunicaciones y Redes de Computadores”. Séptima Edición. PRETICE HALL. Madrid, España. 2004.

[6] HIDALGO LASCANO, Pablo William. Folleto “Redes TCP/IP”. Escuela Politécnica Nacional. Quito, Ecuador. Marzo, 2009.

[7] MILES, David. MAGLIONE, Roberta. TOWNSLEY, Mark. “IPv6 for PPP Broadband Access TR-187”. Broadband Forum Technical Report. Mayo, 2010.

[8] ANÓNIMO. “Acceso a la WAN - CCNA 4”. Academia de red Cisco. Módulo cuatro. Cuarta edición. Capítulos 4 y 7. Madrid, España. 2007-2008.

[9] ANÓNIMO. “Aspectos Básicos de Networking - CCNA 1”. Academia de red Cisco. Módulo uno. Cuarta edición. Capítulo 8. Madrid, España. 2007-2008.

[10] CICILEO, Guillermo. ROQUE, Gagliano. O’FLAHERTY, Christian. “IPv6 para Todos - Guía de uso y aplicación para diversos entornos”. Internet Society. Buenos Aires, Argentina. 2009.

[11] PALET, Jordi. “Introducción a IPv6”. Consulintel. Cancún, México. Mayo, 2011.

[12] ANÓNIMO. “Nivel de Servicio Garantizado”. Telconet S.A. sucursal Quito, Ecuador. Agosto, 2011.

[13] VIVES, Álvaro. “Despliegue de IPv6”. 6Deploy. Santa Cruz, Bolivia. Octubre, 2010.

[14] ROMERO TERNERO, MariCarmen. “Seguridad en Redes y Protocolos Asociados”. Ingeniería de Protocolos. España, 2010.

[15] ALMEIDA ARCOS, Andrés. “BGP y Calidad de Servicio en Redes Convergentes”. Academia de Certificaciones Internacionales en Redes y Tecnologías de Información ACIERTE-EPN. Quito, Ecuador. Noviembre, 2011.

[16] GONT, Fernando. “Seminario IPv6”. Cisco Seminars: IPv6 Migration. Buenos Aires, Argentina. Julio, 2011.

[17] VALDIVIA GÓMEZ, Javier Rafael Ms.C. PEÑA MOLINER, Carmen DrC. “MPLS y su Aplicación en Redes Privadas Virtuales (L2VPN Y L3VPN)”. LACCET - Information Technology Track. Paper No. 83. Cartagena de Indias, Colombia, 2005. W: http://laccei.org/LACCEI2005-Cartagena/Papers/IT083_MolinerPena.pdf

[18] DE GHEIN, Luc CCIE. “MPLS Fundamentals”. Cisco Press. No. 1897. ISBN: 1-58705-197-4. Indianapolis, Estados Unidos de América. Noviembre, 2006.

[19] ANÓNIMO. “Conceptos y Protocolos de Enrutamiento - CCNA 2”. Academia de red Cisco. Módulo dos. Cuarta edición. Capítulos 4 y 5. Madrid, España. 2007-2008.

[20] ANÓNIMO, “Implementing Cisco Quality of Service”. *Student Guide* Cisco *Systems*, Inc. Versión 2.2. Volúmenes 1 y 2. 2006.

[21] ANÓNIMO. “Portafolio 2011”. Departamento de Ventas de Telconet S.A.-Quito. Ecuador. 2011.

[22] ALVARADO, Alexandra. “Diagrama Capa 3”. ESP PROY 06 Versión Jul 11. Guayaquil, Ecuador. Julio, 2011.

[23] TIPÁN, Milton. “Diagrama de Red MPLS Quito-Telconet S.A.”. PROY 06 Ver 17-02-2012. Quito, Ecuador. Febrero, 2011.

[24] ANÓNIMO. “Conmutación y Conexión Inalámbrica de LAN – CCNA 3”. Academia de red Cisco. Módulo cuatro. Cuarta edición. Capítulo 1. Madrid, España. 2007-2008.

[25] JIMÉNEZ, María Soledad MSc. “Comunicación Digital.” Escuela Politécnica Nacional. Quito, Ecuador. Marzo, 2005.

[26] CERVANTES, Javier. “Manual para el tendido de la fibra óptica de Telconet S.A. – parte A”. Quito, Ecuador. Enero 2011.

[27] ANÓNIMO, “Portable Product Sheet – Switch Perf”. *Catalyst Switching Performance.* Cisco *Systems* Inc. 25 de agosto de 2005.

[28] ANÓNIMO, “Portable Product Sheet – Router Perf”. *Router Switching Performance in Packets Per Second (PPS).* Cisco *Systems* Inc. 15 de diciembre de 2006.

[29] ANÓNIMO. “Estudio de Mercado de Telconet S.A.”. Departamento de Proyectos de Telconet S.A. Guayaquil, Ecuador. Diciembre, 2010.

[30] ANÓNIMO, “Salidas Internacionales de Telconet Dic-2011”, Departamento de Networking de Telconet S.A. Quito, Ecuador. Diciembre, 2011.

[31] ANÓNIMO. “Ventas Facturadas Telconet S.A. Quito 2007-2011”, Departamento de Facturación de Telconet S.A. Quito, Ecuador. Mayo, 2012.

[32] ANÓNIMO, “Manual de configuración de equipos Streambox”. Departamento IAC de Telconet S.A. Quito, Ecuador. Enero, 2011.

[33] ANÓNIMO. “Documento de Resultados de Búsquedas en SIT - Clientes Activos de Quito”. Departamento IAC de Telconet S.A. Quito, Ecuador. 31 de marzo de 2012.

[34] ANÓNIMO. “Registros de la migración de MPLS de Telconet S.A.- Documento de Resultados de Búsquedas en SIT”. Departamento IAC de Telconet S.A. Quito, Ecuador. 23 de mayo de 2012.

[35] PARNELL, Teré. “Guía de redes de alta velocidad”. Mc Graw Hill. 2da edición. Madrid, España. 2001.

[36] ANÓNIMO. “Registros de las emergencias del Cacti - Documento de Resultados de Búsquedas en SIT”. Departamento NOC de Telconet S.A. Quito, Ecuador. 2010-2012.

PROYECTOS DE TITULACIÓN

[37] NIETO PORRAS, Luisana Bertilda. “Diseño y Configuración de Calidad de Servicio en la Tecnología MPLS para un Proveedor de Servicios de Internet”. EPN. Mayo, 2010.

[38] MARCHÁN MERINO, Julia Soledad. YÁNEZ QUINTANA, Daniel Alfonso. “Estudio y Diseño para la Migración de una Red Gigabit Ethernet de datos de una Empresa Portadora de Servicios a la Tecnología MPLS (Multiprotocol Label Switching)”. Abril, 2008.

[39] HINOJOSA LÓPEZ, Mayra Alexandra. HERRERA MERCHÁN, Fabricio Fernando. “Diseño de una Red MPLS utilizando el Protocolo IPv6 para Proveedores de Servicios de Telecomunicaciones”. Julio, 2009.

[40] HIDALGO LLUMIQUINGA, Carlos Luis, LAGUAPILLO MUÑOZ, David Alejandro. “Diseño e Implementación de una Laboratorio que permita emular y probar servicios IP y MPLS de la red de Backbone CISCO de la Corporación de Telecomunicaciones CNT”. Noviembre, 2011.

DIRECCIONES ELECTRÓNICAS

[41] INTERNET ENGINEERING TASK FORCE. “Multiprotocol Label Switching Architecture”. Enero, 2001.
http://www.ietf.org/rfc/rfc3031.txt

[42] GARCÍA CAPEL, Daniel. “Comandos CISCO CCNA Exploration”. Cisco Systems, Inc. 13 de abril de 2011.
http://dani.albatalia.com/code/cisco/comandos_cisco_ccna_exploration.pdf

[43] VYNCKE, Eric. “IPv6 Security Best Practices”. Distinguished System Engineer. Estados Unidos de América. 2007.
http://www.cisco.com/web/SG/learning/ipv6_seminar/files/02Eric_Vyncke_Security_Best_Practices.pdf

[44] ANÓNIMO. “TACACS.net TH”. 2010. Web: http://www.tacacs.net/

[45] ANÓNIMO. “Internet Protocol Version Address Space”. Internet Assigned Numbers Authority.
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

[46] ANÓNIMO. “Implementing Traffic Filters and Firewalls for IPv6 Security”. Cisco Systems, Inc. Estados Unidos de América. 2010.
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-sec_trfltr_fw.html

[47] ANÓNIMO. “IPv6 Filtering”. ISP/IXP Workshops. Cisco Systems, Inc. Estados Unidos de América. 2006. http://support.udsm.ac.tz/ipv6/c6-1up.pdf

[48] CLAUBERG, Axel. “Deploying IPv6 Networks Cisco”. Session RST-231. Cisco IOS Software. 2002.
http://www.ipv6-es.com/02/docs/patrick_grossetete_1.pdf

[49] VIVES, Álvaro. “Despliegue de IPv6”. WALC2011. Guayaquil, Ecuador. 10-14 de octubre de 2011.

http://www.6deploy.eu/workshops2/20111010_guayaquil_ecuador/DIA5-1-2-Consulintel _Curso-IPv6_WALC2011.pdf

[50] LIAKOPOULOS, Athanassios. “IPv6 over IPv4/MPLS Networks: The 6PE Approach”. III Global IPv6 Summit. Greek Research & Technology Network (GRNET). Moscow, Rusia. 25 de noviembre de 2004. http://www.free.net/NTL/IP6/presentation/ALiakopoulos%20-%206PE%20-%203rd%20Global%20IPv6%20Summit.pdf

[51] ANÓNIMO. “Cisco IOS IPv6 Provider Edge Router (6PE) over MPLS”. Cisco IOS Software Releases 12.2 Mainline. http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_data_sheet09186a008052edd3.html

[52] GROSSETET, Patrick. “IPv6 over MPLS: Cisco IPv6 Provider, Edge Router (6PE), Cisco IPv6 VPN, Provider Edge y Router (6VPE)”. Cisco Systems, Inc. Estados Unidos de América. 2006. http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/prod_presentation0900aecd80311df4.pdf

[53] CONVERY, Sean. MILLER, Darrin. “IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)”. Cisco Systems, Inc. Estados Unidos de América. 2004. http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf

[54] ANÓNIMO. “IPv6 Security”. Cisco Networkers. Estados Unidos de América. 2006. http://www.cu.ipv6tf.org/pdf/cdccont_0900aecd8057a244.pdf

[55] ANÓNIMO. “Configuring IPv6 ACL”. Chapter 37. Cisco IOS Software Releases 12.2 Mainline. Estados Unidos de América. 2010. http://www.cisco.com/en/US/docs/switches/metro/me3400/software/release/12.2_50_se/configuration/guide/swv6acl.pdf

[56] STRETCH, Jeremy. “IPv6 Access Lists on IOS”, PacketLife. Virginia, Estados Unidos de América. 2010. http://packetlife.net/blog/2010/jun/30/ipv6-access-lists-acl-ios/

[57] ANÓNIMO. “Cisco Express Forwarding (CEF) Introduction”. Cisco IOS Software Releases 12.2 Mainline. http://www.cisco.com/en/US/tech/tk827/tk831/tk102/tsd_technology_support_sub-protocol_home.html

[58] ANÓNIMO. “MPLS Label Distribution Protocol” Cisco IOS Software Releases 12.2 T. Cisco Systems. http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ft_ldp7t.html

[59] ANÓNIMO. “LACNIC XVII - Quito, Ecuador”. Registro de Internet de América Latina y el Caribe. 29 de julio de 2011. http://lacnic.net/sp/anuncios/lacnicxvii.html

[60] REKHTER, Y. MOSKOWITZ, B. “Asignación de direcciones para Internet Privadas - RFC 1918”. Febrero, 1996. http://www.rfc-es.org/rfc/rfc1918-es.txt

[61] ANÓNIMO. “FREERADIUS The world's most popular RADIUS Server”. Network RADIUS Inc. 2012. Web: http://freeradius.org/

[62] LAKSHMI. “Secure Neighbor Discovery (SEND)”. IPv6.com Tech Spotlight. http://www.ipv6.com/articles/research/Secure-Neighbor-Discovery.htm

[63] PATTERSON, Michael. “What is VRF: Virtual Routing and Forwarding”. 10 de diciembre de 2009. http://www.plixer.com/blog/netflow/what-is-vrf-virtual-routing-and-forwarding/

[64] ANÓNIMO. “Virtual Private LAN Services (VPLS)”. Cisco Systems Inc. http://www.cisco.com/en/US/products/ps6648/products_ios_protocol_option_home.html

[65] ANÓNIMO. Internet Assigned Numbers Authority (IANA). Web: http://www.iana.org/

[66] ANÓNIMO. “Cisco Any Transport over MPLS”. Cisco Systems, Inc. Estados Unidos de América. 2002. http://www.cisco.com/warp/public/cc/so/neso/vpn/unVPNt/atomf_wp.pdf

[67] ANÓNIMO. “Protocol Registries”. Internet Assigned Numbers Authority (IANA). http://www.iana.org/protocols

[68] ANÓNIMO. “SSH Support Over IPv6”. Cisco Systems, Inc., 23 de julio de 2012. http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_nman/configuration/15-2mt/ip6-ssh.pdf

[69] ANÓNIMO. “Configuring IPv6 ACL”. Catalyst 3750 Software Configuration Guide, Release 12.2(55)SE. http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_55_se/configuration/guide/swv6acl.html

[70] ANÓNIMO. “Quality of Service on Cisco Catalyst 6500”. Cisco Catalyst 6500 Series Switches. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_white_paper0900aecd803e5269.html

[71] ANÓNIMO. “StreamBox Rackmount Encoders/Decoders”. 2012. http://www.streambox.com/products/rackmount-encoder-decoder.html

[72] ANÓNIMO. “Telconet S.A. la fibra del Ecuador”. Telconet S.A. Ecuador. 2011. http://www.telconet.net/?section=home

[73] ANÓNIMO. “Fundamentals of DWDM Technology”. Cisco Systems. http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm_ovr.htm

[74] ANÓNIMO. “Cisco 7609 Chassis”. Cisco Systems, Inc. 1992-2006. http://www.cisco.com/en/US/prod/collateral/routers/ps368/ps367/product_data_sheet09186a0080169ead_ps368_Products_Data_Sheet.html

[75] ANÓNIMO. “Cisco Catalyst 3750 Series Switches”. Cisco Systems, Inc. 1992-2008.
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/product_data_sheet0900aecd80371991.pdf

[76] ANÓNIMO. “Cisco Catalyst 3550 Series Intelligent Ethernet Switches”. Cisco Systems, Inc. 1992-2008.
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps646/product_data_sheet09186a00800913d7.html

[77] ANÓNIMO. “APC Smart-UPS RT 10000VA 208V”. ErickProtect. Ecuador.
http://www.upsecuador.com/equipos-proteccion-electrica-venta-importador-distribuidor-quito-ecuador.php?recordID=123

[78] PALET, Jordi. “Taller de IPv6- Despliegue de IPv6 en Ecuador”. Consulintel Quito- Ecuador, 2 de diciembre de 2011.
http://www.6deploy.eu/workshops2/20111202_quito_ecuador/evento_IPv6_SENATEL_v2.pptx.pdf

[79] ANÓNIMO. “Regresión No Lineal”. SEQC.
http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CFMQFjAA&url=http%3A%2F%2Fwww.seqc.es%2Fdl.asp%3F175.145.205.255.15.30.27.21.118.133.24.113.255.173.47.5.166.145.65.153.249.7.59.180.219.25.233.119.115.80.195.223.111.197.213.82.70.131.125.124.232.86.165.216.192.188&ei=-xS4T_KtDYGo8QTGrvycCg&usg=AFQjCNEgnspoWKlfHtUgBlmtjArYu1q5FA&sig2=kPpI3d_iNJQlNUL8JZeA8A

[80] ANÓNIMO. “CEDIA ¿Qué es Cedia?”.
http://www.cedia.ec/index.php?option=com_content&view=article&id=1&Itemid=8

[81] MITTAL, Kunal. “Internet Traffic Growth-Analysis of Trends and Predictions”. Paper del Departamento de Administración de la Universidad de Nebraska. Estados Unidos de América. Septiembre, 2011.

http://www.kunalmittal.com/includes/Papers/PredictingInternetTrafficGrowth.pdf

[82] ANÓNIMO. “Cisco Catalyst 6500 and 6500-E Series Datasheet”. Cisco Systems, Inc. 2009.
http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a00800ff916_ps708_Products_Data_Sheet.html

[83] ANÓNIMO. “Cisco 7200 VXR Series Routers Overview”. Cisco Systems, Inc. 1992-2008.
http://www.cisco.com/en/US/prod/collateral/routers/ps341/data_sheet_c78_339749.pdf

[82] ANÓNIMO. “MPLS Traffic Engineering”. Cisco IOS Software Releases 12.2S. Cisco Systems.
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/TE_1208S.html

[84] ANÓNIMO. “Commands: queue-limit – random-detect precedence”. Cisco IOS Software Releases 12.2. Cisco Systems.
http://www.cisco.com/en/US/docs/ios/12_2/qos/command/reference/qrfcmd7.html#wp1053418

[85] ANÓNIMO. “Configuring Quality of Service for MPLS Traffic”. Cisco 10000 Series Router Calidad de Servicio: Guía de Configuración. Cisco Systems.
http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/qos/10qmpls.html

[86] ANÓNIMO. “Configuring IP Version 6”. Cisco 10000 Series Router Calidad de Servicio: Guía de Configuración. Cisco Systems.
http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/broadband/ipv6.html

[87] ANÓNIMO. “Cisco Catalyst 6500 and 6500-E Series Datasheet”. Cisco Systems, Inc. 2009.
http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a00800ff916_ps708_Products_Data_Sheet.html

[88] ANÓNIMO. “Cisco 7609 Chassis”. Cisco Systems, Inc. 1992-2006. http://www.cisco.com/en/US/prod/collateral/routers/ps368/ps367/product_data_sheet09186a0080169ead_ps368_Products_Data_Sheet.html

[89] ANÓNIMO. “Cisco IOS Router IPv6”. IPv6INT.NET. Enero, 2012. http://ipv6int.net/systems/cisco_ios_router-ipv6.html

[90] DELFINO, Adrián. RIVERO, Sebastián. SAN MARTÍN, Marcelo. BELZARENA, Pablo. “Ingeniería de Tráfico en Redes MPLS”. Instituto de Ingeniería Eléctrica, Facultad de Ingeniería de la República. Agosto, 2005. http://iie.fing.edu.uy/investigacion/grupos/artes/fce/nette/Ingenieria_de_Trafico_en_Redes_MPLS.pdf

[91] CLAUBERG, Axel. “Deploying IPv6 Networks Cisco”, Session RST-231. Cisco IOS Software. 2002. http://www.ipv6-es.com/02/docs/patrick_grossetete_1.pdf

[92] LIAKOPOULOS, Athanassios. “IPv6 over IPv4/MPLS Networks: The 6PE Approach”. III Global IPv6 Summit. Greek Research & Technology Network (GRNET). Moscow, Rusia. 25 de noviembre de 2004. http://www.free.net/NTL/IP6/presentation/ALiakopoulos%20-%206PE%20-%203rd%20Global%20IPv6%20Summit.pdf

[93] ANÓNIMO. “Políticas para la Distribución y Asignación de Direcciones IPv6”. Manual de Políticas de LACNIC. Capítulo 4 v1.9 – 23/05/2012. http://lacnic.net/sp/politicas/manual5.html

[94] ANÓNIMO. “IAB/IESG Recommendations on IPv6 Address Allocations to Sites”. Network Working Group. RFC 3177. Septiembre, 2001. http://tools.ietf.org/html/rfc3177

[95] NARTEN, T. HUSTON, G. ROBERTS, L. “IPv6 Address Assignment to End Sites”. Internet Engineering Task Force (IETF). RFC 6177. Marzo, 2011. http://tools.ietf.org/html/rfc6177

[96] ANÓNIMO. “Cisco Catalyst 4900M Series”. Cisco Systems, Inc. 1992–2008. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6021/ps9310/Prod_Bulletin_447737_Cat_4900M-Ex.html

[97] ANÓNIMO. “Cisco Catalyst 3560 v2 Series Switches”. Cisco Systems, Inc. 1992–2008. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/data_sheet_c78-530976.html

[98] ANÓNIMO. “Release Notes for MPLS Cisco IOS Release 11.1(28a)CT”. Cisco Systems, Inc. 25 de febrero, 2002. http://www.cisco.com/en/US/docs/ios/11_1/release/notes/rn111ct.pdf

[99] ANÓNIMO. “Data Center and Virtualization”. Cisco Systems, Inc. 2012. http://www.cisco.com/en/US/netsol/ns340/ns394/ns224/index.html

[100] ANÓNIMO. “The HP 6600 Router Series feature an innovative multi-core and distributed architecture”. *Hewlett-Packard*. 2012. http://h17007.www1.hp.com/us/en/products/routers/HP_6600_Router_Series/index.aspx

[101] ANÓNIMO. “NE40E Universal Service Router”. Huawei *Technologies* Co. Ltd. 2012. http://www.huawei.com/ucmf/groups/public/documents/attachments/hw_132368.pdf

[102] ANÓNIMO. “The HP 5500 EI Switch Series”. *Hewlett-Packard*. 2012. http://h17007.www1.hp.com/us/en/products/switches/HP_5500_EI_Switch_Series/index.aspx?jumpid=reg_r1002_usen_c-001_title_r0001#JD375A

[103] ANÓNIMO. “The HP 5820 Switch Series are advanced flex-chassis switches”. *Hewlett-Packard*. 2012. http://h17007.www1.hp.com/us/en/products/switches/HP_5820_Switch_Series/index.aspx

[104] ANÓNIMO. “S5300 Switches Product Brochure”. Huawei *Technologies* Co. Ltd. 2012. http://www.huawei.com/ucmf/groups/public/documents/attachments/hw_093970.pdf

[105] ANÓNIMO. “MPLS Virtual Private Networks (VPN)”. Cisco IOS Software Releases 12.2 T. Cisco Systems. http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftvpn13.html

[106] ANÓNIMO. “IXIA 400T”. IXIA Enabling a Converged World. March 1998-2012. http://www.ixiacom.com/products/display?skey=ch_400t

[107] ANÓNIMO. “Mls Qos (global configuration mode) Through Mpls Experimental”. Cisco IOS Software Releases 12.2 S. Cisco Systems. http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_m2.html

[108] ANÓNIMO. “MPLS Basic Traffic Enrineering Using OSPF Configuration Example”. Cisco IOS Software Releases 12.2 S. Cisco Systems. http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a0080093fd0.shtml

[109] ANÓNIMO. “6VPE: IPv6 over MPLS VPN”. Cisco IOS Software Releases 12.2 S. Cisco Systems. https://sites.google.com/site/amitsciscozone/home/important-tips/mpls-wiki/6vpe-ipv6-over-mpls-vpn

[110] ANÓNIMO. “Passwords and Privileges Commands”. Cisco IOS Software Releases 12.2. Cisco Systems. http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/srfpass.html

[111] ANÓNIMO. “Network Based Application Recognition (NBAR)”. Cisco IOS Software. Cisco Systems, Inc. http://www.cisco.com/en/US/products/ps6616/products_ios_protocol_group_home.html

ANEXOS

Los anexos se incluyen en el CD que acompaña este documento

ANEXO A

DISPOSITIVOS DE LA RED DE TELCONET S.A.-QUITO

ANEXO B

CIRCULAR DE LA SENATEL PARA LA PRESTACIÓN DE SERVICIOS DE VALOR AGREGADO DE INTERNET

ANEXO C

GRÁFICAS DE USO DEL CPU DE LOS EQUIPOS DEL *BACKBONE* DE LA CIUDAD DE QUITO

ANEXO D.1

COTIZACIONES CISCO SYSTEMS, Inc.

ANEXO D.2

COTIZACIONES HEWLETT-PACKARD

ANEXO D.3

COTIZACIONES HUAWEI TECHNOLOGIES CO. LTD.

ANEXO E

DATA SHEETS DE LOS EQUPOS UTILIZADOS EN EL REDISEÑO DE LA RED DE TELCONET S.A-QUITO

ANEXO F

CARACTERÍSTICAS TÉCNICAS DE LOS DISPOSITIVOS UTILIZADOS EN EL PROTOTIPO

ANEXO G

CONFIGURACIONES DEL PROTOTIPO DE LA RED MPLS DE TELCONET S.A.-QUITO

ANEXO H

TUTORIAL DEL GENERADOR DE TRÁFICO IXIA 400T

ANEXO I

PRUEBAS DE SEGURIDAD EN IPv6