UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

Trabajo de fin de carrera titulado:

DISEÑO DE UNA RED MULTISERVICIO MEDIANTE UN MECANISMO DE TRANSPORTE DE DATOS MPLS (MULTIPROTOCOL LABEL SWITCHING) PARA LA EMPRESA TRANSELECTRIC S.A.

Realizado por:

DANIEL LEONARDO AMOROSO ABAD

Como requisito para la obtención del título de:
INGENIERO EN SISTEMAS DE TELECOMUNICACIONES

QUITO, JULIO DE 2010

DECLARACIÓN JURAMENTADA

Yo Daniel Leonardo Amoroso Abad, 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 UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

……

Daniel Leonardo Amoroso Abad.

AGRADECIMIENTOS

En estas pocas palabras quiero expresar mis más sinceros agradecimientos a todas las personas que con su ayuda y aliento formaron parte importante para el desarrollo de este proyecto principalmente:

A mis padres Leonardo y Carlota, a mis hermanos Santiago y Ángela, por su incesante aliento y apoyo, durante toda mi vida estudiantil.

Al Ingeniero Wilmer López por su excelente dirección durante el desarrollo de este proyecto, su gran ayuda y consejos en el desarrollo del mismo.

A la Ingeniera Anita Zurita, que fue un pilar fundamental para mis inquietudes, por toda la ayuda brindada no solo durante la elaboración de este proyecto sino también en los años de prácticas profesionales.

Existen muchos nombres más, que por falta de espacio no los puedo enumerar, de eso no hay duda, por esto agradezco a todas las personas que me ayudaron, apoyaron y alentaron a lo largo de este proyecto, amigos, compañeros, profesores, familia, principalmente a Gabriela Franco, Gracias por estar ahí .

RESUMEN

El presente proyecto desarrolla el diseño de una red multiservicios para a la red de datos de TRANSELECTRIC S.A, con el fin de asegurar y mejorar el funcionamiento de esta red.

La tecnología MPLS brinda a Transelectric S.A la posibilidad de unificar múltiples plataformas y mantener requerimientos de diversos clientes para prestación de multiservicios, ya que utiliza las características de capa red con la rapidez de la conmutación de la capa de enlace.

Para poder desarrollar el presente diseño, fue necesario estudiar la red de la empresa Transelectric S.A, a partir de la información proporcionada por dicha empresa, conociendo su estructura, funcionamiento, ventajas y desventajas, para realizar la migración a la tecnología MPLS, de la manera más conveniente.

MPLS se presenta como una alternativa de solución óptima, para el adecuado funcionamiento de las redes de telecomunicaciones, ya que separa el envío de datos, de los procedimientos de enrutamiento estándar IP, produciendo beneficios de rendimiento y flexibilidad.

Los equipos seleccionados para la implementación de la red MPLS, que mejor se acoplaron a los son los requerimientos planteados, son de la marca comercial CISCO, que es el líder en el desarrollo de hardware, especializado en redes de internetworking.

Uno de los resultados considerables que se obtuvo, luego de haber realizado el presente trabajo, es que varios de los equipos con los que cuenta la red actual se conservarán para formar parte de capa Acceso, donde no se requiere el manejo de MPLS, optimizando de esta manera los recursos de la red.

ÍNDICE

CAPÍTULO I 16

DISEÑO CONCEPTUAL DE LA INVESTIGACIÓN 16

1.1 DETERMINACIÓN DEL PROBLEMA 16

1.2 DEFINICIÓN DEL TEMA 17

1.3 JUSTIFICACIÓN E IMPORTANCIA 17

1.4 OBJETIVOS 18

1.4.1 Objetivo General 18

1.4.2 Objetivos específicos 19

1.5 HIPÓTESIS 19

1.6 DELIMITACIÓN DEL TEMA 20

1.7 MARCO TEÓRICO 20

1.7.1 Antecedentes de MPLS 20

1.7.2 Capa de red 21

1.7.3 Protocolos de capa 3 22

1.7.3.1 Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) 22

1.7.3.2 Systems Network Architecture (SNA) 26

1.7.3.4 ATM (Asynchronous Transfer Mode). 30

1.7.3.5 Modelo IP/ATM 35

1.7.3.6 Conmutación IP 38

CAPÍTULO II 40

CONCEPTOS Y ELEMENTOS BÁSICOS DE UNA RED MPLS 40

2.1 INTRODUCCIÓN 40

2.2 RESEÑA HISTÓRICA 41

2.2.1 IP / ATM 42

2.2.2 Cell Switching Router (CSR) de Toshiba 45

2.2.3 Conmutación IP (IP SWITCHING) De Ipsilon 45

2.2.4 Conmutación de etiquetas de CISCO (TAG SWITCHING) 46

2.2.5 ARIS (Agregate Route-based Ip Switching) de IBM 47
2.3 CARACTERÍSTICAS BÁSICAS MPLS 48
2.3.1 Flexibilidad 49
2.3.2 Escalabilidad 50
2.3.3 Accesibilidad 50
2.3.4 Eficiencia 50
2.3.5 Calidad de servicio (QoS) y Clases de servicio (CoS) 51
2.3.6 Administración 52
2.3.7 Monitoreo y SLA's 52
2.3.8 Fácil Migración 52
2.3.9 Seguridad 53
2.3.10 Bajo Costo 53
2.4 FUNCIONAMIENTO MPLS 54
2.5 ARQUITECTURA DE UNA RED MPLS 56
2.5.1 LSR (Label Switching Router) 56
2.5.2 LSR de contorno 57
2.5.3 LSR-ATM 58
2.5.4 LER (Label Switching Router) 60
2.5.5 FEC (Forwarding Equivalence Class) 60
2.5.6 LSP (Label Switched Path): 61
2.5.7 LDP (Label Distribution Protocol): 61
2.6 ESTABLECIMIENTO DE UN LSP 62
2.7 JERARQUÍA MPLS 65
2.7.1 Etiquetas MPLS 66
2.8 APLICACIÓN MPLS 67
2.9 INGENIERÍA DE TRÁFICO 68
2.10 REDES PRIVADAS VIRTUALES 70
CAPITULO III 74
RED MULTISERVICIO (RED CONVERGENTE) 74
3.1 EVOLUCIÓN A REDES NGN 74
3.1.1 Factores para el cambio 76
3.2 DESCRIPCIÓN RED MULTISERVICIOS 77

3.3 CARACTERÍSTICAS PRINCIPALES DE LAS REDES MULTISERVICIOS. 81
3.4 EJEMPLO DE CONVERGENCIA BASADA EN IP 83
3.5 ELEMENTOS Y PROTOCOLOS EN UNA RED DE CONVERGENCIA. 85
3.5.1 Softswitch 85
3.5.1.1 Características del Softswitch 86
3.5.1.2 Arquitectura del Softswitch 87
3.5.1.3 Elementos de un Softswitch 87
3.5.1.4 Media Gateway (Pasarela de medios) 89
3.5.1.5 Media Server (Servidor de Medios) 90
3.5.1.6 Feature Server (Servidor de Capacidades) 91
3.5.1.7 El Access Media Gateway (AMG) 92
3.6 PROTOCOLOS UTILIZADOS EN NGN 94
3.6.1 PROTOCOLO SIP 94
3.6.1.1 Características de SIP 95
3.6.1.2 Llamadas y Transacciones SIP 96
3.6.1.3 Términos y definiciones SIP 98
3.6.2 Protocolo H.323 100
3.6.2.1 Componentes principales 100
3.6.2.2 Pila de protocolos H.3.23 103
3.6.2.3 Señalización 105
3.6.3 MEGACO/H.248 107
3.6.3.1 Componentes y funcionamiento de una llamada con H.248 107
3.6.4 Protocolo IP 110
3.6.4.1 Características IP 112
3.7 VENTAJAS DE NGN SOBRE LAS REDES IP TRADICIONALES. 114
3.8 BENEFICIOS DE UNA NGN 117
CAPÍTULO IV 120
TRANSELECTRIC S.A. 120
4.1 MISIÓN, VISIÓN, VALORES Corporativos. 120
4.2 RESEÑA HISTÓRICA Y CONSTITUCIÓN 121
4.3 PORTAFOLIO DE TELECOMUNICACIONES 122
4.4 SERVICIOS 124
4.5 TELECOMUNICACIONES EN TRANSELECTRIC 127

4.6 DESCRIPCIÓN DE LA RED DE TRANSELECTRIC S.A 131
4.6.1 BACKBONE 131
4.6.2 Infraestructura del backbone 133
4.7 SERVICIOS 135
4.7.1.3 Servicios al Mercado Eléctrico Mayorista 138
CAPÍTULO V 140
DISEÑO DE LA RED 140
5.1 DESCRIPCIÓN ACTUAL DE LA RED. 140
5.1.1 SDH 140
5.1.2 Módulo de transporte síncrono 141
5.1.2.1 Elementos de red de un sistema de transmisión síncrona 144
5.2 SUBESTACIONES DE TRANSELECTRIC 146
5.3 ESTRUCTURA DEL SISTEMA NACIONAL DE TRANSMISIÓN 148
5.4 ESTRUCTURA DE LA RED 148
5.5 CAPACIDADES 149
5.5.1 Tráfico Internacional 149
5.5.2 Tráfico Interno (Nacional) 150
5.6 EQUIPOS DE LA RED DE TRANSPORTE ÓPTICO 153
5.6.1 Core 153
5.6.2 Metro Access 153
5.6.2.1 Descripción de los equipos del Core 154
5.6.2.2 Descripción de los equipos del metro Access 157
5.6.2.3 Equipos de sincronización para la red de transporte 159
5.7 TOPOLOGÍA ACTUAL 162
5.7.1 Características principales 165
5.7.1.1 CISCO 1605 165
5.7.1.2 CISCO 1601 166
5.7.1.3 CISCO 1841 167
5.7.1.4 CISCO 1721 168
5.7.1.5 CISCO 2801 169
5.7.1.6 CISCO 2621 M 170
5.8 DISEÑOS DE LA RED 171
5.8.1 Servicios a prestarse 171

5.8.2 Área de cobertura 172
5.8.3 Equipos a utilizarse en core MPLS 173
5.8.4 Cambios en equipos activos TRANSELECTRIC S.A 175
Tabla 5.11 Cambios en Equipos Activos 176
5.8.5 Configuración de Equipos. 176
5.8.5.1 Configuración de una interfaz Loopback 176
5.8.5.2 Configuración de una subinterfaz 177
5.8.5.3 Configuración básica de OSPF: 177
5.8.5.4 Verificación del estado de OSPF 178
5.8.5.5 Configuración Básica de BGP 178
5.8.5.6 Configurar el proceso de routing BGP 179
5.8.5.7 Verificación del estado de BGP 180
5.8.5.8 Configuración básica de MPLS 180
5.8.5.9 Verificación del funcionamiento de MPLS en la red 181
5.8.5.10 Configuración de VPNs sobre MPLS 182
5.8.5.11 Configuración de equipos con funcionalidad PE 182
5.8.5.12 Verificación del funcionamiento de la VPN-MPLS 186
5.8.6 Medición del tráfico 187
5.9 MEJORAS CON LA IMPLEMENTACIÓN DE MPLS 187
CONCLUSIONES Y RECOMENDACIONES. 190
BIBLIOGRAFÍA 192
ANEXOS 196
6.1 ANEXO 1 196
Catálogos equipos 196
6.1.1 Cisco 2801 Integrated Services Router 196
6.1.2 Cisco 1841 Security Bundle 200
6.2 ANEXO 2 204
Diseño de la red mpls 204
6.3 ANEXO 3 206
Análisis de tráfico entre los elementos activos de la red 206

ÍNDICE DE FIGURAS

CAPÍTULO I 16

DISEÑO CONCEPTUAL DE LA INVESTIGACIÓN 16

Figura 1.1 Diagrama de Celdas ATM (UNI , NNI) 33

Figura 1.2: Topología Física ATM 36

Figura 1.3: Topología Lógica 37

Figura 1.4 Separación entre las funciones de control y envío 39

CAPÍTULO II 40

CONCEPTOS Y ELEMENTOS BÁSICOS DE UNA RED MPLS 40

Figura 2.1 Arquitectura IP / ATM 43

Figura 2.2 Routing Over Large Clouds 44

Figura 2.3 Cabecera MPLS 56

Figura 2.4 Tipos de LSR en el dominio MPLS 59

Figura 2.5 Arquitectura de una Red MPLS 61

Figura 2.6 Etiquetas MPLS 66

Figura 2.6 Ingeniería de Tráfico. 68

CAPITULO III 74

RED MULTISERVICIO (RED CONVERGENTE) 74

Figura 3.1: Modelos de Red Clásica Vs. NGN 74

Figura 3.2 Descripción de una red multiservicios 78

Figura 3.3: Red Basada en convergencia IP 84

Imagen 3.4 Arquitectura NGN 94

Figura 3.5: Llamada SIP 97

Figura 3.6: Pila de Protocolos H.323 104

Figura 3.7 Señalizacion H323 106

Figura 3.8 Componentes MEGACO 107
Figura 3.9 Llamada de H.248 109
CAPÍTULO IV 120
TRANSELECTRIC S.A. 120
Figura 4.1 Clientes de TRANSELECTRIC S.A. 123
Figura 4.2 Medios de transmision utilizados por Transelectric S.A 124
Figura 4.3 Servicios que ofrece Transelectric S.A 125
Figura 4.4 Sistema Nacional de Transmisión 125
Figura 4.5 Conformación de cable submarino Arcos -1 130
Figura 4.6 Conformación de cable submarino MAYA –I 131
Figura 4.7 Fibra óptica OPGW 132
Figura 4.8 Red de FO de Transelectric S.A. 135
CAPÍTULO V 140
DISEÑO DE LA RED 140
Figura 5.1 Estructura del módulo de transporte síncrono 144
Figura 5.2 Mapa del anillo de fibra 145
Figura 5.3. Mapa del anillo de fibra 146
Tabla 5.1 - Capacidades de trafico ruta Quito – Jamondino. 149
Figura 5.4 – Fotografía Siemens Surpass hiT7070 154
Figura 5.5 – Fotografía Siemens SMA16. 155
Figura 5.6 – Diagrama de la red de sincronismo actual de TRANSELECTRIC 159
Figura 5.7 – Fotografía Symmetricom TimeSource 3100. 160
Figura 5.8 – Fotografía Symmetricom SSU 55400A. 161
Figura 5.9 Descripción general de la red 162
Figura 5.10 Red actual de Transelectric S.A 163
Figura 5.11 Distribución Core MPLS. 173

Figura 5.12 Descripción General de la Red..... 174

CONCLUSIONES Y RECOMENDACIONES. 190

BIBLIOGRAFÍA 192

ANEXOS 196

CAPÍTULO I 16
DISEÑO CONCEPTUAL DE LA INVESTIGACIÓN 16
CAPÍTULO II 40
CONCEPTOS Y ELEMENTOS BÁSICOS DE UNA RED MPLS 40
CAPITULO III 74
RED MULTISERVICIO (RED CONVERGENTE) 74
CAPÍTULO IV 120
TRANSELECTRIC S.A. 120
Tabla 4.1: Cobertura a nivel Nacional de Transelectric S.A 126
Tabla 4.2: Capacidad de la red de Transelectric S.A 127
Tabla 4.3 Clientes Principales y servicios de Transelectric S.A 128
Tabla 4.4: Backbone Capacidades Transelectric S.A. 134
Tabla 4.5 Características Portador de Portadores TRANSELECTRIC 138
Tabla 4.6 Características Servicios al MEM 139
CAPÍTULO V 140
DISEÑO DE LA RED 140
Tabla 5.1 - Capacidades de trafico ruta Quito – Jamondino 149
Tabla 5.2 – Capacidades de trafico ruta Quito – Santo Domingo. 150
Tabla 5.3 – Capacidades de trafico ruta Santo Domingo – Quevedo 150
Tabla 5.4 – Capacidades de trafico ruta Quevedo – Manta. 151
Tabla 5.5 – Capacidades de trafico ruta Quevedo – Guayaquil. 151
Tabla 5.6 – Capacidades de trafico ruta Guayaquil – Milagro 151
Tabla 5.7 – Capacidades de trafico ruta Milagro – Machala 152
Tabla 5.8 – Capacidades de trafico ruta Milagro – Cuenca. 152

Tabla 5.9 – Capacidades de trafico ruta Cuenca – Loja. 152
Tabla 5.10 Equipos Activos en la red de Transelectric S.A 165
Tabla 5.11 Cambios en Equipos Activos 176
CONCLUSIONES Y RECOMENDACIONES. 190
BIBLIOGRAFÍA 192
ANEXOS 196
Tabla 5.11 Elemento Babahoyo 206
Tabla 5.12 Calderón 207
Tabla 5.13 Cuenca Capulispamba 208
Tabla 5.14 Chone 209
Tabla 5.15 Dos Cerritos 210
Tabla 5.16 Loja 211
Tabla 5.17 Machala 212
Tabla 5.18 Manta 213
Tabla 5.19 Milagro 214
Tabla 5.20 Molino 215
Tabla 5.21 Mulalo 216
Tabla 5.22 Pascuales 217
Tabla 5.23 Pomasqui 218
Tabla 5.24 Puyo 219
Tabla 5.25 Quevedo 220
Tabla 5.26 Riobamba 221
Tabla 5.27 Ibarra 222
Tabla 5.28 Salitral 223
Tabla 5.29 San Idelfonso 224

Tabla 5.30 Santa Elena..... 225

Tabla 5.31 Santa Rosa..... 226

Tabla 5.32 Santo Domingo 227

Tabla 5.33 Guangopolo Termo Pichincha..... 228

Tabla 5.34 Totoras 229

Tabla 5.35 Trinitaria..... 230

Tabla 5.36 Santa Rosa..... 231

Tabla 5.37 Vicentina 232

CAPÍTULO I

DISEÑO CONCEPTUAL DE LA INVESTIGACIÓN

1.1 DETERMINACIÓN DEL PROBLEMA

El enorme crecimiento de la red Internet ha convertido al protocolo IP en la base de las actuales redes de telecomunicaciones.

Por su desempeño la red IP hoy en día se ha convertido en una extensa red en la que las posibilidades de negocio y los mercados de consumo inducen al desarrollo de nuevas aplicaciones de voz y multimedia que requieren mayor QoS (Calidad de Servicio) ancho de banda en el servicio.

Actualmente nos acercamos a una convergencia entre voz, datos y video en la red IP y su infraestructura y protocolos han sido optimizados sólo para datos por este motivo, los diferentes protocolos existentes como: IGPs (Interior Gateway Protocol), RIP (Routing Information Protocol), OSPF (Open Shortest Path First), EGPs (Exterior Gateway Protocol) y BGP4 (Border Gateway Protocol v4), no son la solución óptima. Muchos de estos protocolos de enrutamiento están basados en algoritmos para obtener el camino más corto sin tener en cuenta métricas adicionales como retardo, jitter y congestión del tráfico.

Todo esto se traduce en varios complicaciones tales como: sobrecargas en el router IP, problemas de propagación de las rutas y la obligación de integrar redes IP con ATM (Modo de Transferencia Asíncrona).

MPLS ha sido desarrollado para eliminar varios de estos problemas, como son el retardo y la congestión del tráfico. Es un estándar IP de conmutación de paquetes del IETF contenido en el RFC 3031, que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión. Básicamente es una arquitectura multinivel, capaz de soportar cualquier tipo de tráfico e independiente del nivel de transporte de datos sobre el que se apoya. Puede ofrecer una gran eficiencia a la hora de realizar la transmisión de paquetes de un extremo a otro de la red MPLS, gracias a que combina la flexibilidad del nivel de red IP con los beneficios propios de un modelo de red orientado a conexión.

1.2 DEFINICIÓN DEL TEMA

"Diseño de una red de multiservicios mediante un mecanismo de transporte de datos MPLS (Multiprotocol Label Switching) para la empresa Transelectric S.A."

1.3 JUSTIFICACIÓN E IMPORTANCIA

El Internet ha permitido un considerable crecimiento en la innovación tecnológica. MPLS es un claro ejemplo de esto. Hoy en día el uso de las Tecnologías de Información y Comunicación (TIC) se ha convertido en un componente central de toda organización que busque un crecimiento sostenido.

Como resultado del uso de estas tecnologías la organización puede reducir el tamaño de su estructura jerárquica e incrementar el flujo de información, además de proveer de una ventaja competitiva a la misma.

La creciente popularidad del Multi-Protocol Label Switching debido a su capacidad para integrar voz, vídeo y datos en una plataforma común con garantías de calidad de servicio (QoS), mejoras del rendimiento, disponibilidad así como su soporte de una amplia y escalable gama de servicios, hacen que muchas empresas estén migrando a servicios basados en MPLS o, al menos, estén considerando el cambio.

Por estas razones se ve la necesidad de realizar una investigación que documente las principales características de MPLS, su capacidad como núcleo común para integrar voz, datos, video, y los principales requerimientos que una empresa necesita para realizar tal migración.

1.4 OBJETIVOS

1.4.1 Objetivo General

- Diseñar una red multiservicios mediante el uso de Multiprotocol Label Switching MPLS con garantías de calidad de servicio, rendimiento, disponibilidad y soporte en la empresa Transelectric S.A.

1.4.2 Objetivos específicos

- Describir el funcionamiento básico de la arquitectura MPLS y sus principales componentes.

- Definir e implementar las principales características de seguridad en una red basada en MPLS.

- Determinar los principales pasos necesarios para realizar una migración hacia una red MPLS.

- Determinar las principales ventajas y desventajas que posee una red MPLS con redes tradicionales.

- Determinar las características y la importancia de una red multiservicios.

- Brindar una visión futura de las redes con arquitectura MPLS como solución tecnológica altamente viable.

- Evaluar y diagnosticar el estado actual de la red LAN (Local Área Network, Red de Área Local) de información de TRANSELECTRIC S.A.

- Describir las diferentes aplicaciones que utiliza esta tecnología: Redes virtuales privadas, ingeniería de tráfico y calidad de servicio.

1.5 HIPÓTESIS

Considerando que el presente estudio se basa en una investigación aplicada, carece de hipótesis, puesto que, en el desarrollo del tema se considera aspectos importantes de la

tecnología de comunicaciones y propone el diseño de una red multiservicios basada en MPLS, por ello, no hay demostraciones resultantes de la investigación.

1.6 DELIMITACIÓN DEL TEMA

Para la empresa Transelectric S.A la implementación de MPLS en su red es de vital importancia, por tal motivo diseñar una red multiservicios mediante el uso de este protocolo, con garantías de calidad de servicio, rendimiento, disponibilidad y soporte es fundamental para que en conjunto con estudios de factibilidad económica, dicha empresa tome la resolución de su implementación.

Por lo tanto este proyecto está dirigido a el diseño Describir el funcionamiento básico de la arquitectura MPLS y sus principales componentes con sus respectivas seguridades, analizando los puntos críticos y pasos necesarios para realizar dicha una migración en la empresa, enumerando las principales ventajas y desventajas que se adquiriría con la implementación de dicha tecnología en comparación a sus antecesoras.

1.7 MARCO TEÓRICO

1.7.1 Antecedentes de MPLS

Antes de hablar de MPLS es importante conocer las tecnologías que le precedieron y que sirvieron como base para la creación de este estándar. Como ya se ha mencionado, el crecimiento de la red Internet y la aparición de nuevas aplicaciones, obligaron al uso de un mayor ancho de banda y una mejor gestión de la red. Esto obligo a los proveedores de servicios a mejorar la infraestructura de la red para lograr una mayor eficiencia en el transporte de información. Los primeros esfuerzos trataban de integrar funciones de las capas 2 y 3 del modelo OSI con el fin de aumentar el rendimiento de los routers

tradicionales a la de un conmutador ATM. De esta forma, surgieron dos nuevas tecnologías: Primero IP sobre ATM y luego Conmutación IP, las cuales brindaron una solución inicial a algunos de los problemas existentes en la red.

1.7.2 Capa de red

La capa de red, se ocupa de la transmisión de los paquetes (datagramas) y de encaminar cada uno en la dirección adecuada. Según la normalización OSI, es una capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas.

Tipos de servicios

Los niveles superiores no deben conocer el tipo de red o redes sobre lo que función y la capa de red debe ocultar todos estos detalles. Los servicios del nivel de red se pueden diseñar orientados o no a la conexión y con control o no de errores.

Servicios Orientados conexión: Sólo el primer paquete de cada mensaje tiene que llevar la dirección destino. Con este paquete se establece la ruta que deberán seguir todos los paquetes pertenecientes a esta conexión. Cuando llega un paquete que no es el primero se identifica a que conexión pertenece y se envía por el enlace de salida adecuado, según la información que se generó con el primer paquete y que permanece almacenada en cada conmutador o nodo.

Servicios no orientados a conexión: Cada paquete debe llevar la dirección destino, y con cada uno, los nodos de la red deciden el camino que se debe seguir. Existen muchas

técnicas para realizar esta decisión, como por ejemplo comparar el retardo que sufriría en ese momento el paquete que se pretende transmitir según el enlace que se escoja.

Datagramas: Cada paquete se encamina independientemente, sin que el origen y el destino tengan que pasar por un establecimiento de comunicación previo.

Circuitos virtuales: En una red de circuitos virtuales dos equipos que quieran comunicarse tienen que empezar por establecer una conexión. Durante este establecimiento de conexión, todos los routers que haya por el camino elegido reservarán recursos para ese circuito virtual específico.

1.7.3 Protocolos de capa 3

Algunos protocolos de la capa de red son:

1.7.3.1 Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

Protocolo Novell o simplemente IPX es una familia de protocolos de red desarrollados por Novell y utilizados por su sistema operativo de red NetWare.

Características principales

- Creados a principios de 1998.
- Deriva de la familia de protocolos Xerox Network Services (XNS) de Xerox.

- Fue diseñados para eliminar la necesidad de enumerar los nodos individuales de una red.

- Se ha implementado en otros sistemas operativos como el NWLink de Windows.

- Ha sobrevivido durante 15 años ya que actualmente está en desuso desde que el boom de Internet hizo a TCP/IP casi universal.

- En la actualidad su uso se ha reducido únicamente a juegos en red antiguos.

Protocolos que lo componen:

IPX (Internetwork Packet Exchange)

- El protocolo Intercambio de Paquetes Entre Redes.

- Es una implementación del protocolo **IDP** (Internet Datagram Protocol) de Xerox.

- Es un protocolo de datagramas rápido orientado a comunicaciones sin conexión que se encarga de transmitir datos a través de la red, incluyendo en cada paquete la dirección de destino.

- Pertenece a la capa de red (nivel 3 del modelo OSI) y al ser un protocolo de datagramas es similar al protocolo IP del TCP/IP en sus operaciones básicas pero

diferentes en cuanto al sistema de direccionamiento, formato de los paquetes y el ámbito general.

- Más simple y con menor fiabilidad que IP de TCP/IP

SPX **(Sequenced Packet Exchange)**

- Protocolo de Intercambio de Paquetes en Secuencia SPX

- Es la implementación del protocolo SPP (Sequenced Packet Protocol) de **Xerox**.

- Es un protocolo fiable basado en **comunicaciones con conexión** y se encarga de controlar la integridad de los paquetes y confirmar los paquetes recibidos a través de una red.

- Pertenece a la capa de transporte (nivel 4 del modelo OSI) y actúa sobre IPX para asegurar la entrega de los paquetes (datos), ya que IPX por sí solo no es capaz.

- Es similar a TCP ya que realiza las mismas funciones.

- Se utiliza principalmente para aplicaciones cliente/servidor.

Direccionamiento

Soporta direcciones de 32 bits que se asignan completamente sobre una red en vez de sobre equipos individuales.

Para identificar cada equipo dentro de la red, se emplea hardware específico.

Cada dirección posee tres componentes:

- Dirección de red
- Número del nodo
- Número de socket

De esta forma, un nodo dentro de la red se representará como:

Dirección de red	Numero de nodo

Mientras que un proceso dentro de la red se representará como:

Numero de conexión	Numero de socket

Ventajas

Se ha utilizado sobre todo en redes de área local (LANs) porque es muy eficiente para este propósito (típicamente su rendimiento supera al de TCP/IP en una LAN).

Desventajas

En redes medianas (MANs) y grandes (WANs) no se puede enrutar y por tanto no es utilizable, y también puede llegar a saturar la red con el alto nivel de tráfico que genera los broadcast que lanzan los equipos para anunciarse en la red.

1.7.3.2 Systems Network Architecture (SNA)

Arquitectura de red diseñada y utilizada por IBM para la conectividad con grandes ordenadores y servidores muy robustos que soportan millones de transacciones que por lo general son utilizados en bancos.

Características principales

- Su primera versión en el año de 1974, sólo permite redes centralizadas, es decir, redes en forma de árbol con sólo un HOST y sus terminales.

- Su versión posterior, de 1974, ya permitía tener múltiples HOST's con sus respectivos árboles, con la posibilidad de tener comunicación entre árboles, solamente a través de sus raíces.

- La versión de 1979 eliminó esta restricción, teniendo ahora la capacidad para comunicarse de manera más general.

- Por último en 1985 incluyó la aparición de topologías arbitrarias de HOST y LAN.

- Fácil comunicación entres usuarios finales, incluyendo transparencia de la red para esos usuarios.

- Separación de la función que realiza la arquitectura estratificada de SNA.

- Posibilidad de utilizar muchos tipos de dispositivos con la red realizando cualquier conversión necesaria a protocolos independientes de los dispositivos de SNA.

Soporte de funciones distribuidas.

- Soporte de la compartición de recursos permitiendo a los usuarios finales asignar o desasignar recursos de manera dinámica.

- Posibilidad de reconfigurar o modificar la red en forma dinámica.

- Es común que las redes de cajeros automáticos estén conectadas bajo SNA.

Ventajas

- Más seguro que el TCP/IP.

- Los Bancos todavía la siguen utilizando.

Desventajas

- SNA es muy complejo de utilizar para los programadores.

1.7.3.3 AppleTalk

Conjunto de protocolos desarrollados por Apple Inc. para la conexión de redes. Fue incluido en un Macintosh en 1984 y actualmente está en desuso en los Macintosh en favor de las redes TCP/IP.

Historia

1984 Desarrollo e inclusión en un Macintosh.

1985 En ese tiempo solo se compartían impresoras utilizando el concepto del Selector.

1986 Se introducen los enrutadores, su función es la de separar redes en pequeñas porciones para evitar la saturación y el tráfico.

1987 Se introduce EtherTalk y un servidor de archivos. Hasta este año se comparten archivos y se tiene un servidor como tal.

1988 Se introducen VAXes y PC's a la red. En este momento se dan las primeras conexiones de Macintosh con otros ambientes.

1989 Ya se tienen miles de nodos EtherTalk. Se introducen las primeras interconexiones a redes de Internet.

Características Principales

AppleTalk identifica varias entidades de red, cada una como un nodo.
Los nodos más comunes son computadoras Macintosh e impresoras Láser, pero muchos otros tipos de computadoras como IBM PC's, Digital VAX/VMS Systems y una gran variedad de estaciones de trabajo y enrutadores son también capaces de comunicarse con AppleTalk,.

Una red AppleTalk es simplemente un cable lógico sencillo y una zona AppleTalk es un grupo lógico de una o más redes.

AppleTalk fue diseñada como un cliente/servidor o sistema de red distribuido.

El diseño de Appletalk se basa en el modelo OSI pero a diferencia de otros de los sistemas LAN no fue construido bajo el sistema Xerox XNS,

El problema de Appletalk es que fue pensado originalmente para ser parte de un proyecto conocido como Macintosh Office, que consistiría en un ordenador central que proporciona el encaminamiento, compartición de impresoras y compartición de archivos.

Direccionamiento

- Una dirección de Appletalk constaba de 4 bytes.
- Un número de red de dos bytes.
- Un número de nodo de un byte

- Un número de socket de un byte.

De éstos, solamente el número de red requería configuración y era obtenido de un enrutador.

En lugar de direcciones, todos los servicios tenían nombres que intentaban ser significativos a los usuarios, y también eran suficientemente largos para reducir al mínimo los conflictos de conexión.

1.7.3.4 ATM (Asynchronous Transfer Mode).

El Modo de Transferencia Asíncrona o Asynchronous Transfer Mode (ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

El propósito de ATM es el de permitir a los usuarios mucho más flexibilizad para seleccionar cualquier ancho de banda que desee para favorecer su aplicación. La mayor parte de la base instalada de equipo de usuario tienen puertas con anchos de banda designados para competir con los sistemas de comunicación para los cuales se conecta. La mayoría de los puertos están por ello en 64 Kbps, 768 Kbps, y así sucesivamente.

El propósito de ATM es el de permitir más opciones para diseñadores de equipo de usuario, así que el ancho de banda de los puertos pueden ser más cercanamente competitivos a los requerimientos de las aplicaciones de usuario.

Otro propósito de ATM es el de permitir al usuario variar el ancho de banda durante el curso de una llamada. Esto puede deberse a las variaciones naturales en el tráfico siendo mandado por ejemplo: el estallido en el tráfico de interconexión (AN). Alternativamente esto se debe a que el usuario desea cambiar los requerimientos de ancho de banda durante el curso de una llamada (Por ejemplo, durante una llamada de voz, el usuario desea mandar una imagen de alta resolución para ilustrar un punto durante una discusión.

Esto debe de hacer notar que todas las formas de comunicación en su forma pura requieren una variación de ancho de banda dinámico. Las voces contienen pausas entre palabras, fax e imagen congelada, contienen áreas con más detalles que otras y el video tiene más rango de información cuando las escenas involucran más movimiento.

Esas variaciones están clasificadas dentro de rangos de bit constantes, de manera que se ajuste a los requerimientos de canales de telecomunicación con anchos de banda fijos.

Historia de ATM

La primera referencia del ATM (Asynchronous Transfer Mode) tiene lugar en los años 60 cuando un norteamericano de origen oriental perteneciente a los laboratorios Bell describió y patentó un modo de transferencia no síncrono. Sin embargo el ATM no se hizo popular hasta 1988 cuando el CCITT decidió que sería la tecnología de conmutación de las futuras redes ISDN en banda ancha (rec I.121). Para ello, el equipo detrás del ATM tuvo primero que persuadir a algunos representantes de las redes de comunicaciones que hubieran preferido una simple ampliación de las capacidades de la ISDN en banda estrecha.

Conseguido este primer objetivo y desechando los esquemas de transmisión síncronos, se empezaron a discutir aspectos tales como el tamaño de las celdas. Por un lado los representantes de EEUU y otros países proponían un tamaño de celdas grande de unos 64 bytes. Sin embargo para los representantes de los países europeos el tamaño ideal de las celdas era de 32 bytes (Según Tanenbaum), y señalaban que un tamaño de celda de 64 bytes provocaría retardos inaceptables de hasta 85 ms.

Este retardo no permitiría la transmisión de voz con cierto nivel de calidad a la vez que obligaba a instalar canceladores de eco. Después de muchas discusiones y ante la falta de acuerdo, en la reunión del CCITT celebrada en Ginebra en junio de 1989 se tomó una decisión salomónica: “Ni para unos ni para otros. 48 bytes será el tamaño de la celda”. Para la cabecera se tomó un tamaño de 5 bytes. Un extraño número primo 53 (48+5) sería el tamaño definitivo, en octetos, de las células ATM. Un número que tuvo la virtud de no satisfacer a nadie, pero que suponía un compromiso de todos los grupos de interés y evitaba una ruptura de consecuencias imprevisibles.

Formato de las celdas ATM

Son estructuras de datos de 53 bytes compuestas por dos campos principales:

Header: sus 5 bytes tienen tres funciones principales: identificación del canal, información para la detección de errores y si la célula es o no utilizada. Eventualmente puede contener también corrección de errores y un número de secuencia.

Payload: tiene 48 bytes fundamentalmente con datos del usuario y protocolos AAL que también son considerados como datos del usuario.

Dos de los conceptos más significativos del ATM, Canales Virtuales y Rutas Virtuales, están materializados en dos identificadores en el header de cada célula (VCI y VPI) ambos determinan el enrutamiento entre nodos. El estándar define el protocolo orientado a conexión que las transmite y dos tipos de formato de celda:

NNI (Network to Network Interface o interfaz red a red) El cual se refiere a la conexión de Switches ATM en redes privadas.

UNI (User to Network Interface o interfaz usuario a red) este se refiere a la conexión de un Switch ATM de una empresa pública o privada con un terminal ATM de un usuario normal, siendo este último el más utilizado.

Diagrama de una celda UNI

7			4	3			0
GFC				VPI			
VPI							
VCI							
				PT		CLP	
HEC							
Payload (48 bytes)							

Diagrama de una celda NNI

7			4	3			0
VPI							
VPI							
VCI							
				PT		CLP	
HEC							
Payload (48 bytes)							

Figura 1.1 Diagrama de Celdas ATM (UNI , NNI)

Campos

GFC (Control de Flujo Genérico, Generic Flow Control, 4 bits): El estándar originariamente reservó el campo GFC para labores de gestión de tráfico, pero en la práctica no es utilizado. Las celdas NNI lo emplean para extender el campo VPI a 12 bits.

VPI (Identificador de Ruta Virtual, Virtual Path Identifier, 8 bits) y VCI (Identificador de Circuito Virtual, Virtual Circuit Identifier, 16 bits): Se utilizan para indicar la ruta de destino o final de la celula.

PT (Tipo de Información de Usuario, Payload type, 3 bits): identifica el tipo de datos de la celda (de datos del usuario o de control).

CLP (Prioridad, Cell Loss Priority, 1 bit): Indica el nivel de prioridad de las celda, si este bit esta activo cuando la red ATM esta congestionada la celda puede ser descartada.

HEC (Corrección de Error de Cabecera, Header Error Correction, 8 bits): contiene un código de detección de error que sólo cubre la cabecera (no la información de usuario), y que permite detectar un buen número de errores múltiples y corregir errores simples.

1.7.3.5 Modelo IP/ATM

En los años noventa IP fue ganando terreno como protocolo de red ante otras arquitecturas que en esa época como las mencionadas, IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange), SNA **(**Systems Network Architecture), ApleTalk.

El gran auge de la Internet y su explosivo crecimiento generó un déficit de ancho de banda, ya que los "backbones" IP de los proveedores de servicio (NSP network service provider) estaban construidos con enrutadores conectados por líneas dedicadas T1/E1 y T3/E3, lo que ocasionaba congestión y satura miento de las redes. Había entonces que idear otras alternativas de ingeniería de tráfico.

Del mismo modo los NSPs se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo.

Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los routers tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los routers IP. A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de telecomunicación.
Estas redes ofrecían entonces una buena solución a los problemas de crecimiento de los NSPs. proporcionando mayores velocidades (155 Mpbs) y la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto

ganó adeptos entre la comunidad de NSPs, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de enrutadores IP sobre una topología real de conmutadores ATM. Cada enrutador se comunica con el resto mediante los circuitos virtuales permanentes (PVC) que se establecen sobre la topología física de la red ATM, desconociendo la topología real de la infraestructura ATM que sustenta los PVC como se observa en la figura 1 y figura 2.

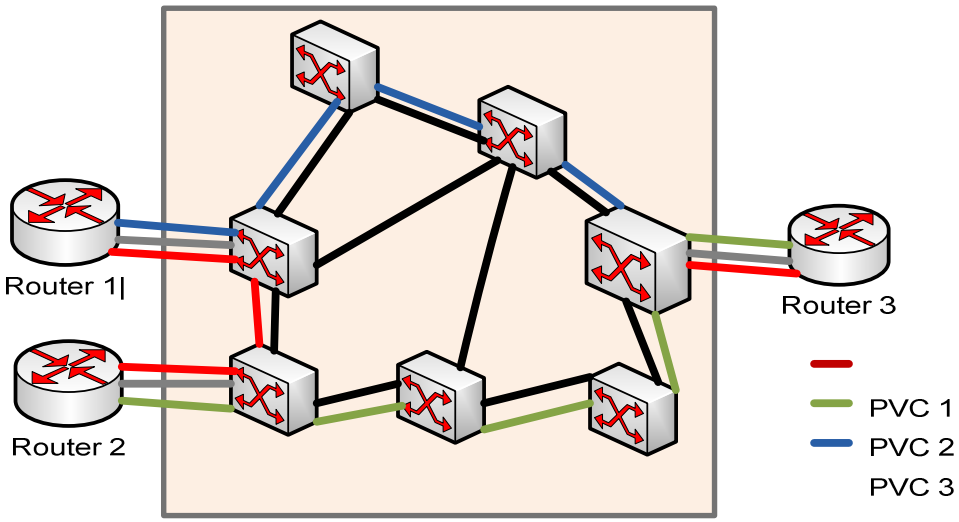


Figura 1.2: Topología Física ATM

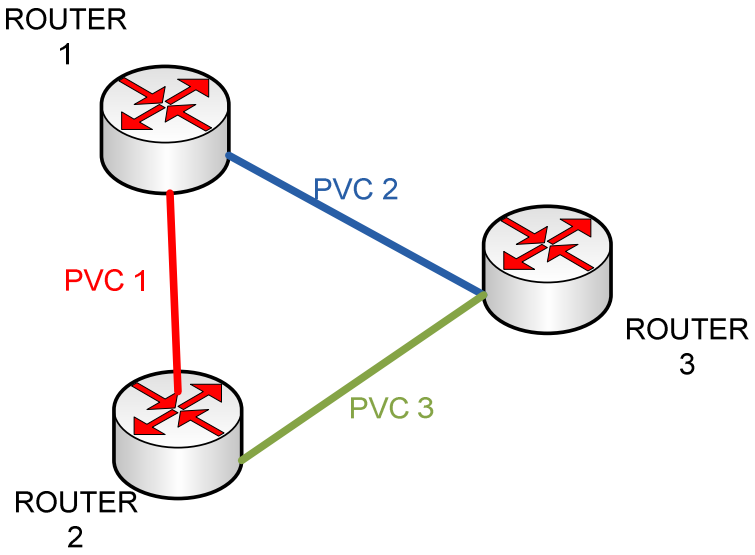


Figura 1.3: Topología Lógica

El hecho de superponer IP sobre ATM permite aprovechar la infraestructura ATM ya existente, obteniendo de esta manera un ancho de banda a precios competitivos, y una rapidez de transporte de datos proporcionada por los conmutadores.

Sin embargo, el modelo IP/ATM tiene también sus inconvenientes: hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio unos mayores costes de gestión global de sus redes.

1.7.3.6 Conmutación IP

La conmutación IP son técnicas para la integración de los niveles de forma efectiva y nace en respuesta a los problemas derivados del rendimiento de la solución IP/ATM,
El problema que presentaban estas soluciones o técnicas era la falta de interoperabilidad, ya que se usaban diferentes tecnologías privadas para combinar las capas 2 y 3 (OSI). Todas las soluciones de conmutación multinivel se basan en dos componentes básicos comunes:

• La separación entre las funciones de control y envío.

• El paradigma de intercambio de etiquetas para el envío de datos.

En la figura 1.4 se representa la separación funcional de esas dos componentes, una de *control* y la otra de *envío*. La componente de control utiliza los protocolos estándar de encaminamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros *routers* para la construcción y el mantenimiento de las tablas de encaminamiento.

Al llegar los paquetes, la componente de envío busca en la tabla de envío, que mantiene la componente de control, para tomar la decisión de encaminamiento para cada paquete. En concreto, la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde la interfaz de entrada al de salida a través del correspondiente hardware de conmutación.

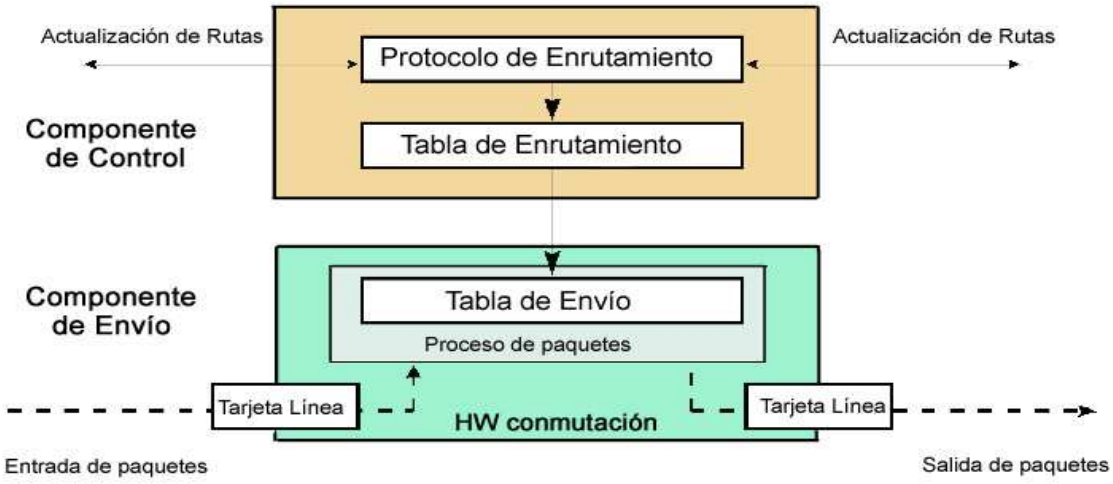


Figura 1.4 Separación entre las funciones de control y envío

Al separar la componente de control de la componente de envío, cada una de ellas se puede implementar y modificar independientemente. Para el envío de datos, se realiza un intercambio de etiquetas. Una etiqueta es un campo de unos pocos bits y de longitud fija, que se añade a la cabecera del paquete y que identifica a una "clase equivalente de envío" (FEC, "Forwarding Equivalente Class").

El algoritmo de intercambio de etiquetas permite así la creación de caminos virtuales conocidos como LSP (Label Switched Path), funcionalmente equivalente a los PVCs de ATM. La diferencia básica entre las técnicas de conmutación y el modelo IP/ATM es que en el fondo lo que se hace es imponer una conectividad entre extremos a una red no conectiva por naturaleza (como son las redes IP), pero todo ello sin perder la visibilidad del nivel de red.

CAPÍTULO II

CONCEPTOS Y ELEMENTOS BÁSICOS DE UNA RED MPLS

2.1 INTRODUCCIÓN

MPLS es hoy día una solución clásica y estándar al transporte de información en las redes. Reconocido por toda la comunidad de Internet, ha sido hasta hoy una solución aceptable para el envío de información, utilizando enrutamiento de paquetes con ciertas garantías de entrega y permitiendo la incorporación de calidad de servicio y conmutación a nivel de capa 2.

A su vez, los avances en el hardware y una nueva visión a la hora de manejar las redes, están dando lugar al empleo creciente de las tecnologías de Conmutación, aportando velocidad, calidad de servicio y facilitando la gestión de los recursos en la red por esto la tecnología MPLS se constituye como la base para las nuevas redes de banda ancha.

En la actualidad, la banda ancha está basada principalmente en SDH[1], con velocidades que va de los 155,52 Bit/s hasta varios Bit/s. esta tecnología de conmutación esta pronta a ser renovada, siendo el principal candidato MPLS. SDH seguirá todavía, pero por el momento su convivencia con MPLS será necesaria. MPLS ofrece grandes ventajas y soluciones tecnológicas para el futuro, como son MP λ S y GMPLS, orientadas al dominio óptico, que permitirán a las redes alcanzar velocidades de trasmisión del orden del Tbit/s por una sola fibra. Aunque parezcan capacidades enormes, podemos dar por supuesto que tarde o temprano serán velocidades de trasmisión Que llegaran a un punto de saturación por los distintos servicios que los usuarios demanden, en especial los relacionados con Videoconferencia, videotelefonía, vigilancia remota, video bajo demanda, entre otros.

2.2 RESEÑA HISTÓRICA

El grupo de Trabajo en Ingeniería de Internet (IETF[2]) a cargo de MPLS se creó en 1997. Bajo la necesidad de lograr mejoras en el desempeño de las redes, para esto el IETF planteo los siguientes objetivos para la elaboración de dicho estándar.

- MPLS debía soportar el envío de paquetes tanto unicast como multicast.

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM.

- MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP (protocolo de reserva de recursos).

[1] **SDH (Jerarquía digital sincrónica)**: es un una norma para el transporte de datos en telecomunicaciones formulado por la Unión de Telecomunicación Internacional (ITU).
[2] **IETF:** Organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad.

- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

- MPLS debía permitir el crecimiento constante del Internet.

Antes de la creación de este grupo del IETF existieron otras tecnologías de conmutación, a continuación describiremos las principales.

2.2.1 IP / ATM

La arquitectura ATM difiere significativamente de la arquitectura IP. La primera es una arquitectura orientada a conexión mientras que la segunda no lo es. Además, el esquema de direcciones es totalmente diferente, al igual que lo es el modelo de comunicación multicast o multienvío. Éstas son algunas de las diferencias entre ambos modelos.

Dada la necesidad existente de transportar paquetes IP sobre redes ATM, han surgido grupos de trabajo del IETF.

Cabe destacar dos RFC[3]

- RFC 1483: IP sobre ATM
- RFC 1577: IP clásico sobre ATM y ATM ARP (servidor ATM ARP)

[3] **RFC:** conjuntó de documentos que sirven de referencia que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general.

La primera RFC trata sobre cómo encapsular datagramas IP en enlaces ATM.

En el modelo clásico los nodos IP pueden comunicarse entre sí, si pertenecen a la misma subred IP lógica (LIS, Logical IP Subnet). Una LIS es simplemente un conjunto de hosts y encaminadores conectados a través de una red ATM. Dichos hosts y encaminadores están en una red IP, por lo que comparten la misma dirección de subred.

Si un dispositivo en una LIS se quiere comunicar con otro que esté en otra LIS distinta, debe hacerlo a través de un encaminador que comunique ambas LIS's como se observa en la figura 4.

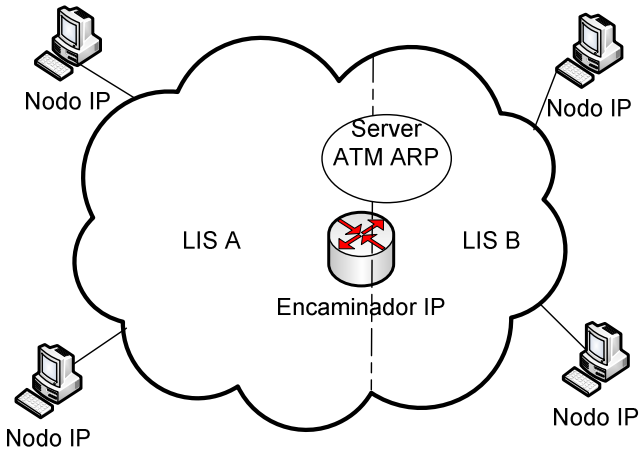


Figura 2.1 Arquitectura IP / ATM

Para que dos dispositivos que están en la misma LIS se puedan comunicar, es necesario que conozcan sus direcciones ATM. Para tal cosa es necesario disponer de un servidor ARP (Addres Resolution Protocol). En redes convencionales como las redes Ethernet, los

dispositivos IP aprenden sus respectivas direcciones gracias al protocolo ARP que se apoya en la difusión del nivel de enlace. Como las redes ATM carecen de esto se necesita el mencionado servidor para hacer la conversión de direcciones IP a direcciones ATM. Los dispositivos registran en dicho servidor su dirección ATM y su dirección IP de tal forma que cuando un dispositivo se quiere comunicar con otro que está en la misma LIS le solicita al servidor que haga la traducción de la dirección IP a la dirección ATM. Con la dirección ATM ya podrá comunicarse estableciendo un circuito virtual.

La RFC-1577 no aborda el tema de que dos dispositivos que se encuentren en distinta LIS puedan establecer un circuito virtual para comunicarse. Para esto surgió el grupo del IETF ROLC (Routing Over Large Clouds) que más o menos quiere decir "Encaminamiento a través de grandes nubes". Se definió el protocolo NHRP (Next Hop Resolution Protocol, Protocolo de resolución del siguiente salto) para resolver el problema del salto a través del encaminador que conecta ambas Lisas. Esto se consigue teniendo servidores NHS (Next Hop Servers), de tal forma que un dispositivo en una LIS puede aprender la dirección ATM de otro dispositivo de otra LIS a través del mencionado servidor. Con la dirección ATM ya pueden establecer un circuito virtual.

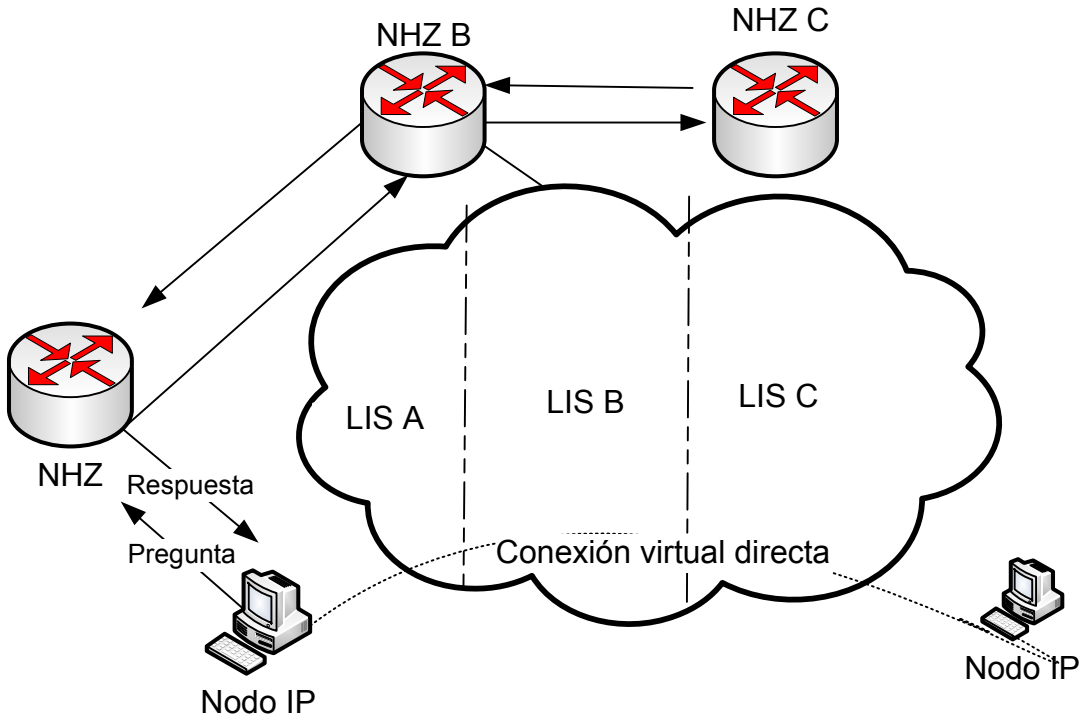


Figura 2.2 Routing Over Large Clouds

2.2.2 Cell Switching Router (CSR) de Toshiba

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

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

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

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

2.2.3 Conmutación IP (IP SWITCHING) De Ipsilon

Esta solución fue desarrollada por Ipsilon y lanzada al mercado a comienzos del año 1996. Se basa en un dispositivo que puede realizar funciones de conmutador ATM, al que se le ha eliminado el plano de control y también de encaminador IP de una manera sencilla y eficiente.

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

Para realizar correctamente estas funciones se definieron dos nuevos protocolos, uno destinado a establecer la relación entre los flujos de datos y las etiquetas denominadas Ipsilon Flow Management Protocol (IFMP); y otro para gestionar las funciones del conmutador ATM y controlar el establecimiento de los Circuitos Virutales a través de él, conocido como General Switch Management Protocol (GSMP).

2.2.4 Conmutación de etiquetas de CISCO (TAG SWITCHING)

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

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

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

2.2.5 ARIS (Agregate Route-based Ip Switching) de IBM

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

La idea que subyacía a la hora de diseñar ARIS fue la utilización de ATM como nivel de enlace, por lo que los protocolos propios de ARIS son protocolos "peer-to-peer" , que se establecen entre los ISR implicados directamente a nivel IP y permiten establecer conexiones con los vecinos e intercambiar las correspondientes etiquetas asociadas a los distintos flujos de datos.

Este mecanismo de distribución de etiquetas comienza en el extremo donde finaliza el flujo de datos en la red ARIS, también conocido como "egress router", y es propagado de forma ordenada hasta el ISR que comenzó el flujo.

2.3 CARACTERÍSTICAS BÁSICAS MPLS

"MPLS Multi-Protocol Label Switching es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de los servicios que poseen otras redes como Prívate Line, Frame Relay o ATM".

Su principal objetivo es crear redes flexibles y escalables con un incremento en el desempeño y la estabilidad. Esto incluye Ingeniería de Tráfico y Soporte de VPN[4] el cual ofrece Calidad de servicio (QoS[5]) con múltiples clases de servicios (CoS.)

Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia. Y todo ello en una única red.

Las etiquetas son insertadas entre el encabezado de capa 3 y el encabezado de capa 2 para el caso de tecnologías basadas en Frames.

Para tecnologías basadas en celdas, ATM por ejemplo están contenidas entre los campos VPI y VCI.

[4] **VPN (Red Virtual Privada)** : ttecnología de red que permite extender la red local sobre una red pública
[5] **QoS (Quality of service**): tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (throughput).

MPLS realiza la decisión del reenvió de paquetes basado en el contenido de una etiqueta en lugar de realizar un complejo lookup basado en la dirección IP destino. Esta técnica brinda muchos beneficios a las redes basadas en IP como son:

- VPN’s
- Ingeniería de Trafico
- Calidad de Servicio.

2.3.1 Flexibilidad

Cada empresa, corporación u organismo tiene y desarrollada su propia estructura interna, tanto en infraestructura como en recursos humanos, generadas en base a sus necesidades y recursos disponibles. En base a ésta estructura, muchas veces única, se montan los servicios de comunicaciones para acomodar de la mejor manera posible y al menor costo, el transporte de la información interna, así como también externa, con sus clientes y proveedores.

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

2.3.2 Escalabilidad

Con un nuevo concepto de aprovisionamiento, llamado "Point-to-Cloud" (punto a la nube), se implementan los nuevos puntos. Este concepto proviene del hecho de que cada vez que sea necesario "subir" un nuevo punto a la red, sólo habrá que configurar el equipamiento del Service Provider que conecte este nuevo punto.

De esta forma, evitamos tareas complejas y riesgosas, como las que se producen cuando se activa un nuevo punto en una red basada en circuitos virtuales de Frame Relay o ATM, en donde es necesario re-configurar TODOS los puntos involucrados.

2.3.3 Accesibilidad

La arquitectura de MPLS permite utilizar prácticamente todas las tecnologías de acceso para interconectar las oficinas del cliente con su "Service Provider" (Proveedor de Servicios).

Por dicho motivo, la versatilidad que nos permite utilizar xDSL o un enlace Wireless Ethernet en las oficinas más pequeñas y hasta incluso en usuarios móviles, mientras que en el Backbone utilizamos líneas (TDM) en altas capacidades como E3/T3, nos permite dimensionar cada punto de la red acorde a sus necesidades sin limitar o restringir la de otros puntos.

2.3.4 Eficiencia

En una infraestructura 100% IP, es decir, aquellas empresas en donde todo el equipamiento involucrado y las aplicaciones utilizadas son basadas en IP, el uso de servicios de transporte ATM o Frame Relay someten al cliente a incurrir en un costo adicional por el overhead que los protocolos de transporte que introducen. Mediante MPLS este costo extra desaparece.

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

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

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

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

2.3.6 Administración

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

2.3.7 Monitoreo y SLA's[6]

Las MPLS pueden ser monitoreadas, controladas y en forma permanente, las 24 horas los 7 días de la semana, por parte del Proveedor de Servicio. Además, se puede garantizar y asegurar la estabilidad y performance que el cliente necesite con la creación Salas.

2.3.8 Fácil Migración

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

[6] **SLA**(acuerdo nivel de servicio): contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio

2.3.9 Seguridad

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

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

2.3.10 Bajo Costo

Son varios los motivos que permiten afirmar que un servicio MPLS ofrece más por menos, entre ellos podemos destacar:

Al ser un servicio Network-based, la implementación de la red no requiere un hardware específico ni costoso para ser instalado en las oficinas del cliente.

Por ser una red que Soporta de Clases de Servicio (CoS) se puede integrar distintos servicios y aplicaciones sobre una misma plataforma. De este modo, empresas que al día de hoy mantienen distintos y costosos servicios para soportar sus necesidades de voz, datos

y video; pueden unificar estos requerimientos concluyendo en un ahorro significativo y manteniendo relación con un único proveedor de servicios.

2.4 FUNCIONAMIENTO MPLS

MPLS intenta conseguir las ventajas de ATM, pero sin sus inconvenientes Asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los routers intermedios (solo se mira la etiqueta, no la dirección de destino)

Es de notar que la conmutación IP es realizada en la capa 3 y está basada en la dirección IP destino (en algunos casos también en la IP de origen); si miramos una tabla de enrutamiento sólo vemos la asociación "red destino" - "próximo salto".

El enrutamiento en sí, impone restricciones y ciertos cuidados en nuestras redes, como por ejemplo que en la asignación de direcciones IP no haya colisiones es decir que dos segmentos de red no pueden tener las mismas direcciones.

Lo interesante de MPLS es que la conmutación de paquetes está basada en etiquetas y se realiza entre la capa 2 y la capa 3 (no depende del encabezado IP), estas etiquetas son agregadas antes del ingreso a la red MPLS y son removidas cuando los paquetes salen de ella.

MPLS funciona adicionando a los paquetes un header MPLS, que contiene una o más etiquetas, los campos de la cabecera MPLS de 4 bytes, son los siguientes:

Label (20 bits): Es el valor actual, con sentido únicamente local, de la etiqueta MPLS. Esta etiqueta es la que determinará el próximo salto del paquete.

CoS (3 bits): Este campo afecta a los algoritmos de descarte de paquetes y de mantenimiento de colas en los nodos intermedios, es decir, indica la QoS del paquete. Mediante este campo es posible diferenciar distintos tipos de tráficos y mejorar el rendimiento de un tipo de tráfico respecto a otros.

Stack (1 bit): Mediante este bit se soporta una pila de etiquetas jerárquicas, es decir, indica si existen más etiquetas MPLS. Las cabeceras MPLS se comportan como si estarían apiladas una sobre otra, de modo que el nodo MPLS tratará siempre la que esté más alto en la pila.

La posibilidad de encapsular una cabecera MPLS en otras, tiene sentido, por ejemplo, cuando se tiene una red MPLS que tiene que atravesar otra red MPLS perteneciente un organismo administrativo externo distinto; esto hace que al terminar de atravesar esa red, se continúe trabajando con MPLS como si no existiera dicha red externa.

TTL (8 bits): Este campo es copiado directamente de la cabecera IP y proporciona la funcionalidad de tiempo de vida del paquete o TTL (Time To Live) típica de IP; la cual

permite mitigar el efecto de posibles bucles en la red decrementando el valor inicial en una unidad por cada salto o nodo por el que pase el paquete.

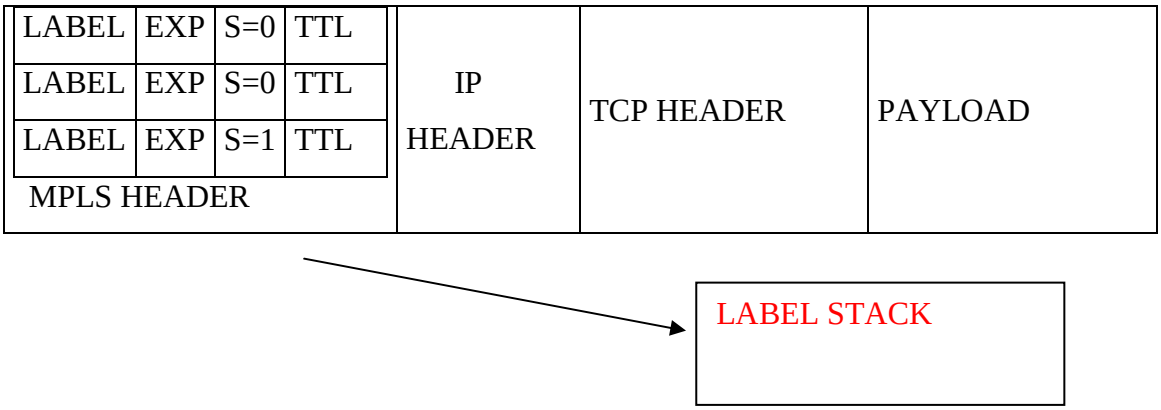


Figura 2.3 Cabecera MPLS

2.5 ARQUITECTURA DE UNA RED MPLS

Como cualquier nueva tecnología, aparecen nuevos términos para describir los dispositivos que conforman la arquitectura. Estos términos nuevos describen la funcionalidad de cada dispositivo y sus funciones en la estructura del dominio MPLS

Una red MPLS está compuesta por Routers MPLS:

2.5.1 LSR (Label Switching Router)

El primer dispositivo novedoso es el router de conmutación por etiquetas LSR. Todo router o Switch que implemente procedimientos de distribución de etiquetas y que pueda enviar

paquetes basándose en etiquetas, entra en esta categoría. La función básica de los procedimientos de distribución de etiquetas es la de permitir que un LSR distribuya sus enlaces de etiquetas a otros LSR de la misma red MPLS.

Los LSR son Router de gran velocidad en el núcleo de la red MPLS. Sus principales funciones son: Participar en el establecimiento de los circuitos extremo-extremo de la red o

LSP's (Label Switched Path) usando un protocolo de señalización apropiado y conmutar rápidamente el tráfico de datos entre los caminos establecidos.

Existen diferentes tipos de LSR que se diferencian por la funcionalidad que proporcionan a la infraestructura de red. Estos diferentes tipos de LSR se describen en la arquitectura como LSR de contorno, LSR ATM y LSR ATM de contorno. La distinción entre los diferentes tipos de LSR es puramente arquitectónica.

2.5.2 LSR de contorno

Es un router que realiza tanto la imposición de etiquetas como la determinación de etiquetas en el contorno de la red MPLS. La imposición de etiquetas es el acto de añadir una etiqueta, o pila de etiquetas, a un paquete en el punto de entrada (con respecto al flujo de tráfico desde el origen al destino) del dominio MPLS. La determinación de etiquetas es lo contrario, es decir el acto de eliminar la ultima etiqueta de un paquete en el punto de salida en el punto de salida antes de que se envíe a un vecino que está afuera del dominio MPLS.

Todo LSR que tenga vecinos que no sean MPLS se considera un LSR de contorno. No obstante, si este LSR tuviera alguna interfaz conectada a través de MPLS a un LSR ATM, entonces se ha de considerar un LSR ATM de contorno. Los LSR de contorno emplean la tradicional tabla de envíos IP, incrementada con información de etiquetado, para etiquetar paquetes IP o para eliminar etiquetas de los paquetes etiquetados antes de enviarlos a los nodos que no son MPLS.

Las acciones que realiza un LSR de contorno son:

- Recibir un paquete IP
- Efectúa consultas Capa 3,
- Impone una pila de etiquetas antes de enviar el paquete dentro del domino LSR.
- Puede recibir paquetes etiquetados
- Eliminar etiquetas
- Enviar paquete IP hacia el siguiente salto.

2.5.3 LSR-ATM

Un LSR- ATM es un Switch ATM que puede actuar como LSR. Los LSR- ATM efectúa el enrutamiento IP y la asignación de etiquetas en el plano de control y envía los paquetes de datos utilizando mecanismos de conmutación por celdas ATM adicionales en el plano de datos. En otras palabras, la matriz de conmutación ATM de un Switch ATM se utiliza como tabla de envió de etiquetas de un nodo MPLS. Por ello, los Switches ATM

tradicionales pueden desplegarse como LSR mediante una actualización del software de sus componentes de control.

Un LSR – ATM realiza las siguientes acciones:

- Ejecuta protocolos MPLS en el plano de control para establecer circuitos ATM virtuales.

- Envía paquetes etiquetados como celdas ATM.

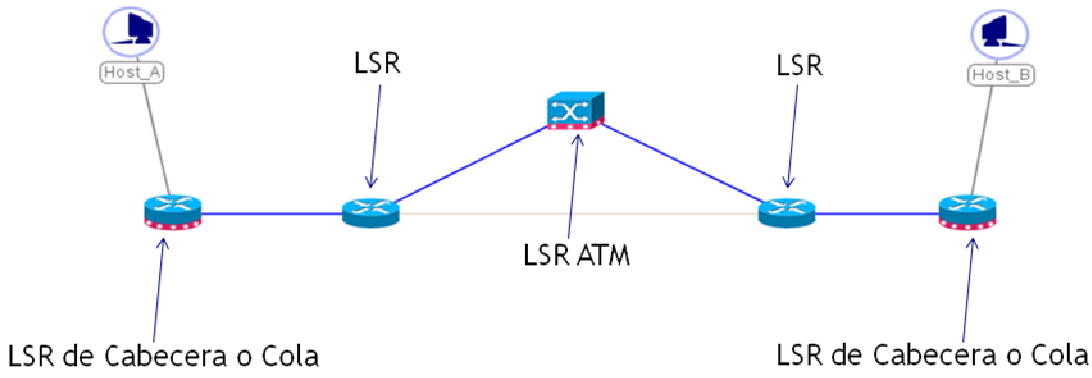


Figura 2.4 Tipos de LSR en el dominio MPLS

2.5.4 LER (Label Switching Router)

Los LER's están ubicados en el borde de la red MPLS para desempeñar las funciones tradicionales de encaminamiento y proporcionar conectividad a sus usuarios, generalmente routers IP convencionales. El LER analiza y clasifica el paquete IP entrante considerando hasta el nivel 3, es decir, considerando la dirección IP de destino y la QoS demandada; añadiendo la etiqueta MPLS que identifica en qué LSP está el paquete. Es decir, el LER en vez de decidir el siguiente salto, como haría un router IP normal, decide el camino entero a lo largo de la red que el paquete debe seguir. Una vez asignada la cabecera MPLS, el LER enviará el paquete a un LSR.

Los LSR están ubicados en el núcleo de la red MPLS para efectuar encaminamiento de alto rendimiento basado en la conmutación por etiqueta, considerando únicamente hasta el nivel 2. Cuando le llega un paquete a una interfaz del LSR, éste lee el valor de la etiqueta de entrada de la cabecera MPLS, busca en la tabla de conmutación la etiqueta e interfaz de salida, y reenvía el paquete por el camino predefinido escribiendo la nueva cabecera MPLS. Si un LSR detecta que debe enviar un paquete a un LER, extrae la cabecera MPLS; como el último LER no conmuta el paquete, se reducen así cabeceras innecesarias.

2.5.5 FEC (Forwarding Equivalence Class)

Un FEC es un conjunto de paquetes que comparten unas mismas características para su transporte, así todos recibirán el mismo tratamiento en su camino hacia el destino. Cada FEC puede representar unos requerimientos de servicio para un conjunto de paquetes o para una dirección fija. La clase FEC a la cual se asigna el paquete se codifica como un valor corto de longitud fija conocido como etiqueta. Esta etiqueta es usada por los

conmutadores de la red para encaminar el paquete hacia su siguiente nodo. Cuando un paquete se envía a su siguiente router, la etiqueta es enviada con él. La etiqueta se usa como un índice en la tabla que especifica el próximo salto y una nueva etiqueta. La etiqueta vieja es sustituida por la nueva, y el paquete es enviado al salto siguiente.

2.5.6 LSP (Label Switched Path):

Nombre genérico de un camino MPLS (para cierto tráfico o FEC), es decir, del túnel MPLS establecido entre los extremos. A tener en cuenta que un LSP es unidireccional.

2.5.7 LDP (Label Distribution Protocol):

Protocolo para la distribución de etiquetas MPLS entre los equipos de la red.

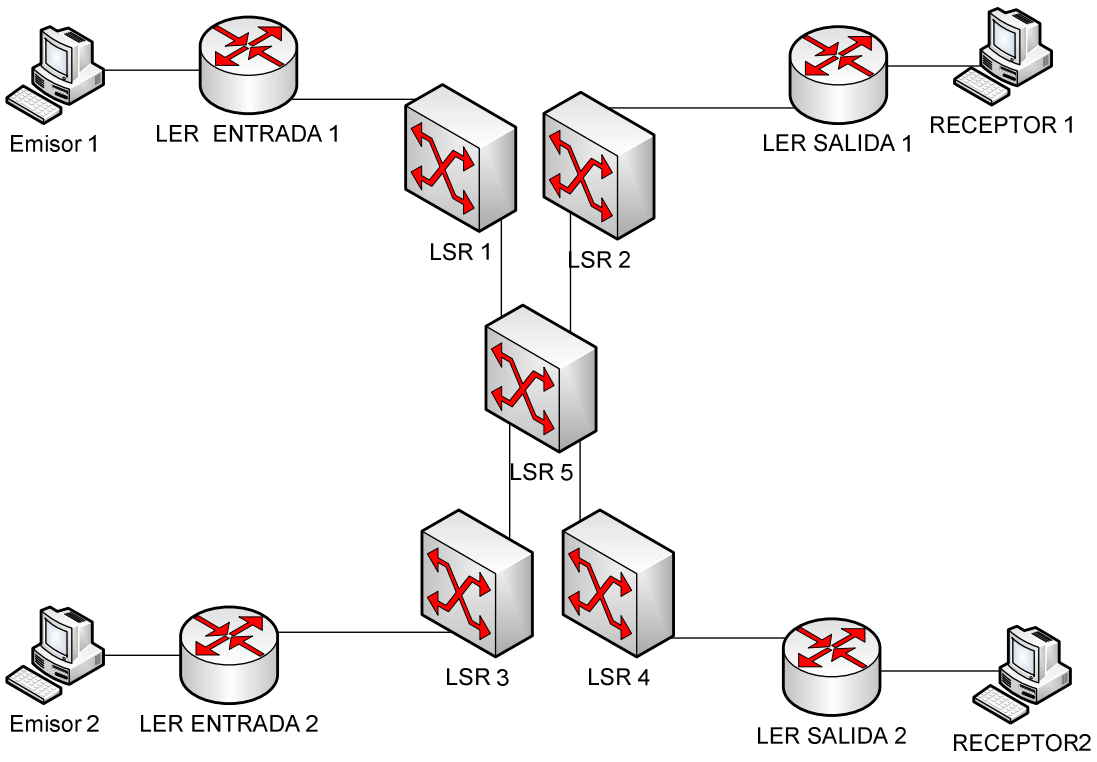


Figura 2.5 Arquitectura de una Red MPLS

2.6 ESTABLECIMIENTO DE UN LSP

Dentro de un dominio MPLS, un camino es establecido para que un paquete dado viaje con un determinado FEC. Existen dos mecanismos para establecer un LSP:

• Encaminamiento salto a salto: cada LSR selecciona independientemente el próximo salto para un FEC determinado (similar a la metodología utilizada en redes IP). El LSR utiliza cualquier protocolo de encaminamiento disponible como OSPF, ATM PNNI (ATM Private Network-Node Interface),etc.

• Encaminamiento explícito: El LER de entrada determina la secuencia de saltos explícito desde la entrada hasta la salida. Puede que la ruta no esté completamente especificada, es decir, puede haber un conjunto de nodos que es representado como un único salto en la ruta.

También puede contener un identificador de Sistema Autónomo que permita que el LSP sea encaminado a través de un área de la red que está fuera del control administrativo de quien inició el LSP. Dentro de estos dos casos se hará un encaminamiento salto a salto.

MPLS permite establecer LSP primarios y además establecer LSP de respaldo (backup) asociados a los de trabajo. El establecimiento de todos estos LSP se realiza usando algoritmos de encaminamiento con calidad de servicio que buscan la ruta óptima, tanto desde el punto de vista de la calidad de servicio requerida como desde el punto de vista del uso los recursos de la red.

A partir de este punto la gestión de recursos básicamente se encarga de ajustar los LSP establecidos en la red adaptándolos al uso real que se esté haciendo de ellos, de forma parecida a la que se emplea en ATM. Para conseguir esta adaptación al tráfico real de la red, los mecanismos de ingeniería del tráfico deben realizar tareas de monitorización. Por lo tanto, se puede afirmar que los mecanismos de gestión de recursos están constantemente pendientes del estado real de la red y fuertemente relacionados con el establecimiento de LSP de trabajo y de respaldo con algoritmos de encaminamiento con calidad de servicio.

Por este motivo, la gestión de recursos también cubre la detección de las alarmas en el momento en que se produce un fallo en la red y la activación de los LSP de respaldo, así como la monitorización del estado real de la red y procede a su adaptación (cambiando los LSP existentes) al tráfico real y a los posibles fallos que puedan surgir (activando los LSP de respaldo necesario). Una vez establecidos los LSP, éstos tendrán una cierta vida, corta o larga, durante la cual pueden sufrir una serie de problemas. Se puede establecer un LSP con un cierto ancho de banda asignado para una cierta cantidad de tráfico con una determinada calidad de servicio.

Sobre este LSP puede suceder que, al cabo de un cierto tiempo, la demanda de tráfico supere la reserva inicial y se produzca un rechazo de tráfico de entrada. Este rechazo o bloqueo se produce debido a algún tipo mecanismo de control de admisión, necesario para garantizar la calidad de servicio de las distintas conexiones existentes, y puede cuantificarse calculando la probabilidad de bloqueo para cada LSP. Otro fenómeno que puede suceder es que, una vez reservada una cierta cantidad de ancho de banda para un cierto LSP, después de cierto tiempo este LSP esté poco utilizado y se estén desperdiciando los recursos de la red, cuando posiblemente otros LSP puedan estar congestionados y rechazando tráfico.

La técnica habitual para adaptar el ancho de banda de los LSP al tráfico real es la reasignación de banda de los mismos, incrementándola o decrementándola según sea el caso. Para poder incrementar la banda de un LSP es necesario que a lo largo del camino que sigue este LSP (los diferentes enlaces físicos que atraviesa) existan los suficientes recursos libres. Si esto no sucede, existen dos posibles acciones a tener en cuenta. La primera es buscar en qué enlaces físicos no se cumple la condición de que no exista suficiente banda disponible, y posteriormente, en estos enlaces comprobar si existe algún otro LSP infrautilizado y del que se pueda tomar la banda necesaria. En otras palabras, consiste en traspasar banda de LSP´s pocos usados a un LSP congestionado y que necesita incrementar su banda. La segunda posibilidad, en el caso de que la primera no sea posible, es reencaminar el LSP que necesita mayor ancho de banda a través de otro camino que pueda satisfacer sus necesidades. También en este caso, si no es posible reencaminar al LSP congestionado, existe la posibilidad de reencaminar uno o varios de los demás LSP con los que comparten los mismos enlaces físicos, con lo cual se liberan recursos y permite incrementar su banda. En los casos en los que hay que reencaminar LSP se puede hacer uso de los algoritmos de encaminamiento dinámicos y con calidad de servicio.

De ahí que estos mecanismos de gestión de recursos estén estrechamente relacionados con los mecanismos de establecimiento de LSP de trabajo y de respaldo con calidad de servicio, creando un entorno global de ingeniería del tráfico. Otro aspecto a tener en cuenta es qué mecanismos toman la decisión de adaptar la banda de los LSP y realizar las operaciones anteriormente descritas. Existen diferentes ejemplos en la literatura, y dependiendo de dónde se tome la decisión, se puede hablar de mecanismos centralizados o distribuidos. Estos mecanismos, por las tareas que realizan, se situarían dentro del plan de gestión.

Tradicionalmente la gestión, en este caso de recursos y de fallos, se ha realizado de forma centralizada, lanzando algoritmos de optimización que, disponiendo de los datos de monitorización de toda la red, calculan la distribución óptima de los LSP. En redes troncales relativamente grandes, por las que circula gran cantidad de LSP, es muy difícil

disponer de todos los datos de monitorización de forma centralizada y calcular la distribución óptima a tiempo antes de que el estado de la red ya haya cambiado. Una de las opciones que aparecen en la literatura reciente es tratar de mantener la distribución de LSP lo más cercana posible a la óptima haciendo pequeños ajustes usando algoritmos distribuidos. La ventaja principal de los algoritmos distribuidos es que disponen de la información de forma local y permanentemente actualizada. Por el contrario, la desventaja está en que no se dispone de una visión global de la red.

2.7 JERARQUÍA MPLS

- MPLS funciona sobre multitud de tecnologías de nivel de enlace.

    - IP sobre Ethernet, Fast Ethernet o Gigabit Ethernet
    - IP sobre ATM
    - IP sobre Frame Relay.

- La etiqueta MPLS se coloca delante del paquete de red y detrás de la cabecera de nivel de enlace.

- Las etiquetas pueden anidarse, formando una pila con funcionamiento LIFO (Last In, First Out). Esto permite ir agregando (o segregando) flujos. El mecanismo es escalable.

- Cada nivel de la pila de etiquetas define un nivel de LSP - Túneles MPLS

- Así dentro de una red MPLS se establece una jerarquía de LSPs.

- En ATM y Frame Relay la etiqueta MPLS ocupa el lugar del campo VPI/VCI o en el DLCI, para aprovechar el mecanismo de conmutación inherente.

2.7.1 Etiquetas MPLS

- Las etiquetas MPLS identifican a la FEC asociada a cada paquete

- Etiqueta MPLS genérica:

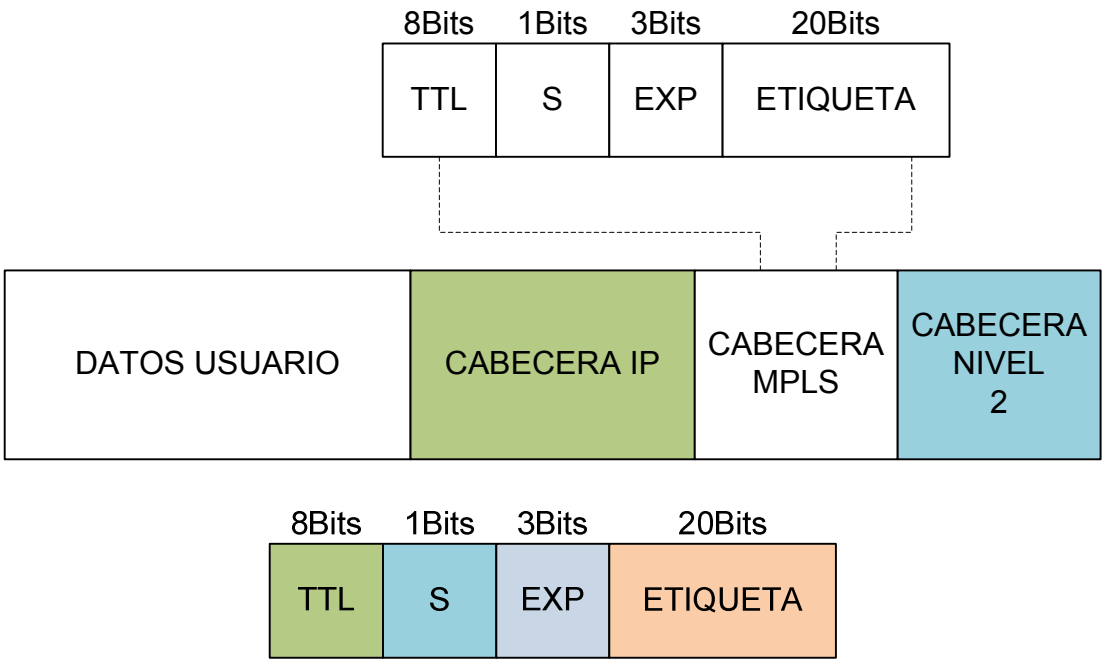


Figura 2.6 Etiquetas MPLS

Etiqueta: Esta identifica una FEC

Exp: Bits para uso experimental, se puede trasmitir en ella información de DiffServ.

S: Vale 1 para la primera entrada en la pila 0 para el resto.

TTL: Contador del numero de saltos este campo remplaza al TTL de la cabecera IP durante el viaje del datagrama por la red MPLS.

2.8 APLICACIÓN MPLS

Las aplicaciones principales de MPLS son:

- Encaminamiento explícito e ingeniería de tráfico.
- Soporte a las CoS
- Servicio de redes privadas virtuales (VPN: Virtual Private Network).
- Integración de IP con todo tipo de redes subyacentes: Frame Relay, ATM, SDH

2.9 INGENIERÍA DE TRÁFICO

La ingeniería de tráfico persigue adaptar flujos de tráfico a recursos físicos de la red, de tal forma que exista un equilibrio entre dichos recursos. De esta forma se conseguirá que no haya recursos excesivamente utilizados, con cuellos de botella, mientras existan recursos poco utilizados.

Uno de los mayores problemas de las redes IP actuales es la dificultad de ajustar el tráfico IP para hacer un mejor uso del ancho de banda, así como mandar flujos específicos por caminos específicos. En las redes IP convencionales los paquetes suelen seguir el camino más corto. Por ejemplo, los protocolos IGP siguen este criterio. Esto suele provocar que algunos enlaces se saturen mientras otros están infrautilizados. Este problema se ha venido resolviendo añadiendo más capacidad a los enlaces. Veamos un ejemplo:

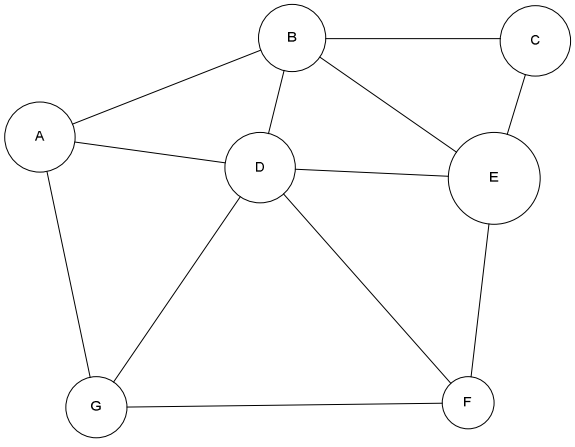


Figura 2.6 Ingeniería de Tráfico.

El camino más corto entre A y C según la métrica normal IGP es el que tiene dos saltos (A-B-C), pero puede que el exceso de tráfico sobre estos enlaces o la carga de los encaminadores hagan aconsejable la utilización de un camino que requiera saltos adicionales, como por ejemplo A-D-E-C.

MPLS es una herramienta efectiva para la ingeniería de tráfico:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.

- Permite obtener estadísticas de uso LSP.

- Permite usar el encaminamiento basado en restricciones de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales con distintos niveles de calidad (por ejemplo, con garantías de ancho de banda, etc.).

Soporte a las clases de servicio

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

Históricamente, Internet ha ofrecido un solo nivel de servicio: "Best effort". Con la aparición de aplicaciones multimedia y aplicaciones en tiempo real, surgió la necesidad de la diferenciación de servicios en Internet. De esta forma se podrán diferenciar servicios

como el correo electrónico de otros que dependen mucho más del retardo y de la variación del mismo como el video y la voz interactiva.

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

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

2.10 REDES PRIVADAS VIRTUALES

Una de las principales razones del despliegue de MPLS en proveedores de servicios y redes empresariales son los servicios de VPNs (VPN: Virtual Private Network).

Una red privada virtual se puede definir como una red en la que la conectividad entre múltiples lugares se realiza a través de una infraestructura compartida con las mismas políticas de acceso y seguridad que en una red privada. Una compañía en la que su intranet corra encima de un servicio de VPN tendrá la misma seguridad, fiabilidad, etc, que el resto de sus redes privadas. Por tanto, el objetivo de las VPN's es el soporte de aplicaciones

intra/extranet, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables.

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

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

Posteriormente, con la introducción de las VPN's, se pueden conectar múltiples sitios usando el backbone de un proveedor de servicios. Dicho proveedor ofrecerá servicios VPN a un precio inferior que con líneas dedicadas ya que el proveedor de servicios podrá utilizar los recursos de su Backbone de forma compartida para múltiples clientes. Estas tecnologías de VPN se basaban fundamentalmente en protocolos de capa de red, típicamente Frame Relay e X.25.

Debido a que las soluciones existentes de aquel entonces no eran compatibles surgió un gran interés por las redes privadas virtuales basadas en IP que funcionaran en la red de redes (Internet) y que utilizaran estándares que funcionaran a través de múltiles proveedores de servicios. De esta forma se consigue una mayor flexibilidad en el diseño e implantación con unos menores costes de gestión y provisión del servicio. La forma de conseguir VPN's IP es construyendo túneles IP de diversos modos.

El objetivo de un túnel IP es crear una asociación permanente entre dos extremos de modo que funcionalmente parezcan conectados. Se está utilizando una estructura no orientada a conexión para simular dichas conexiones.

El inconveniente de este tipo de soluciones es que:

- Están basadas en conexiones punto a punto.

- La configuración es manual: una nueva conexión supone alterar todas las configuraciones.

- Plantean problemas de crecimiento.

- La gestión de la QoS es posible pero costosa.

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

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

Las ventajas que ofrece MPLS para VPN’s IP son las siguientes

- Modelo acoplado frente al superpuesto.

- La provisión del servicio es sencilla.

- Es más fácilmente escalable.

- Se puede garantizar la QoS de los datos que entran en la VPN reservando los recursos necesarios para el túnel LSP.

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

CAPITULO III

RED MULTISERVICIO (RED CONVERGENTE)

3.1 EVOLUCIÓN A REDES NGN

El proceso de evolución ha sido largo y no siempre claro en sus objetivos finales. No obstante, en la actualidad aparece una tendencia clara hacia entornos convergentes basados en el modelo NGN. Por tal motivo es necesario establecer una comparación entre los modelos de red clásica y NGN que ayude a entender las ventajas que el modelo NGN aporta.

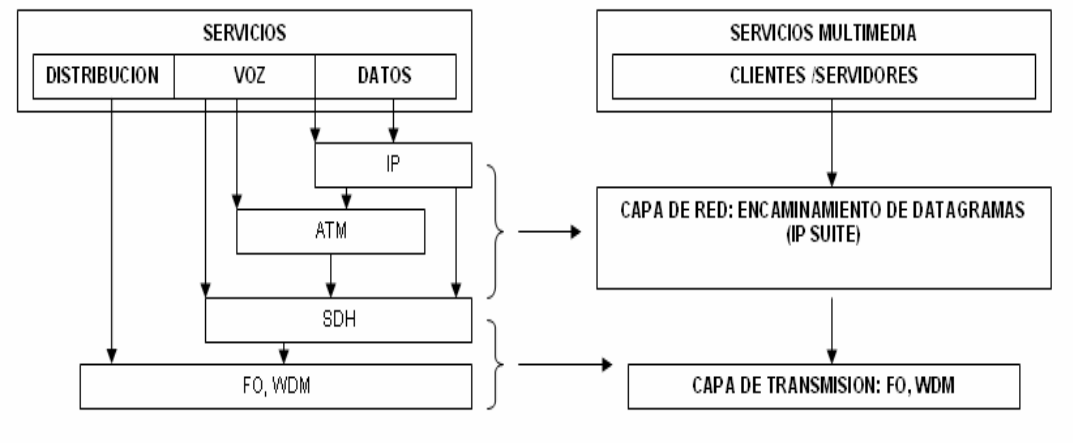


Figura 3.1: Modelos de Red Clásica Vs. NGN

La funcionalidad normalmente asignada a cada capa en una Red Clásica es:

• Capa FO/WDM: Física (trasmisión)

• Capa SDH: Agregación y protección.

• Capa ATM: Agregación, gestión de tráfico y calidad de servicio.

• Capa IP: Capa de Red, Encaminamiento de datagramas.

La funcionalidad normalmente asignada a cada capa en una Red de Nueva Generación sería:

• Capa FO/WDM: Capa física o de transmisión, agregación y protección.

• Capa de Red: Encaminamiento, agregación, gestión de tráfico, calidad de servicio y protección.

Previsiblemente el proceso de evolución se plantea en varias fases:

Comenzando por una evolución del núcleo de la red e irá extendiéndose de forma progresiva hacia el acceso. Este proceso se da con el fin de mantener las soluciones existentes mientras se produce la evolución, asegurando de esta manera un proceso poco traumático.

Conforme se extienda la implantación de la NGN hacia el acceso se podrá absorber la funcionalidad de las redes de acceso existentes, estando siempre sujeta a la discreción de

cada operador de red y siguiendo las pautas particulares que hayan sido establecidas en cada caso.

NGN debe permitir la evolución, migración en términos de sustitución o emulación de los actuales servicios de telecomunicación. La convergencia es imperativa en todos los aspectos: desde la convergencia de aplicaciones hasta la convergencia de infraestructuras.

3.1.1 Factores para el cambio

La aparición de un nuevo factor, en forma de libre competencia, motivó el que se intentara ampliar los servicios que brindaban cada operador sobre las infraestructuras existentes.
Es así que las redes se vieron en la necesidad de dar soporte a servicios para los que inicialmente no habían sido diseñadas, mostrando incapacidad de las redes existentes para proveer de forma óptima nuevos servicios. Comenzó así la búsqueda de mejores soluciones adaptadas al nuevo escenario.

Paralelo a lo anteriormente mencionado, se producía una evolución tecnológica en las redes de datos, motivada, principalmente, por una creciente necesidad de comunicación en entornos empresariales. Las primeras soluciones se desarrollaron en el estándar de comunicaciones ATM, aunque fue rápidamente absorbido, al menos en los entornos empresariales, por las soluciones nativas IP/Ethernet,[7] una vez que éstas alcanzaron los niveles de velocidad y funcionalidad requeridos.

[7] Ethernet/IP: protocolo de red en niveles para aplicaciones de automatización industrial. Basado en los protocolos estándar TCP/IP. El protocolo de red Ethernet/IP está basado en el Protocolo de Control e Información (Control and Information Protocol - CIP).

Pero un factor predominante que provocó una verdadera revolución en el sector de las telecomunicaciones, convirtiéndose en el definitivo detonante del cambio; fue la aparición y desarrollo del fenómeno Internet a escala global.

3.2 DESCRIPCIÓN RED MULTISERVICIOS

Las redes convergentes o redes de multiservicio hacen referencia a la integración de los servicios de voz, datos y video sobre una sola red basada en IP como protocolo de nivel de red.

Tradicionalmente, estos servicios se han ofrecido en forma separada sobre redes especializadas. En la gran mayoría de corporaciones, por ejemplo, la red de voz se basa en uno o varios PBX (private Branch eXchange) conectados a la PSTN (Public Switched Telephone Network) externa, mientras que la red de datos se basa en conmutadores y enrutadores IP (Internet Protocol) interconectando redes LAN (Local Area Network) y permitiendo el acceso a Internet. Sin embargo, cada vez es mayor la necesidad de una red única en la que tanto la voz como los datos y el video converjan naturalmente y permitan, además, reducir costos de administración, mantenimiento y manejo de la información, así como aumentar la productividad y disminuir los tiempos de atención a los clientes.

Aunque en un principio se consideró la posibilidad de integrar la red sobre el PBX y acceder a la ISDN, una característica fundamental de las redes de convergencia actuales y futuras es que los diferentes tipos de tráfico se soportan mediante protocolos basados en el concepto de conmutación de paquetes[8]. Por supuesto, ATM y Frame Relay son opciones

[8] Conmutación de paquetes: Técnica de conmutación que para hacer un uso eficiente de los enlaces físicos en una red de computadoras. El emisor divide los mensajes a enviar en un número arbitrario de paquetes del mismo tamaño, donde adjunta una cabecera y la dirección origen y destino así como datos de control que luego serán transmitidos por diferentes medios de conexión entre nodos temporales hasta llegar a su destino.

importantes para considerar como fundamento de las redes de convergencia, pero dada la actual y creciente ubicuidad de Internet y las modificaciones que la IETF está introduciendo en las nuevas versiones de IP para atender tráfico de tiempo real con una adecuada calidad de servicio y la conmutación de etiquetas en MPLS, el protocolo dominante en el desarrollo actual de las redes de convergencia es IP.

En efecto, la aplicación del protocolo IP para la transmisión integrada de voz y datos es un concepto que ha revolucionado a la industria de las telecomunicaciones, elevando la posición de la Internet a un plano de competencia comercial. Sobre la Internet ya se pueden ofrecer servicios de transmisión de voz, a precios muy inferiores a los tradicionales, gracias al desarrollo de aplicaciones de tiempo real sobre IP.

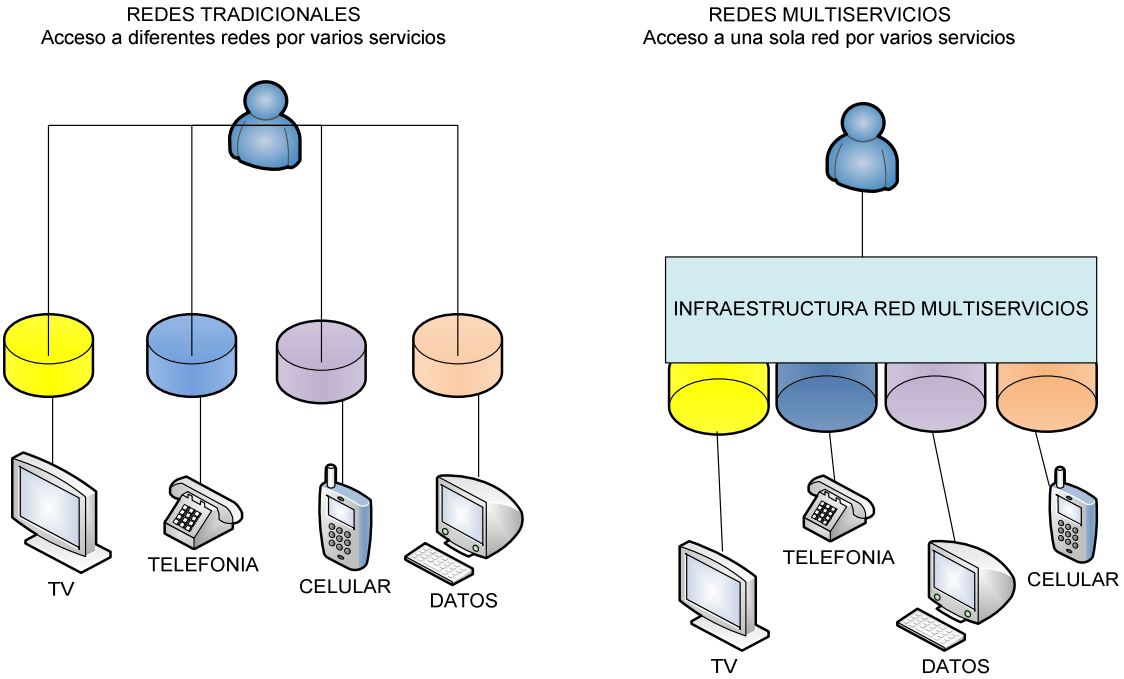


Figura 3.2 Descripción de una red multiservicios

Por supuesto, las redes de convergencia han tenido y tendrán aún dificultades técnicas que superar ya que los distintos servicios por ofrecer tienen diferentes características y requerimientos de red. Por ejemplo, los datos se presentan en ráfagas que consumen grandes volúmenes de ancho de banda durante cortos intervalos de tiempo, mientras que el tráfico de voz requiere un ancho de banda constante y un bajo retardo de transmisión.

Estas demandas del tráfico de voz han sido satisfechas mediante conmutación de circuitos basada en multiplexaje por división de tiempo (TDM), mientras que el tráfico de datos ha sido satisfecho por las redes de conmutación de paquetes. Sin embargo, la existencia de dos redes independientes implica procesos de mantenimiento y administración independientes, con el correspondiente incremento en costos y la dificultad para dar respuesta oportuna a los requerimientos de servicio de los clientes.

Adicionalmente, el tráfico de datos no sólo ya es mayor al tráfico de voz sino que el primero crece exponencialmente mientras que el segundo lo hace linealmente. Esta situación contrasta con el hecho de que las principales ganancias económicas de las empresas de telecomunicaciones provienen en su gran mayoría del tráfico de voz, generando un interés especial en la integración de voz sobre la infraestructura ya existente, lo cual permitiría mejores servicios a sus clientes y mayores ingresos para las empresas.

Así pues, desde la perspectiva de los proveedores de servicios de comunicación, es de fundamental importancia introducir nuevos servicios en respuesta a las necesidades de sus clientes para poder adquirir y mantener una porción del mercado. Y desde la perspectiva de los fabricantes de equipos, esta condición les exige la rápida innovación de sus equipos y sistemas.

Es en estas condiciones es donde las redes de convergencia basadas en IP adquieren su importancia. A diferencia de los modelos de servicios integrados anteriores, las redes de convergencia basadas en IP permiten aprovechar las habilidades de los desarrolladores de aplicaciones de la Internet en la innovación y desarrollo de nuevos productos, reduciendo significativamente el tiempo de introducción al mercado. Más aún, como los fabricantes no pueden construir todas sus soluciones "desde cero", deben recurrir al outsourcing y, para que este sea efectivo, las soluciones deben basarse en estándares abiertos, de manera que los diferentes equipos y redes puedan interoperar.

Estas condiciones no sólo se presentan en redes alambradas sino en redes móviles inalámbricas, donde el advenimiento de la tercera generación implica la transición de la conmutación de circuitos [9]a la conmutación de paquetes para convergencia de servicios.
Y en este esfuerzo también se conduce al uso de voz y video "paquetizada" y a la aplicación de IP a través de toda la red.

A través de las redes multiservicios, una compañía puede reinventar tanto sus redes de comunicaciones como toda su organización. Las redes multiservicios apoyan aplicaciones vitales para estructurar el negocio Telefonía IP, videoconferencia en colaboración y Administración de Relaciones con el Cliente que contribuyen a que la empresa sea más eficiente, efectiva y ágil con sus clientes.

Dentro de los motivos más importantes que podemos destacar para la migración a redes Multiservicios están:

[9] Es aquella en la que los equipos de conmutación deben establecer un camino físico entre los medios de comunicación previa a la conexión entre los usuarios. Este camino permanece activo durante la comunicación entre los usuarios, liberándose al terminar la comunicación.

- La reducción de costos.

- La mejora en la comunicación y productividad de los empleados.

- La posibilidad de implementar aplicaciones novedosas que permitan una comunicación más flexible y estrecha con los clientes de la organización.

3.3 CARACTERÍSTICAS PRINCIPALES DE LAS REDES MULTISERVICIOS.

- Red Capaz de manejar voz, datos y video.

- Red con las capas de aplicaciones, control y transporte formalmente separadas.

- Red con interfaces abiertas entre el transporte, el control y las aplicaciones.

- Red que usa la conmutación de paquetes para transportar todo tipo de información.

- Red con Calidad de Servicio garantizada para distintos tipos de tráfico.

- Red que permite la ubicuidad de los servicios.

- Red que permite el acceso irrestricto por parte de los usuarios a cualquier proveedor de servicios.

- La NGN provee infraestructuras para la creación, desarrollo y gestión de toda clase de servicios actuales y futuros, distinguiendo y separando los servicios y las redes de transporte; es decir posee una arquitectura de red horizontal basada en una división transparente de los planos de transporte, control y aplicación.

- El plano de transporte se basa en tecnología de conmutación de paquetes IP/MPLS.

- Migración de las redes actuales (PSTN, ISDN y otras) a NGN, a través de interfaces abiertos y protocolos estándares.

- Escalabilidad de la infraestructura de red; esto implica permitir la ampliación de la red de acuerdo a las necesidades, teniendo en cuenta la cantidad de usuarios y la variedad de servicios a ofrecer en cada etapa de su desarrollo.

- Soporte de servicios de diferente naturaleza: tiempo real y no real, streaming[10], servicios multimedia (voz, video, texto).

- Soporte para múltiples tecnologías de última milla.

- Su arquitectura funcional soporta la conexión a red basada en tres modos de conmutación: de circuitos, de paquetes y de paquetes si conexión.

- Flexibilidad para distribuir solo los servicios que el usuario requiera, en cualquier combinación.

- Simplificar al máximo la administración, el mantenimiento y la distribución de los servicios.

- Configuraciones redundantes para asegurar alta tasa de disponibilidad de los servicios.

[10] Streaming es una nueva tecnología para Internet que permite transmitir de forma eficiente audio y vídeo a través de la Red sin necesidad de descargar los archivos en el disco duro del ordenador de usuario.

- Capacidad de banda ancha con calidad de servicios (QoS), garantizada de extremo a extremo.

- Seguridad.

- Acceso Universal.

- Ahorros en mantenimiento y consumo de energía.

- Posibilitar la distribución simultanea de diferentes servicios, como telefonía, televisión, acceso a Internet, datos y otros servicios de valor agregado.

3.4 EJEMPLO DE CONVERGENCIA BASADA EN IP

La integración de voz y datos en una misma red significa que la infraestructura debe ser multiservicio, es decir, que soporte diferentes tipos de tráfico con diferentes requerimientos en cuanto a la calidad de servicio se refiere. Por tanto, es importante tener en cuenta que la infraestructura de este tipo de red de nueva generación debe tener dos características fundamentales que son la flexibilidad y la habilidad para reaccionar a los cambios del trafico, de tal manera que se puedan prestar servicios en tiempo real y garantizar los requerimientos de calidad pactados, tales como ancho de banda, retardo y pérdida de paquetes, entre otros.

MPLS permite tener estas dos características que requieren las redes convergentes, gracias a su mecanismo de ingeniería de tráfico. Con estos mecanismos la red tiene la posibilidad de controlar en forma dinámica el flujo de datos, optimizar la utilización de los recursos disponibles, seleccionar rutas para el tráfico, de acuerdo con la carga y el estado de la red y mover flujos de tráfico a caminos menos congestionados.

La clave para las redes de convergencia basadas en IP es la división de las principales funciones de red en componentes lógicos que pueden implementarse en equipos de propósito específico. Así se pueden construir soluciones escalables e interoperables para satisfacer las diferentes necesidades de los distintos proveedores de servicios a bajo costo y permitiendo que los mismos servicios se puedan ofrecer uniformemente a lo largo de toda la red. De esta manera los proveedores pueden acelerar el desarrollo de sus soluciones mediante la adquisición de elementos de red estándar. La competencia entre fabricantes de equipos se promueve a través de estos estándares abiertos; la separación de los elementos de control y de multimedios permite el rápido desarrollo de nuevas aplicaciones, etc.

Como se puede observar en la Figura la red de IP administrada con MPLS, proporciona gateways para cada diferente función, incluyendo redes inalámbricas y acceso a la PSTN tradicional.

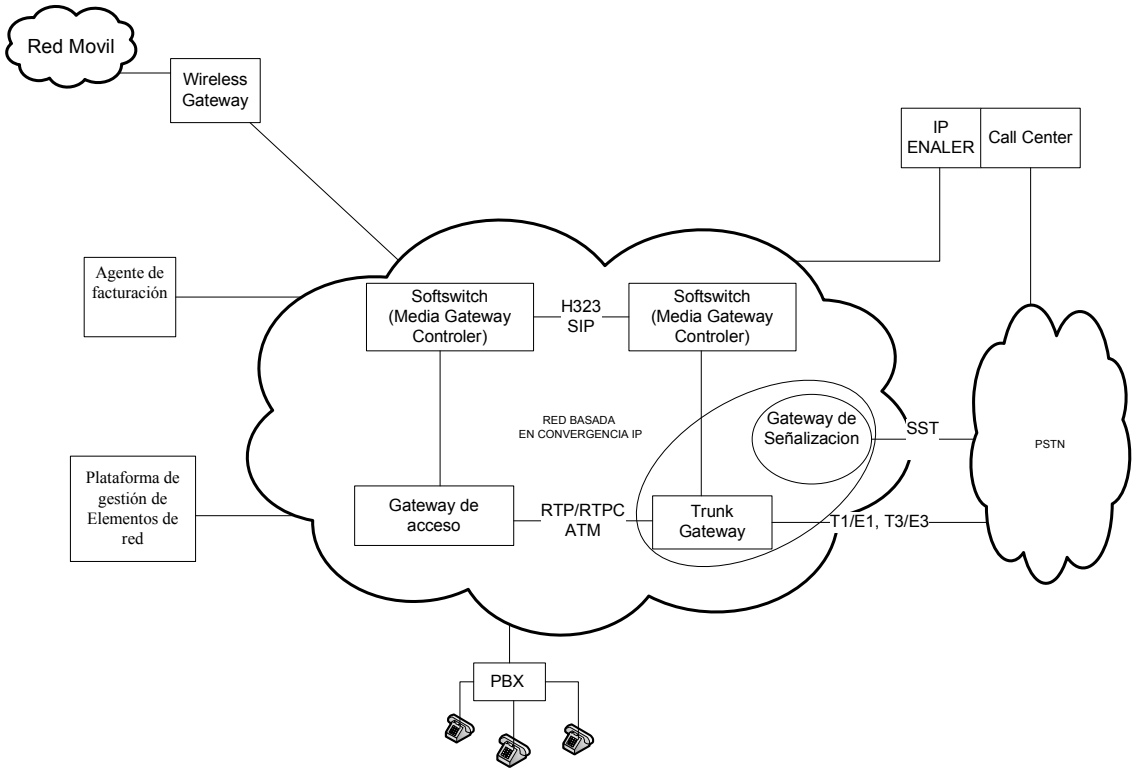


Figura 3.3: Red Basada en convergencia IP

3.5 ELEMENTOS Y PROTOCOLOS EN UNA RED DE CONVERGENCIA.

3.5.1 Softswitch

Es el nombre genérico para un nuevo sistema de telefonía que ha evolucionado hasta la transmisión de voz mediante redes de conmutación de paquetes (IP).

Es el dispositivo más importante en la capa de control dentro de una arquitectura NGN, que se encarga del control de llamada (señalización y gestión de servicios), procesamiento de llamadas, y otros servicios, sobre una red de conmutación de paquetes (IP).

El softswitch opera como administrador, al interconectar redes de telefonía fija, con las redes de conmutación de paquetes (IP), siendo su objetivo principal brindar una confiabilidad y calidad de servicio, igual o incluso mejor a la que brinda una red de conmutación de circuitos, con precios más bajos.

El softswitch trabaja con estándares abiertos para integrar las redes de próxima generación con la capacidad de transportar voz, datos y multimedia, sobre redes IP.

Las diferentes versiones del softswitch dependen del protocolo que se vaya a utilizar en la red, como por ejemplo: Proxy o elemento de registro en el protocolo SIP o como el Gatekeeper en H.323, Media Gateway Controller (MGC) en MEGACO, etc.

3.5.1.1 Características del Softswitch

Permite el control de servicios de conexión asociados a las pasarelas multimedia (Media Gateways) y los puntos terminales que utilizan IP como protocolo nativo.

- Capacidad de proveer sobre la red IP un sistema telefónico tradicional, confiable y de alta calidad en todo momento.

- Selección de procesos en cada llamada.

- El enrutamiento de las llamadas en función de la señalización y de la información almacenada en la base de datos de los clientes.

- La capacidad para transferir el control de una llamada a otro elemento de red. Interfaces con funciones de gestión como los sistemas de facturación y provisión.

- Coexistencia con las redes tradicionales de conmutación.

- Soporte de servicios como: Voz, Fax, vídeo, datos y nuevos servicios que serán ofrecidos en el futuro.

- Los dispositivos finales pueden ser; teléfonos tradicionales, teléfonos IP, computadores, beepers, terminales de video conferencia, etc.

- Separar el software del hardware en una red, lo que implica libertad en la elección de productos de distintos fabricantes en todas las capas de la red. Bajo Costo de desarrollo.

- Mejora los servicios para el cliente, lo que facilita su rápido ingreso al mercado. Mensajería unificada que brinda facilidades para que los usuarios recuperen, respondan y administren todos sus mensajes de voz, llamadas telefónicas, el correo electrónico y los faxes, independientemente del horario, ubicación o dispositivo, todo bajo una misma interfaz.

- Flexibilidad al soportar el desarrollo de equipos de telefonía de gran nivel.

- Mejores ingresos para los proveedores de servicios y operadores.

3.5.1.2 Arquitectura del Softswitch

Un softswitch puede estar compuesto por uno o más componentes, es decir sus funciones se pueden desarrollar en un sistema o a través de varios sistemas.

3.5.1.3 Elementos de un Softswitch

Gateway Controller (Controlador de Pasarela)

También llamado Call Agent, es el centro operativo del softswitch, mantiene las normas para el procesamiento de llamadas, comunicándose con otras partes del Softswitch, y componentes externos utilizando diferentes protocolos.
Es responsable del manejo del tráfico de Voz y datos a través de varias redes.

Las principales funciones del Gateway Controller son:

- Control de llamadas.
- Protocolos de establecimiento de llamadas: H.323, SIP
- Protocolos de Control de Medios: MGCP, MEGACO H.248
- Control sobre la Calidad y Clase de Servicio.
- Protocolo de Control SS7: SIGTRAN (SS7 sobre IP).
- Procesamiento SS7 cuando usa SIGTRAN.
- Enrutamiento de llamadas.
- Detalle de las llamadas para facturación.
- Manejo del Ancho de Banda.

Signalling Gateway (Pasarela de Señalización)

Sirve como puente entre la red de señalización SS7 y la red IP bajo el control del Gateway Controller. Es el responsable de ejecutar el establecimiento y desconexión de la llamada.

Las principales funciones del Signaling Gateway son:

- Proveer conectividad física para la red SS7 vía T1/E1 o T1/V.35.
- Capaz de Transportar información SS7 entre el Gateway Controller y el Signaling Gateway a través de IP.
- Proporciona una ruta de transmisión para la voz y opcionalmente para los datos.
- Alta disponibilidad de operación para servicios de telecomunicaciones.

3.5.1.4 Media Gateway (Pasarela de medios)

El media gateway proporciona el transporte de voz, datos, fax y vídeo entre la Red IP y la red PSTN. El componente más básico que posee el media Gateway es el DSP (digital signal processor) que se encarga de las funciones de conversión de analógico a digital, los códigos de compresión de audio y video, cancelación del eco, detección del silencio, la señal de salida de DTMF11, y su función más importante es transformar la voz en paquetes para poder ser comprendidos por la red IP.

Las principales funciones y características del Media Gateway son:

- Transmisión de paquetes de voz empleando RTP como protocolo de transmisión.

- Posee una entrada y salida de datos alta, la cual puede aumentar a medida que la red aumente su tamaño, por lo tanto debe poseer la característica de ser escalable, en puertos, tarjetas, nodos externos y otros componentes del softswitch.

- Tiene un Interfaz Ethernet12 y algunos poseen redundancia.

3.5.1.5 Media Server (Servidor de Medios)

Mejora las características funcionales del Softswitch, contiene las aplicaciones de procesamiento del medio, esto significa que soporta un alto funcionamiento del hardware del DSP.

Un media server no es estrictamente requerido como parte de las funciones del switch.

Las principales funciones del Media Server son:

- Funcionalidad básica de voicemail.

- Integrar fax y mail box, notificando por e-mail o pre grabación de los mensajes.

- Capacidad de videoconferencia.

- Speech-to-text, el cual se basa en el envío de texto a las cuentas de email de las personas o a los beeper usando entradas de voz.

- Speech-to-Web, es una aplicación que transforma palabras claves en códigos de texto los cuales pueden ser usados en el acceso a la Web.

- Unificación de los mensajes de lectura para voice, fax y e-mail por un interfaz Ethernet.

- Fax-over-IP (Fax sobre IP).

3.5.1.6 Feature Server (Servidor de Capacidades)

Controla los datos para la generación de la facturación, usa los recursos y los servicios localizados en los componentes del softswitch.

Se define como una aplicación a nivel de servidor que hospeda un conjunto de servicios de valor agregado que pueden ser parte de CALL AGENT o no. Las aplicaciones se comunican con el CALL AGENT a través de los protocolos SIP, H.323, etc.

Servicio 1-800: Provee un bajo costo para los altos niveles de llamadas de entrada. La translación del número 800 a un número telefónico es proporcionada por la base de datos. El usuario que recibe la llamada al 800 paga el costo de la misma.

Servicios 1-900: Provee servicios de información, contestación de la llamada, sondeos de opinión pública. El que origina la llamada paga la misma.

GateKeeper que provee servicios de enrutamiento de llamada para cada punto final, puede proveer facturación y control del ancho de Banda para el Softswitch.

Tarjeta de Servicios para llamadas, que permite a un usuario acceder a un servicio de larga distancia por medio de un teléfono tradicional. La Facturación, autenticación PIN y el soporte de enrutamiento son proporcionados en el servicio.
Autorización de llamada: Este servicio establece redes virtuales VPN usando autorización PIN.

Llamadas en espera, transferencia de llamadas, Correo de Voz y búsqueda, marcado automático, identificador de llamada, Velocidad de marcado.
Centralización de llamadas.

3.5.1.7 El Access Media Gateway (AMG)

El AMG es una clase superior de Media Gateway, y es importante porque reemplazan las tarjetas de línea TDM de los switches.

Hay varios subtipos de Access Media Gateways, mostrando diferentes acercamientos a las redes de telecomunicaciones. Un subtipo muy importante son las Pasarelas de Acceso Multiservicio MSAG (Multiservice Access Gateway), también conocida como Nodos de Acceso Multiservicio MSANs (Multiservice Access Nodes), Los cuales brindan servicios de banda ancha y Triple Play, soportando una migración fluida a tecnologías NGN.

El AMG también realiza labores de compresión y descompresión de señales de voz, por lo que requiere potencia de procesamiento.

Terminales de los Usuarios

Las interfaces de usuario final, son físicas y funcionales (control). No se han hecho estimaciones respecto a la diversidad de las interfaces de usuarios y de las redes de usuarios que podrían conectarse a la red de acceso de la NGN.

Todas las categorías de equipos de usuarios son soportadas por la NGN, desde los sencillos aparatos telefónicos convencionales hasta las complejas redes corporativas. El equipo de usuario final puede ser fijo o móvil.

Los Terminales son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware.

Software son las aplicaciones o programas que permiten la comunicación vía Internet, pueden ser usadas simplemente a través de un computador o PC con el respectivo micrófono y los parlantes del mismo, proporcionando la misma experiencia que una llamada telefónica tradicional.

Hardware se refiere a una amplia variedad de equipos terminales de usuario y básicamente a los Teléfonos IP, que permiten realizar llamadas telefónicas vía Internet. El concepto más elemental para explicarlo sería decir que las señales de voz son convertidas en paquetes de información digital que son luego transmitidos a través del protocolo IP (Internet.)

El teléfono IP está basado en el estándar ITU H.323 para VoIP. El software consiste de los siguientes grandes subsistemas: Interfaz de usuario, Procesamiento de Voz, Telephony Signaling Gateway, Protocolos de interfaz de Red, Agente administrador de Red, y servicios del sistema

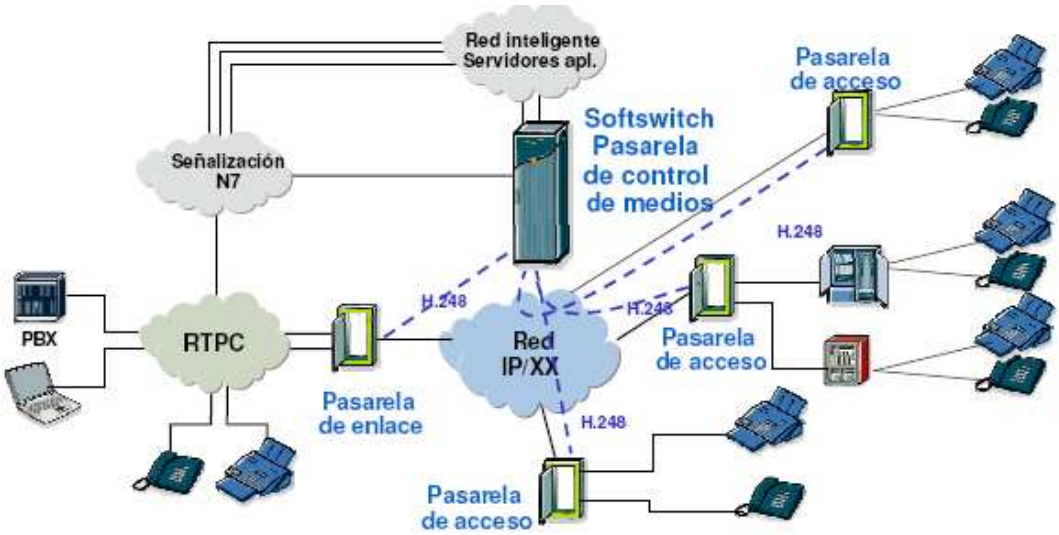


Imagen 3.4 Arquitectura NGN

3.6 PROTOCOLOS UTILIZADOS EN NGN

3.6.1 PROTOCOLO SIP

SIP (Session Initiation Protocol) es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet.

.

Es utilizado en VoIP, gateways, teléfonos IP, softswitches, aunque también se utiliza en aplicaciones de video, notificación de eventos, mensajería instantánea, juegos interactivos.

3.6.1.1 Características de SIP

Usando SIP es posible implementar servicios telefónicos básicos y avanzados (voz, datos y video) sobre redes IP.

Empleando Gateways, soporta comunicaciones entre usuarios de redes IP y también con usuarios de otras redes, incluyendo las redes telefónicas convencionales (PSTN).

SIP es un protocolo de capa de aplicación independiente de los protocolos de las capas inferiores por lo que puede ser soportado sobre TCP (Transmision Control Protocol), UDP (User Datagram Protocol), igualmente sobre IP o ATM.

El SIP ofrece todas las potencialidades y las características comunes de la telefonía de Internet como:

- Llamada o transferencia de medios.
- Conferencia de llamada.
- Llamada en espera.

Puesto que SIP es un protocolo flexible, es posible agregar más características y mantener la interoperabilidad hacia atrás.

El protocolo SIP se aplica para sesiones punto-a-punto únicas. Puede ser usado para enviar una invitación a participar en una conferencia multicast.

Utiliza el modelo cliente-servidor y se adapta para las aplicaciones de Telefonía-IP. El servidor puede actuar en modo proxy o redirect (se direcciona el requerimiento de llamada a un servidor apropiado).

3.6.1.2 Llamadas y Transacciones SIP

El protocolo SIP define varios métodos para realizar una llamada o transacción.

- método SIP invite : Sirve para iniciar las sesiones.
- método SIP ack: Confirma el establecimiento de la llamada.
- método SIP Bye: Termina una sesión.
- método SIP Cancel: Cancela una invitación pendiente.
- método SIP Register: registra una localización con un servidor Registrar SIP
- método SIP re-invite : Cambia una sesion actual
- método SIP Options

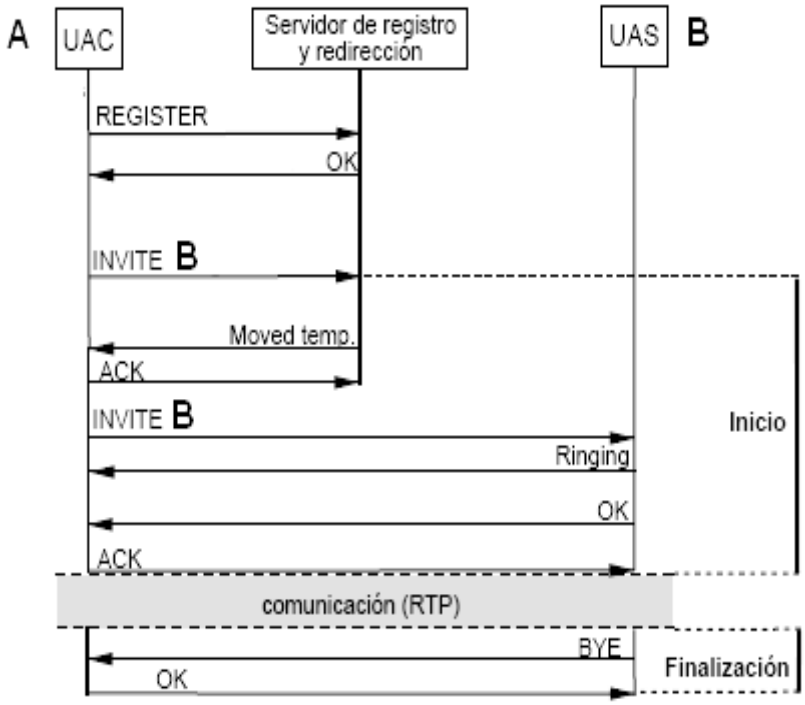


Figura 3.5: Llamada SIP

Las invitaciones de SIP son usadas para crear sesiones y llevar las descripciones de la sesión que permitan que los participantes acuerden un sistema de medios compatibles. El SIP hace uso de elementos llamados Servidores Proxy; con el fin de permitir el acceso a Internet a todos los equipos de una organización cuando solo se puede disponer de un único equipo conectado, esto es, una única dirección IP. El SIP también proporciona una función de registro que permite que los usuarios indiquen sus localizaciones actuales para ser usadas por los servidores Proxy. SIP funciona por encima de diversos protocolos del transporte.

3.6.1.3 Términos y definiciones SIP

UAC (User Agent Client)

El Agente de Usuario Cliente es una aplicación cliente en un sistema SIP que inicia la petición SIP que se envía al UAS. La combinación del UAC y del UAS se llama SIP User Agent (agente de usuario SIP). El agente de usuario SIP permite que las llamadas peer-to-peer sean hechas usando un protocolo cliente/servidor.

UAS (User Agent Server).

El Agente de Usuario Servidor es una aplicación servidor dentro de un sistema SIP que acepta las peticiones de un UAC y genera una respuesta accept, reject o redirect de parte del usuario.

SIP Outbound Proxy: Proxy de salida

Es un Proxy que recibe peticiones de un cliente, aunque puede no ser el servidor resuelto por el Request-URI, que determina el URI de la solicitud.

El Proxy de salida (outbound) es un proxy normal. Una persona puede configurar su cliente, el teléfono o el software, para utilizar el proxy para todas las sesiones SIP, así

como cuando se configura un web browser para utilizar un proxy web para navegar todas las páginas web. En algunos casos, el proxy de salida se pone junto al firewall y es la única manera de dejar pasar el trafico SIP de la red interna a Internet.

SIP Proxy

Es una entidad intermediaria que actúa como servidor y cliente con el fin de hacer peticiones a nombre de otros clientes. Un proxy server desempeña sobre todo el papel del encaminamiento, que significa que su trabajo es asegurarse de que la petición sea enviada a otra entidad "más cercana" al usuario apuntado. Los proxys son también útiles para hacer cumplir las políticas (por ejemplo, cerciorarse que un usuario pueda hacer una llamada). Un proxy interpreta, y, en caso de necesidad, reescribe partes específicas de un mensaje antes de enviarlo.

Los proxys SIP son los elementos que encaminan peticiones SIP a los UAS y respuestas SIP a los UAC.

SIP Redirect Server

Es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor.

SIP Registrar Server

Es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla.

SIP URI

Un SIP URI es el esquema de direccionamiento SIP para llamar a otra persona vía SIP. En otras palabras, un SIP URI es un numero telefónico SIP de un usuario.

3.6.2 Protocolo H.323

H.323 fue diseñado con el objetivo de proveer a los usuarios tele-conferencias teniendo, capacidades de voz, video y datos sobre redes de conmutación de paquetes.

H.323 establece los estándares para la compresión y descompresión de audio y video, asegurando que los equipos de distintos fabricantes se intercomuniquen.

También H.323 hace uso de los procedimientos de señalización de los canales lógicos, en los que el contenido de cada uno de los canales se define cuando se abre. Estos procedimientos se proporcionan para fijar las prestaciones del emisor y receptor, el establecimiento de la llamada, intercambio de información, terminación de la llamada y como se codifica y decodifica. Un punto importante es que se deben determinar las capacidades de los sistemas, de forma que no se permita la transmisión de datos si no pueden ser gestionados por el receptor.

3.6.2.1 Componentes principales

Terminal

Un terminal H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la

especificación, un terminal H.323 puede proporcionar solo voz, voz y datos, voz y video, o voz, datos y video.

Un terminal H.323 consta de las interfaces del equipo de usuario, el codec de video, el codec de audio, el equipo telemático, la capa H.225, las funciones de control del sistema y la interfaz con la red por paquetes.

GateWay

Un gateway H.323 es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. En general, el propósito del gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa.

Gatekeeper

El gatekeeper es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs. El gatekeeper puede también ofrecer otros servicios a los terminales, gateways y MCUs, tales como gestión del ancho de banda y localización de los gateways.

El Gatekeeper realiza dos funciones de control de llamadas que preservan la integridad de la red corporativa de datos. La primera es la traslación de direcciones de los terminales de la LAN a las correspondientes IP o IPX. La segunda es la gestión del ancho de banda, fijando el numero de conferencias que pueden estar dándose simultáneamente en la LAN y rechazando las nuevas peticiones por encima del nivel establecido, de tal manera que se garantice ancho de banda suficiente para las aplicaciones de datos sobre la LAN.

Unidad de Control Multipunto

Está diseñada para soportar la conferencia entre tres o más puntos, bajo el estándar H.323, llevando la negociación entre terminales para determinar las capacidades comunes para el proceso de audio y video y controlar la multidifusión[11].

Controlador Multipunto

Es un componente de H.323 que provee capacidad de negociación con todos los terminales para llevar a cabo comunicaciones. También puede controlar recursos de conferencia tales como multicasting de video.

Procesador Multipunto

Es un componente de H.323 de hardware y software especializado, mezcla, conmuta y procesa el audio, video y / o flujo de datos para los participantes de una conferencia multipunto de tal forma que los procesadores del terminal no sean masivamente utilizados. El procesador multipunto puede procesar un flujo medio único o flujos medio múltiples dependiendo de la conferencia soportada.

[11] **Multidifusión** (multicast) es el envío de la información en una red a múltiples destinos simultáneamente.

Proxy H.323

Es un servidor que provee a los usuarios acceso a redes seguras de unas a otras confiando en la información. El Proxy H.323 se comporta como dos puntos remotos H.323 que envían mensajes e información en tiempo real a un destino; con firewall.

3.6.2.2 Pila de protocolos H.3.23

A continuación se explica de una manera breve los protocolos más significativos para H.323:

RTP/RTCP(Real-Time Transport Protocol / Real-Time Transport Control Protocol)

Protocolos de transporte en tiempo real que proporcionan servicios de entrega punto a punto de datos.

RAS (Registration, Admission and Status)

Sirve para registrar, control de admisión, control del ancho de banda, estado y desconexión de los participantes.

H225.0

Protocolo de control de llamada que permite establecer una conexión y una desconexión.

H.245

Protocolo de control usado en el establecimiento y control de una llamada.

En concreto presenta las siguientes funcionalidades:

- Intercambio de capacidades: Los terminales definen los codecs de los que disponen y se lo comunican al otro extremo de la comunicación.
- Apertura y cierre de canales lógicos: Los canales de audio y video H.323 son punto a punto y unidireccionales. Por lo tanto, en función de las capacidades negociadas, se tendrán que crear como mínimo dos de estos canales. Esto es responsabilidad de H.245.

- Control de flujo cuando ocurre algún tipo de problema.

- Multitud de otras pequeñas funciones.

Q.931 (Digital Subscriber Signalling) Este protocolo se define para la señalización de accesos RDSI básico.

RSVP (Resource ReSerVation Protocol): Protocolo de reserva de recursos en la red para cada flujo de información de usuario.

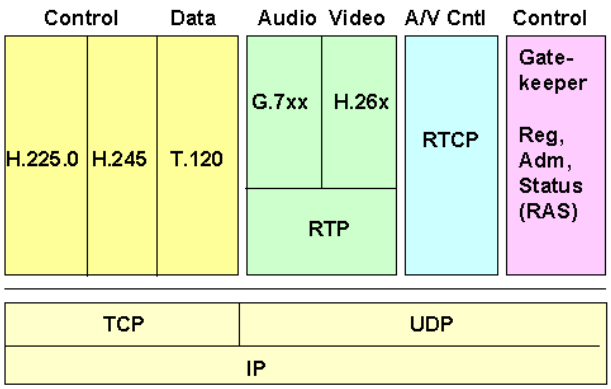


Figura 3.6: Pila de Protocolos H.323

3.6.2.3 Señalización

La función de señalización está basada en la recomendación H.225, que especifica el uso y soporte de mensajes de señalización Q.931/Q932. Las llamadas son enviadas sobre TCP por el puerto 1720. Sobre este puerto se inician los mensajes de control de llamada Q.931 entre dos terminales para la conexión, mantenimiento y desconexión de llamadas.
Los mensajes mas comunes de Q.931/Q.932 usados como mensajes de señalización H.323 son:
Setup. Es enviado para iniciar una llamada H.323, para establecer una conexión con una entidad H.323. Entre la información que contiene el mensaje se encuentra la dirección IP, puerto y alias del llamante o la dirección IP y puerto del llamado.

Call Proceeding. Enviado por el Gatekeeper a un terminal advirtiendo del intento de establecer una llamada una vez analizado el número llamado.

Alerting. Indica el inicio de la fase de generación de tono.

Connect. Indica el comienzo de la conexión.

Release Complete. Enviado por el terminal para iniciar la desconexión.
Facility. Es un mensaje usado como petición o reconocimiento de un servicio suplementario.

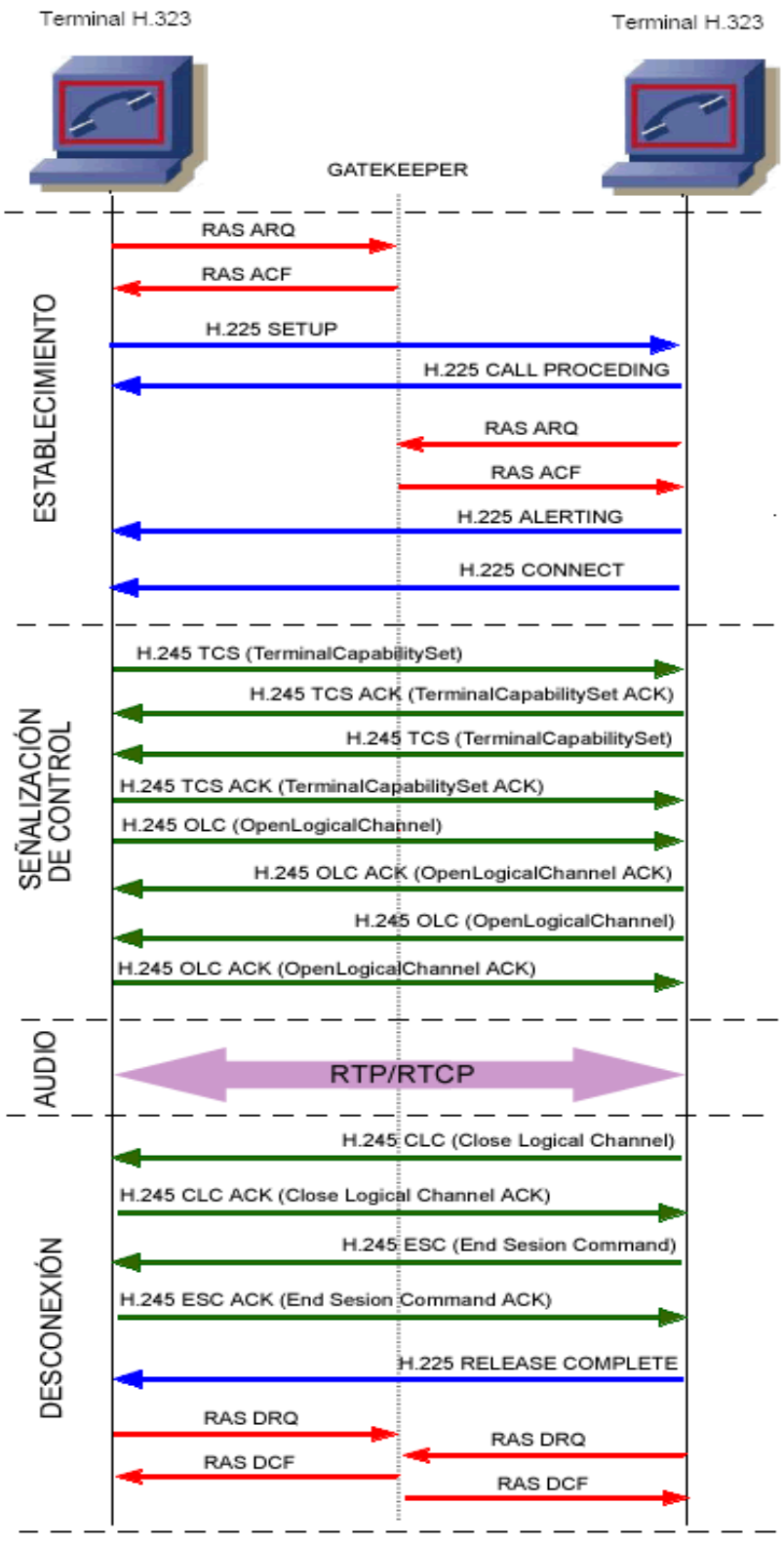


Figura 3.7 Señalizacion H323

3.6.3 MEGACO/H.248

MEGACO, H.248 es un complemento a los protocolos H.323 y SIP: se utilizara para controlar los Media Gateways y el H.323 o SIP para comunicarse con otro controlador Media Gateway.

3.6.3.1 Componentes y funcionamiento de una llamada con H.248

Media Gateway Controller (MGC): Que controla a los Media Gateways para una buena gestión en el intercambio de información a través del protocolo MGCP. El MGC también se suele llamar Call Agent.

Media Gateway son capaces de mantener comunicaciones tanto con el H.323 como con el SIP, algo fundamental para la óptima implantación del sistema VoIP.

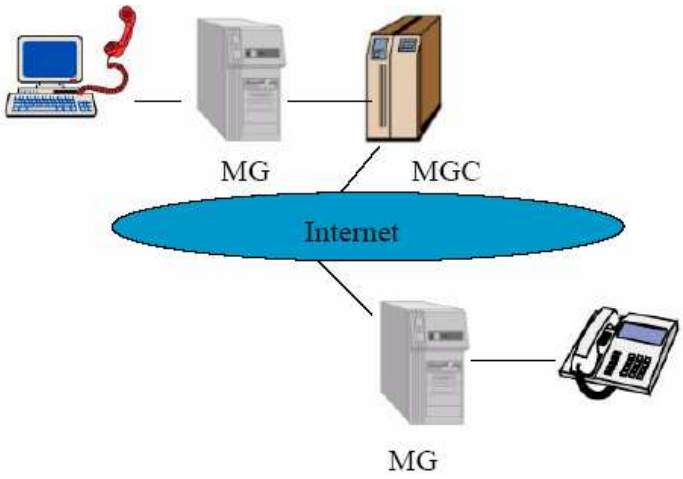


Figura 3.8 Componentes MEGACO

La comunicación, puede realizarse a través de un ordenador con un altavoz y un micrófono, o por medio de un teléfono analógico. Si un usuario desea realizar una llamada, mediante este sistema, los pasos que se siguen son:

1. El usuario descuelga el teléfono y marca el número de teléfono del destinatario. Esta llamada, le llega al Media Gateway.

2. El Media Gateway, notifica al Media Gateway Controller de que una llamada está en camino.

3. El Media Gateway Controller busca en su base de datos, el número de teléfono del destinatario para saber su IP y su número de puerto. Entonces, busca el Media Gateway del destinatario, y le envía un mensaje para indicarle que le está llegando una llamada.

4. El Media Gateway del destinatario, abre una RTP (Protocolo en tiempo real) cuando el usuario descuelga.

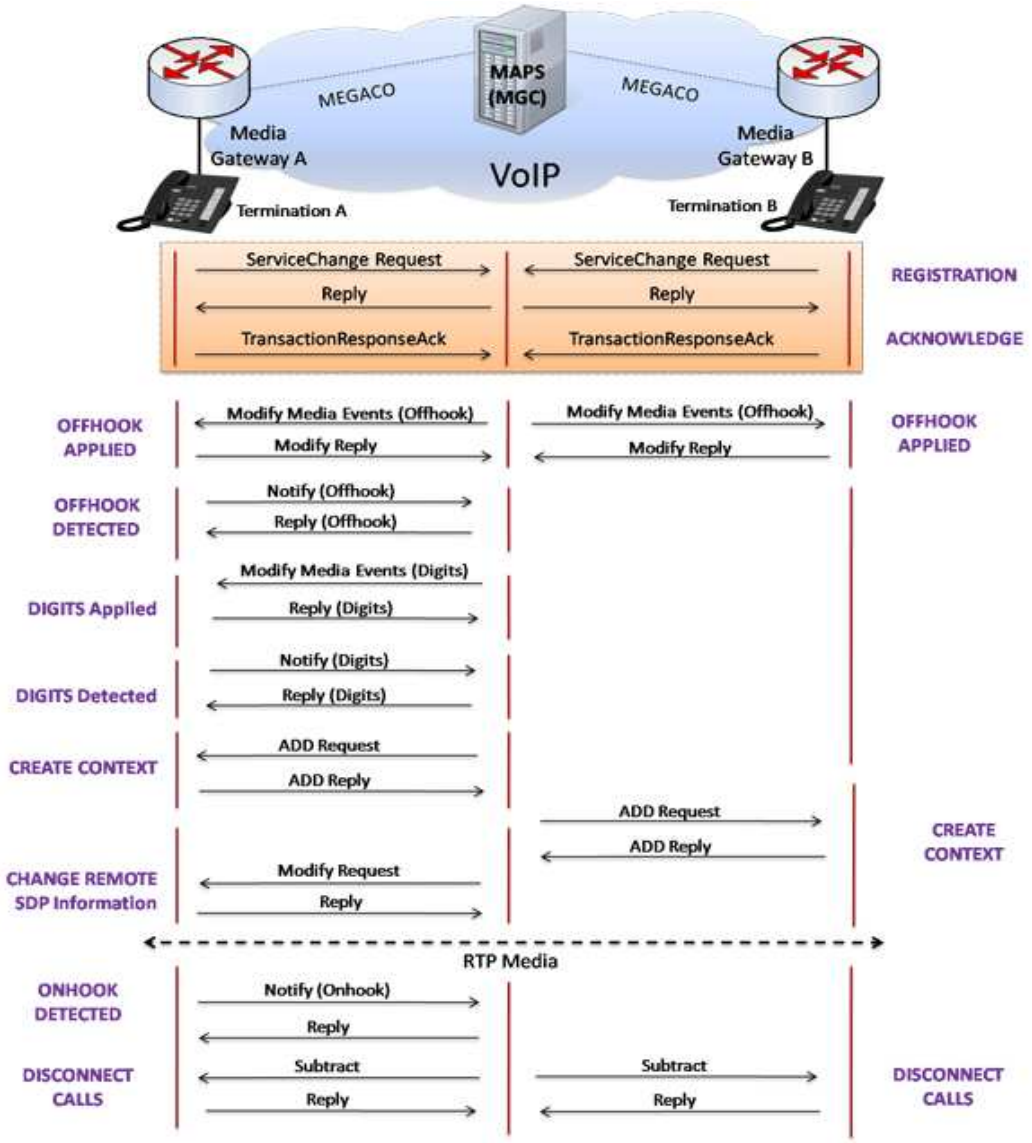


Figura 3.9 Llamada de H.248

RTP Y RTCP para el transporte de voz y video

RTP provee funciones de transporte de red extremo a extremo apropiadas para aplicaciones de transmisión de datos en tiempo real. El transporte de datos esta acompañado por un protocolo de control (RTCP) que permite monitorear la entrega de datos. RTP y RTCP están diseñados para ser independientes de las subcapas de transporte y de las capas de red.

Características

- Temporización
- Detección de perdidas
- Etiquetado de contenidos
- Realimentación
- Estimación de Miembros y detección de Bucles
- No son responsables de las tareas de alto nivel como:
    - Sincronización
    - Recuperación de paquetes perdidos
    - Control de congestión

Funcionamiento:

Se establece una sesión RTP separada para cada tipo de datos transportado.
Paquetes RTCP informan la calidad de recepción para esa sesión.
Para hacer frente al retardo introducido por la red se implementa un mecanismo llamado TimeStamping.

El emisor establece el TimeStamp según el instante en que se muestrea el primer octeto en el paquete. El receptor después de recibir los paquetes de datos utiliza el TimeStamp para reconstruir el tiempo original.

3.6.4 Protocolo IP

El protocolo de IP (Internet Protocol) es la base fundamental de la Internet.
Transporta datagramas de la fuente al destino. El nivel de transporte fragmenta el flujo de datos en datagramas. Durante su transmisión se puede dividir un datagrama en fragmentos que se ensamblan de nuevo en el destino.

Introducción

TCP/IP es un conjunto de protocolos que cubre los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto.

TCP/IP es utilizado por todos los ordenadores conectados a Internet, de manera que estos puedan comunicarse entre sí. Este protocolo se encargara de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, esta debe ser dividida en unidades de información de menor tamaño llamadas datagrama (datagram), y son conjuntos de datos que se envían como mensajes independientes.

3.6.4.1 Características IP

- La tarea de IP es llevar los paquetes de un sitio a otro, mientras TCP se encarga del flujo y asegura que los datos estén correctos.

- . Las líneas de comunicación se pueden compartir entre varios usuarios.

- Brinda Direccionamiento, Control de errores, secuencia miento y control de flujo

- Ofrece enrutamiento dinámico[12].

- Es un sistema no orientado a conexión.

- Cualquier maquina de la red puede comunicarse con otra distinta y esta conectividad permite enlazar redes físicamente independientes en una red virtual llamada Internet.

- TCP/IP proporciona la base para muchos servicios útiles, incluyendo correo electrónico, transferencia de ficheros y login remoto.

- El correo electrónico esta diseñado para transmitir ficheros de texto pequeños. Las utilidades de transferencia sirven para transferir ficheros muy grandes que contengan programas o datos.

- Proporciona chequeos de seguridad controlando las transferencias.

[12] **Enrutamiento dinámico:** Los paquetes no necesitan seguir la misma trayectoria, ni necesariamente tienen que llegar todos al mismo tiempo, la red puede usar la conexión más idónea que esté disponible en ese instante

- El login remoto permite a los usuarios de un ordenador acceder a una maquina remota y llevar a cabo una sesión interactiva.
- Fragmenta paquetes si es necesario.

- Direccionamiento mediante direcciones lógicas IP de 32 bits.

- Si un paquete no es recibido, este permanecerá en la red durante un tiempo finito.

- Realiza el "mejor esfuerzo" para la distribución de paquetes.

- Tamaño máximo del paquete de 65635 bytes.

- Solo ser realiza verificación por suma al encabezado del paquete, no a los datos este que contiene.

Funcionamiento

La flexibilidad del sistema lo hace muy confiable; si un enlace se pierde, el sistema usa otro. Cuando se envía un mensaje, el TCP divide los datos en paquetes, ordena estos en secuencia, agrega cierta información para control de errores y después los envía, y los distribuye. En el otro extremo, el TCP recibe los paquetes, verifica si hay errores y los vuelve a combinar para convertirlos en los datos originales. De haber error en algún punto, el programa TCP destino envía un mensaje solicitando que se vuelvan a enviar determinados paquetes.

Dirección de Internet

El protocolo IP identifica a cada ordenador que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un numero de 32 bit que debe ser único para cada host, y normalmente suele representarse como cuatro cifras de 8 bit separadas por puntos.

La dirección de Internet (IP Address) se utiliza para identificar tanto al ordenador en concreto como la red a la que pertenece.

3.7 VENTAJAS DE NGN SOBRE LAS REDES IP TRADICIONALES

Ofrece diferentes clases de servicios con confiabilidad

A diferencia de Internet, que ofrece servicios del “mejor esfuerzo”, las redes NGN pueden distinguir los paquetes que pertenecen a cada aplicación. Por ejemplo VoIP, video, datos particulares de una empresa sobre una VPN.

La red NGN puede asegurar la calidad de servicio que cada paquete requiere asociada a cada aplicación.

Transporte de tráfico en tiempo real.

Hasta hace poco los enrutadores se tomaban mucho tiempo en las operaciones de procesar, recolectar y reensamblar los paquetes de la información, que imposibilitaban el transporte de trafico sensible al retardo, Ej. La voz.

Sin embargo, la reciente generación de enrutadores son tan rápidos en la transmisión y en el procesamiento de paquetes que los retardos introducidos son menos imperceptibles por el humano.

Combinando enrutadores ultra rápidos con mecanismos que permitan diferenciar los servicios y protocolos que imponen la noción de una sesión IP, las redes NGN soportan realmente servicios como la telefonía y la televisión en vivo.

Interoperabilidad completa con la PSTN

- Las redes NGN en razón a que soportan trafico telefónico deben interoperar con la red PSTN, para posibilitar el intercambio de llamadas con ella

- Las redes NGN soportan funcionalidades básicas tales como:

    - Tono de llamada

    - Establecer y finalizar llamadas

- Las redes NGN soportan todas las funcionalidades de la PSTN incluyendo portabilidad numérica, servicios de emergencia, llamadas gratuitas, facturación detallada, etc.

Servicios de administración y tarifación flexible

- En Internet la tarifa plana es la norma. Ya sea que el servicio se implemente vía conexiones dial up o por circuitos dedicados.
- Las redes NGN poseen sistemas de administración y tarifación que soportan las modalidades de tarifas planas, o por uso.

- El servicio puede ser costeado de una manera tal que refleje el valor para el cliente y la demanda que él ha hecho de los recursos de la red.

Administrar la interconexión

- Los operadores de las redes NGN necesitan manejar el intercambio de tráfico con otros operadores, para:

- Asegurar la calidad de servicio extremo a extremo.

- Implementar las políticas de regulación y los cargos negociados con los otros operadores.

3.8 BENEFICIOS DE UNA NGN

El mercado de las telecomunicaciones ha experimentado una asombrosa metamorfosis desde sus inicios. Pero la industria nunca se había enfrentado, como ahora, al impacto de la demanda de ancho de banda, la inestabilidad competitiva y la presión económica.

Estos factores exigen medidas drásticas para mantener la rentabilidad y el crecimiento del mercado en su conjunto. Las NGN, con sus ofertas de servicios de alto valor agregado y de grandes beneficios para todos, parecen ser la respuesta. Dichas redes deben unificar la flexibilidad y capacidad de creación rápida de servicios demandada por el mercado del futuro, y ofrecer, al mismo tiempo, una ruta de migración para los servicios actuales, optimizando la productividad y los costos.

La complejidad del mercado y las necesidades del usuario final requieren poner una atención cuidadosa a la arquitectura de este tipo de redes, con el fin de asegurar que los valores de la última Generación de redes no se pierdan con el rápido desarrollo.

Servicios NGN

Las NGN soportan comunicaciones conversacionales en tiempo real (otros distintos a la voz) y comunicaciones que no son en tiempo real. Esto implica proveer comunicación extremo a extremo utilizando más de un medio, por ejemplo:

- Servicios de mensajería: mensajería instantánea (IM), servicios de mensajes cortos (SMS), servicios de mensajes multimedia, etc.

- Presionar y hablar (Push to talk) sobre NGN.

- Servicios interactivos multimedia punto a punto: video telefonía, whiteboarding conversación total, conferencia multimedia con compartición de archivos y aplicaciones (juegos, aprendizaje).

- Servicios basados en un solo toque (push-based service15): por ejemplo servicios multimedia sobre IP que incluyen nuevos servicios como seguridad pública, gobierno e información tecnológica corporativa.

- Servicios de distribución de contenidos: radio y video streaming, música y video bajo demanda, distribución de imágenes profesionales y médicas, publicidad electrónica.

- Servicios de difusión/multidifusión.

- Servicios de información: estado del tráfico en las carreteras, información de tickets de vuelo, etc.

- Servicios basados en localización.

Los principales beneficios de las redes NGN son:

- Reduce al máximo el tiempo de recuperación de las inversiones, ya que factura a los usuarios múltiples servicios utilizando una misma Red.

- Cuenta con una amplia variedad de productos y servicios que van de acuerdo a las necesidades de cada usuario.

- Invierte en el desarrollo de la red gradualmente y a medida que va desarrollando su negocio.

- Permitir que el costo por abonado se ajuste a los servicios brindados.

- Reduce los costos operativos e incrementa la rentabilidad de los negocios.

- Dispone de una red con redundancia, lo que implica asegurar la disponibilidad permanente de los servicios y el incremento de la rentabilidad global del negocio.

- Puede diseñar esquemas de negocios donde el abonado pague de acuerdo a los servicios que utiliza, manteniendo un costo base por abonado.

CAPÍTULO IV

TRANSELECTRIC S.A.

La Compañía Nacional de Transmisión Eléctrica, TRANSELECTRIC S.A., es responsable de operar el Sistema Nacional de Transmisión, su objetivo fundamental es el transporte de energía eléctrica, garantizando el libre acceso a las redes de transmisión a los agentes del Mercado Eléctrico Mayorista, compuesto por generadores, distribuidores y grandes consumidores.

4.1 MISIÓN, VISIÓN, VALORES Corporativos.

MISIÓN:

Garantizar al país y a nuestros clientes la disponibilidad del SNT y del sistema de telecomunicaciones, con calidad y eficiencia, generando valor para los accionistas, colaboradores y la comunidad, promoviendo así el desarrollo del sector eléctrico y de las telecomunicaciones.

VISIÓN:

Hasta el 2012 ser una corporación empresarial líder dentro del sector eléctrico y de telecomunicaciones en el país.

VALORES:

• Transparencia

• Calidad

• Pro actividad

• Compromiso

• Responsabilidad Social Empresarial

• Cumplimiento de Normas

• Mejora Continua

4.2 RESEÑA HISTÓRICA Y CONSTITUCIÓN

TRANSELECTRIC S.A., se constituyó como Sociedad Anónima, mediante escritura pública otorgada el 13 de enero de 1999 ante el Doctor Eduardo Orquera Zaragosín, Notario Décimo del Cantón Quito, con un capital suscrito y pagado de

S/.835.310`000.000,00 y como capital autorizado S/.1´670.620´000.000,00, cuyo único accionista fundador fue INECEL en proceso de liquidación.

La Superintendencia de Compañías de Quito con resolución No. 99.1.1.1. 00180 de 20 de enero de 1999 aprobó la constitución de la Compañía, cuya inscripción en el Registro Mercantil corresponde bajo el No. 011 del Registro Industrial, Tomo 31 y anotado en el repertorio No. 002167 de 29 de enero de 1999, fecha en la que la Compañía surge legalmente.

Por efecto de la dolarización, el capital en sucres de la Compañía se re expresó a dólares, mediante escritura pública otorgada el 18 de septiembre del 2001, en la Notaria Segunda de Quito a cargo de la Dra. Ximena Moreno de Solines, estableciéndose el capital suscrito y pagado en US$ 33,412,400.00 y el capital autorizado en US$ 66,824,800.00, modificándose en este sentido el capitulo segundo, Art. Quinto del Estatuto Social.

4.3 PORTAFOLIO DE TELECOMUNICACIONES

Las Telecomunicaciones en Transelectric S.A. constituyen el pilar fundamental en donde se soportan la transferencia de datos y voz del Sistema Nacional de Transmisión (SNT); desde hace 25 años se ha operado y mantenido un Sistema de Telecomunicaciones que utiliza Onda Portadora (PLC) a través de las líneas de alta tensión del SNT, con resultados altamente satisfactorios.

Las actuales necesidades de comunicación y los requerimientos de alta disponibilidad, demandan la utilización de nuevas tecnologías en la transmisión de la información, es por esto que TRANSELECTRIC se ha visto en la necesidad de implementar fibra óptica como parte de su red de Telecomunicaciones. Aprovechando el nuevo marco legal y la apertura a la competencia, TRANSELECTRIC incursiona en el mercado del Servicio Portador

Ecuatoriano, para brindar la calidad y seguridad que requieren sus servicios a todos sus clientes.

TRANSELECTRIC dispone de su propio Centro de Gestión que lo atenderá permanentemente (7x24) para resolver todas sus inquietudes relacionadas con el servicio. La operación y mantenimiento de la red la realiza un grupo de ingenieros altamente capacitados que está siempre listo ante cualquier eventualidad, garantizando una respuesta inmediata.

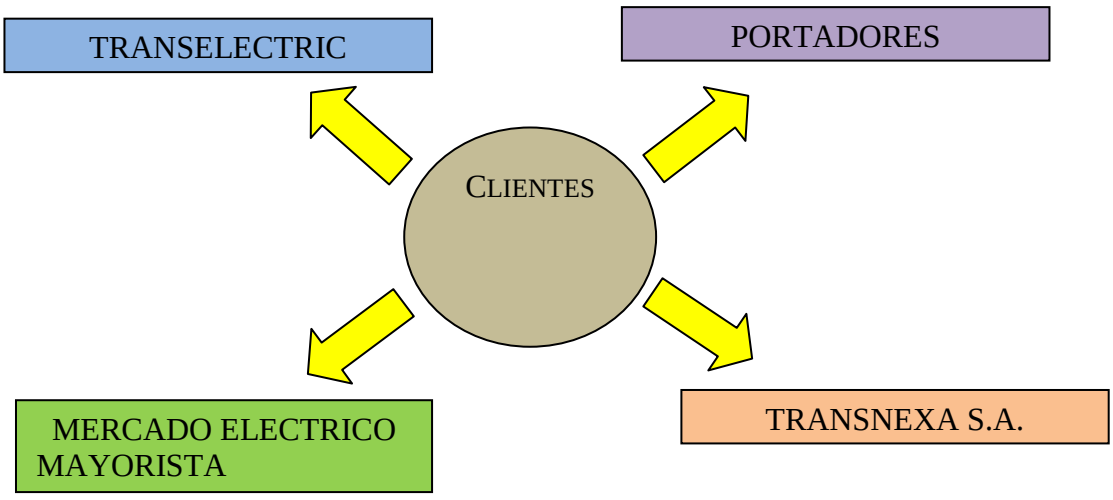


Figura 4.1 Clientes de TRANSELECTRIC S.A[13]

[13] Portal de internet de Transelectric S.A
http://www.transelectric.com.ec/transelectric_portal/portal/main.do?sectionCode=96

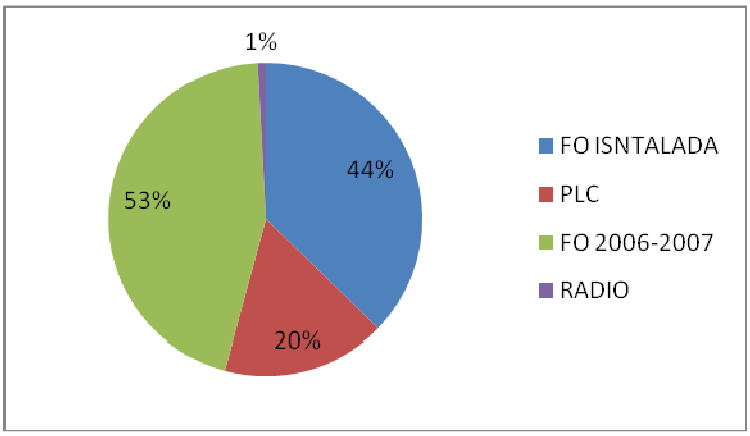


Figura 4.2 Medios de transmision utilizados por Transelectric S.A[1]

4.4 SERVICIOS

TRANSELECTRIC cuenta con una red de telecomunicaciones muy robusta, que consiste en un cable de fibra óptica OPGW[14] montado sobre las torres de transmisión de energía eléctrica (instalación aérea), lo que reduce los inconvenientes producidos por otro tipo de instalaciones y permite ofrecer una disponibilidad muy alta. Durante más de cuatro años de funcionamiento, nuestra red no ha sufrido ninguna falla por rotura del cable de fibra óptica y la disponibilidad anual se ha mantenido sobre el 99.8% ofrecido.

[14] OPGW: sistema de cable compuesto tierra-óptico, para instalación en líneas eléctricas de alta tensión.

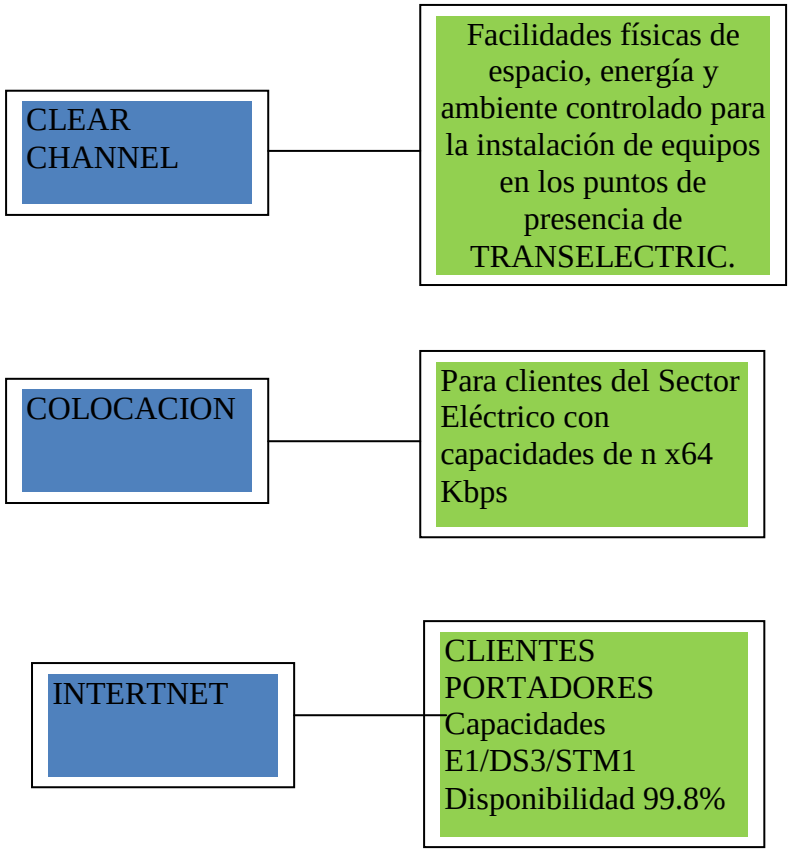


Figura 4.3 Servicios que ofrece Transelectric S.A[15]

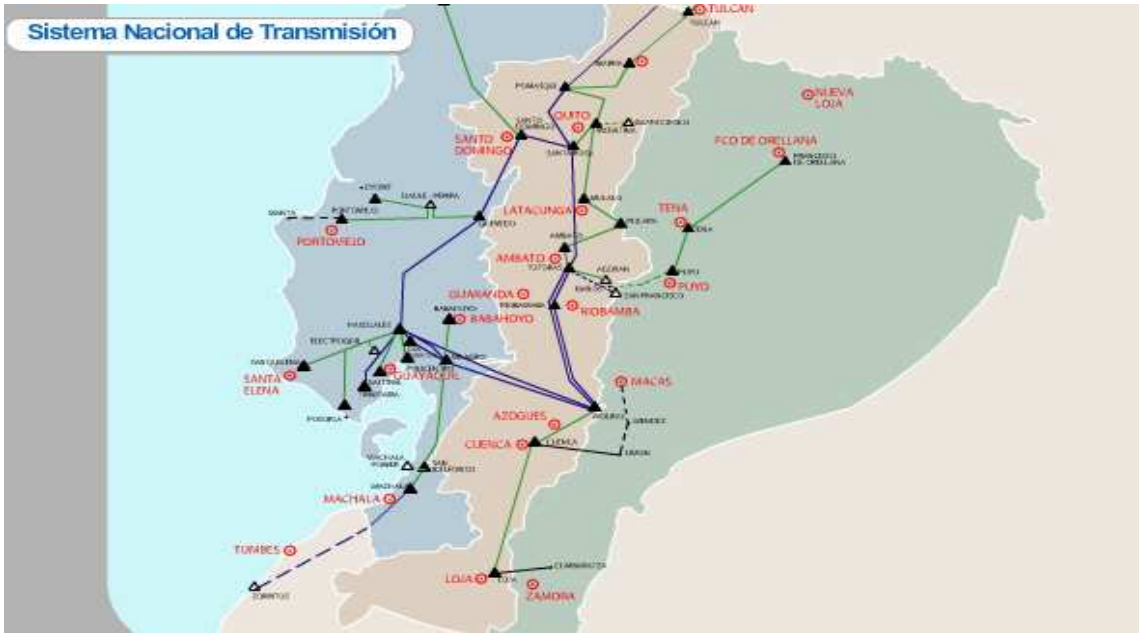


Figura 4.4 Sistema Nacional de Transmisión[16]

[15] Portal de internet de Transelectric S.A
http://www.transelectric.com.ec/transelectric_portal/portal/main.do?sectionCode=96
[16]Portal Internet de Transelectric S.A.
http://www.transelectric.com.ec/transelectric_portal/portal/main.do?sectionCode=15

PROVINCIA	PUNTO DE PRESENCIA (CIUDAD)
Pichincha	Quito
Santo domingo	Santo Domingo
Tungurahua	Ambato
Chimborazo	Riobamba
Cañar	Azogues
Azuay	Cuenca
Loja	Loja
Manabí	Manta, Portoviejo, Montecristi
Guayas	Guayaquil, Milagro
Los Ríos	Quevedo
El Oro	Machala

Tabla 4.1: Cobertura a nivel Nacional de Transelectric S.A

RED NACIONAL TRANSELECTRIC S.A				
TRAMOS	**CAPACIDAD TOTAL (E1)**	**CAPACIDAD UTILIZADA(E1)**	**% UTILIZADO**	**PROTECCION**
Jamondino- Tulcan	4032	1717	42,58	SI
Tulcan- Pomasqui	4032	1718	42,61	SI
Pomasqui-Transelectric	4032	1048	25,99	SI
Transelectric- Santa Rosa	1008	314	31,15	SI
Transelectric- Pomasqui Sur	1008	318	31,55	SI
Santa Rosa- santo Dimingo	1008	316	31,35	SI
Transelectric - Santo Domingo	1008	371	36,81	SI
Santo Domingo – Quevedo	2016	671	33,28	SI
Quevedo- Portoviejo	63	36	57,14	NO
Portoviejo- Monteciristi	63	22	34,92	NO
Montecristi- Manta	63	14	22,22	NO
Quevedo- Pascuales	2016	636	31,55	SI
Pascuales – Policentro	2016	658	32,64	SI
Pascuales- Milagro	1008	60	5,95	SI
Milagro- Zhoray	1008	25	2,48	SI
Zhoray- Cuenca	252	25	9,92	SI
Milagro- Machala	1008	35	3,47	SI
Machala – Zorritos	4032		0,00	SI
Cuenca _ Loja	252	3	1,19	NO

Tabla 4.2: Capacidad de la red de Transelectric S.A

4.5 TELECOMUNICACIONES EN TRANSELECTRIC

Las telecomunicaciones en TRANSELECTRIC S.A constituyen el pilar fundamental en donde se soportan la transferencia de datos y la voz del Sistema Nacional de Transmisión (SNT), desde hace 25 años se ha operado y mantenido un Sistema de Telecomunicaciones que utiliza Onda Portadora(PLC) a través de actuales necesidades de comunicación y los requerimientos de alta disponibilidad, demanda la utilización de nuevas tecnologías en la transmisión de la información, es por esto que TRANSELECTRIC se ha visto en la necesidad de implementar fibra óptica como parte de su red de Telecomunicaciones.

Aprovechando el nuevo marco legal y la apertura a la competencia TRANSELECTRIC S.A Incursiona en el mercado de servicio portador Ecuatoriano, para brindar calidad y seguridad que requieren sus servicios a todos sus clientes.

TRANSELECTRIC S.A dispone de su propio centro de Gestión que lo atenderá permanentemente (7X24) para resolver todas las inquietudes relacionadas con el servicio. La operación y mantenimiento de la red la realiza un grupo de ingenieros altamente capacitados que esta siempre listo ante cualquier eventualidad, garantizando una respuesta inmediata.

El servicio de portador internacional que proporciona TRANSELECTRIC S.A lo realiza a través de TRANSNEXA creada a partir de la unión de TRANSELECTRIC e INTERNEXA, con capacidades de E1, DS3 y STM-1 y servicios de transporte internacional de tráfico de datos IP, datos n*IP y voz, TRANSNEXA se enfoca en dar conexión internacional al tráfico generado hacia y desde el Ecuador por empresas proveedoras de servicios de telecomunicaciones.

Cliente	Servicio
Transelectric	Clear Channel, Colocation, Internet
Portadores	Clear Channel, Colocation, Internet
MEM Mercado Mayorista electrico	Clear Channel, Colocation, Internet
Transnexa	Clear Channel, Colocation, Internet

Tabla 4.3 Clientes Principales y servicios de Transelectric S.A

Opera en forma exclusiva la red de fibra óptica tendida entre Ecuador y Colombia facilitando la conectividad de los ISP’s de Internet con los EEUU a través de redes de cable submarino ARCOS –I y MAYA- I.

ARCOS –I es un sistema de cable submarino de fibra óptica diseñado para brindar servicios de ancho de banda, desarrollado con el fin de proveer la red de comunicaciones más avanzada técnicamente en el Caribe que conectará a 15 Países.

La eficiente topología en forma de anillo de ARCOS convierte a la red totalmente redundante, permitiendo que ARCOS seleccione automáticamente la señal más fuerte para una calidad de transmisión óptima y confiable mientras provee el restablecimiento de la señal de inmediato.

El cambio para protección es inmediato, la interrupción en el servicio es imperceptible y el tráfico de la red no es afectado excepto que el sistema sufra múltiples daños a la vez. Ambas señales, "Trabajando y Protegiendo" (Working & Protect), son analizadas simultáneamente y si alguno de los lados cae por debajo de los límites preestablecidos, el trayecto se cambia en menos de 50ms (50 milisegundos).

La red comprende un anillo totalmente redundante de 8.600 Km que consiste de dos segmentos de cable uno retransmisible y otro no retransmisible usando las tecnologías de punta Dense Wavelength Division Multiplexing ("DWDM") y Synchronous Digital Hierarchy ("SDH"). El sistema actualmente opera a 15 giga bits por segundo ("Gbps"), con una capacidad de mejorar la capacidad a 960 Gbps. El tráfico en el sistema experimenta un período de retraso "latency" en su recorrido menor de 50 milisegundos operando en circunstancias normales.

Características

• Conecta en forma directa 15 países.

Estados Unidos, Bahamas, Turcos & Caicos, Republica Dominicana, Puerto Rico, Curazao, Venezuela, Colombia, Panama, Costa Rica, Nicaragua, Honduras, Guatemala, Belice y México.

• Capacidad Inicial: 15 Gbps equivalente a 6.048 sistemas de 2 Mbps.

• Capacidad final: 960 Gbps equivalente a 387.072 sistemas de 2 Mbps

• Gran capacidad de ampliación, la primera permitirá un incremento de 10080 sistemas de 2 Mbps adicionales.

Se interconecta con otros cables Submarinos Américas –I , Américas –II, Columbus –II, Columbus III, Panamericano.

Figura 4.5 Conformación de cable submarino Arcos -1[17]

[17] Portal de internet http://jealbornoz.blogspot.com/2007/06/desconectados.html

MAYA –I consiste en una rede de fibra óptica de 4.323 Km que opera a una capacidad de 20 Gbps, Utiliza tecnologías SDH y DWDM. Actualmente este cable submarino usa 5000 E1's de su capacidad total y enlaza la cuenca marítima occidental conectando 7 países. Estados unidos, México, Honduras, Isla Caimán, Costa Rica, Panamá, Colombia.

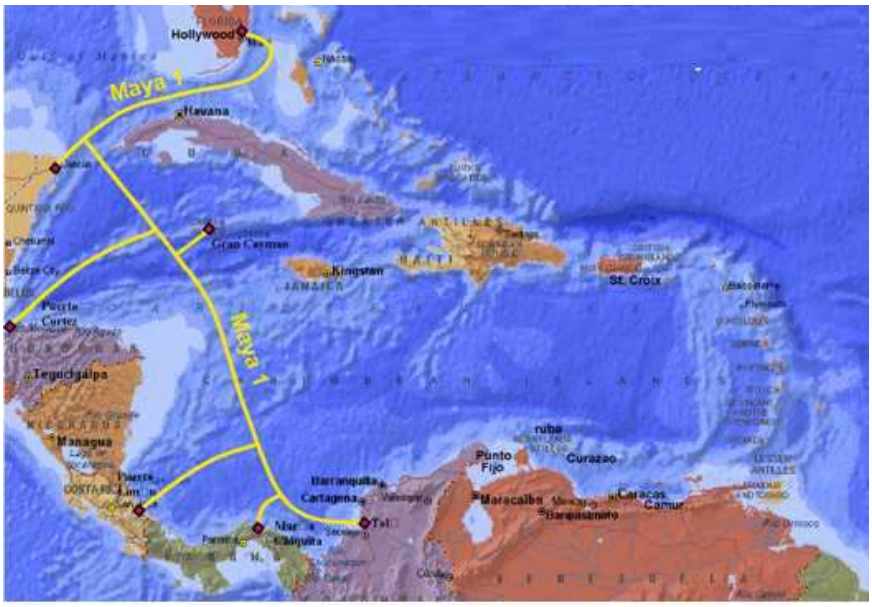


Figura 4.6 Conformación de cable submarino MAYA –I[18]

4.6 DESCRIPCIÓN DE LA RED DE TRANSELECTRIC S.A

4.6.1 BACKBONE

Un backbone es un enlace de gran caudal o una serie de nodos de conexión que forman un eje de conexión principal. Es la columna vertebral de una red.

En el caso de la empresa estatal TRANSELECTRIC S.A., cuenta con una red de telecomunicaciones muy robusta, que consiste en un cable de fibra óptica OPGW

[18]Portal Internet http://jealbornoz.blogspot.com/2007/06/desconectados.html

(OPTICAL GROUND WIRE) cable de Guardia Óptico, solución ideal para transmitir datos por líneas de alta tensión montado sobre las torres de transmisión de energía eléctrica (instalación aérea).

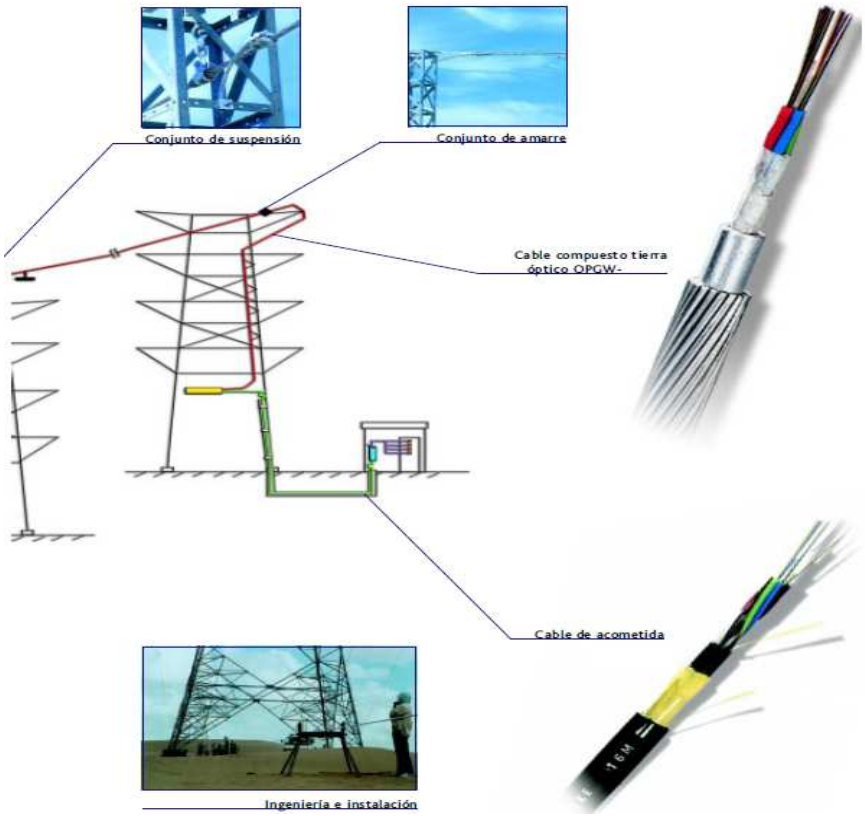


Figura 4.7 Fibra óptica OPGW

Este cable está diseñado para extenderse hasta 10 Km., reemplazando al cable de guarda existente en la red de transmisión eléctrica, permitiendo un doble uso real aprovechando, mejor los recursos de la torre de transmisión eléctrica.

La fibra óptica especializada de propósito dual esta constituido por un núcleo de aluminio flexible, dentro del mismo se concentra los tubos buffer, que permiten a la fibra óptica, distribuirse entre ellos en número de 6, 12, 16,24 o 48 fibras.

La fibra óptica cumple sobradamente con los requerimientos CCITT (Comité consultivo Internacional Telegráfico y Telefónico), G.652, para fibra de mono modo y con G.655 de dispersión desplazada.

Individualmente las fibras ópticas son protegidas por una cubierta de plástico que protege los daños físicos, ambientales y por efecto de manipulación de la misma.

El núcleo de fibras ópticas se aloja en el interior de un tubo de aluminio revestido que proporciona tanto protección mecánica al núcleo óptico como estanqueidad frente a la humedad o penetración de agua.

4.6.2 Infraestructura del backbone

La Infraestructura del backbone esta básicamente constituida de enlaces de Fibra Óptica a lo largo y ancho del Ecuador, como se muestra en la Tabla 4.2 formando un anillo de fibra óptica, el cual permite prestar el servicio de portador de portadores. Los tipos de fibras utilizadas en la construcción del backbone son G.652, G.652b, G.655, G.655b que corresponden a la serie G (sistemas y medios de transmisión, sistemas y redes digitales) de las recomendaciones de la Unión Internacional de Telecomunicaciones ITU-T.

BACKBONE DE TRANSELECTRIC					
Región Sierra					
ENLANCES	**DISTANCIA**	**MEDIO DE TRANSMISION**	**NORMA**	**Instalación**	**ESTADO**
Pomasqui-Vicentina	20 Km	Fibra (48 hilos)	G.655	Aérea Cable OPGW	Instalado
Vicentina-Sta. Rosa	20 Km	Fibra (48 hilos)	G.655	Aérea Cable OPGW	Instalado
Vicentina- Transelectric	4Km	Fibra (48 hilos)	G.655	Subterránea Cable Armado	Instalado
Sta. Rosa- Totoras	113Km	Fibra (24 hilos)	G.652b	Aérea Cable OPGW	Construcción
Totoras-Riobamba	45 Km	Fibra (24 hilos)	G.652b	Aérea Cable OPGW	Construcción
Riobamba-Zhoray	146 Km	Fibra (24 hilos)	G.652b	Aérea Cable OPGW	Instalado
Zhoray-Molino	14 Km	Fibra (24 hilos)	G.652b	Aérea Cable OPGW	Instalado
Molino-Cuenca	64 Km	Fibra (48 hilos)	G.652b	Aérea Cable OPGW	Instalado
Cuenca-Loja	135 Km	Fibra (48 hilos)	G.655b	Aérea Cable OPGW	Instalado
Región Costa					
EN LANCES	**DISTANCIA**	**MEDIO DE TRANSMISION**	**NORMA**	**INST ALACION**	**ESTADO**
Sta. Rosa-Sto. Domingo	80 Km	Fibra (48 hilos)	G.655	Aérea Cable OPGW	Instalado
Sto. Domingo-Ouevedo	109 Km	Fibra (48 hilos)	G.652b	Aérea Cable OPGW	Instalado
Ouevedo-Portoviejo	135 Km	Fibra (24 hilos)	G.652b	Aérea Cable OPGW	Instalado
Ouevedo-Pascuales	149 Km	Fibra (48 hilos)	G.652b	Aérea Cable OPGW	Instalado
Pascuales-Policentro	16Km	Fibra (48 hilos)	G.652b	Aérea Cable OPGW	Instalado
Pascuales-Dos Cerritos	10Km	Fibra (48 hilos)	G.652b	Aérea Cable OPGW	Instalado
Pascuales- T nnitana	30 Km	Fibra (24 hilos)	G.652b	Aérea Cable OPGW	Instalado
Dos Cerritos-Milagro	43 Km	Fibra (48 hilos)	G.652b	Aérea Cable OPGW	Instalado
Milagro-Machala	135 Km	Fibra (24 hilos)	G.652b	Aérea Cable OPGW	Instalado
Milagro-Zhoray	105 Km	Fibra (48 hilos)	G.652b	Aérea Cable OPGW	Instalado
Zhoray-Sinincay	52 Km	Fibra (48 hilos)	G.652b	Aérea Cable OPGW	Construcción

Tabla 4.4: Backbone Capacidades Transelectric S.A.

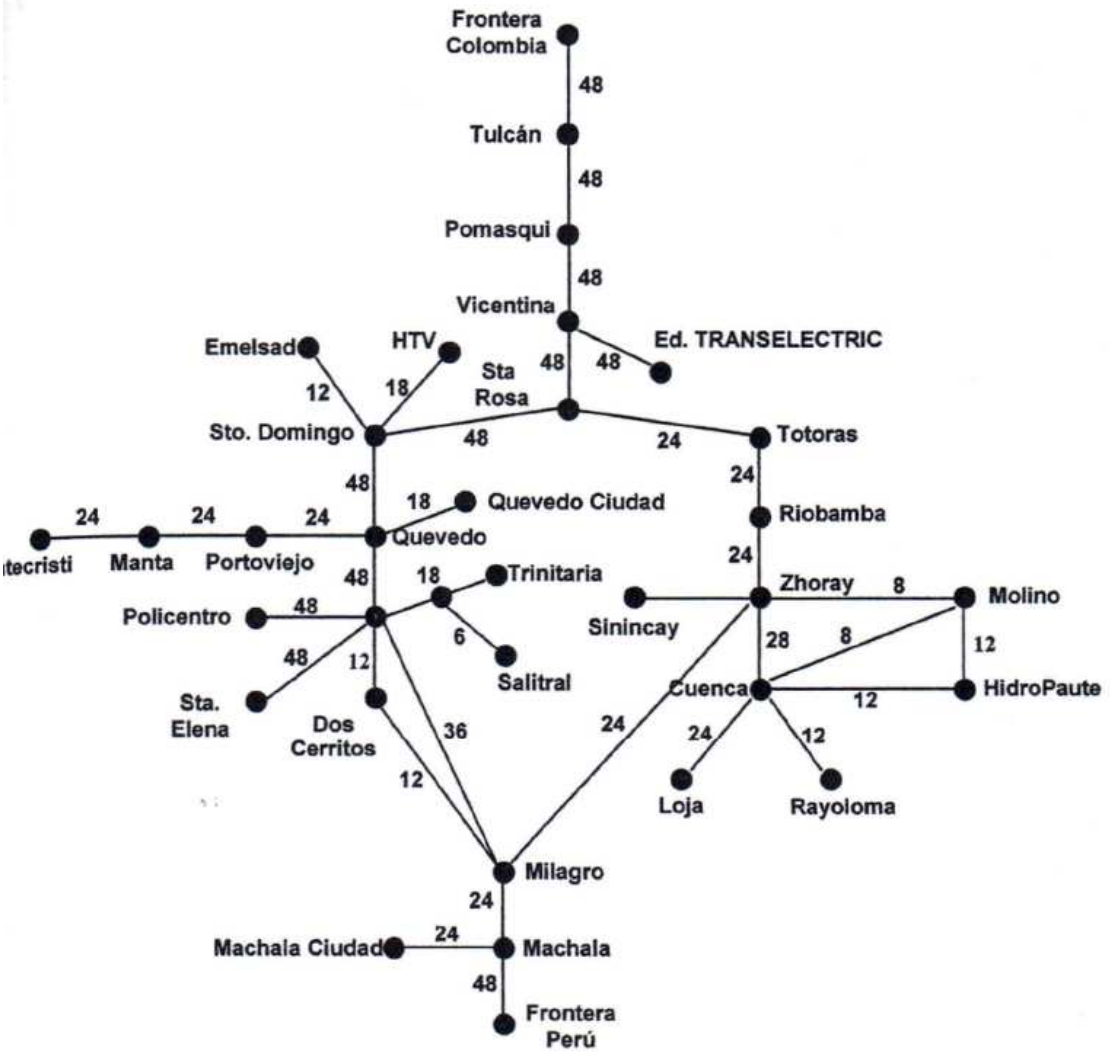


Figura 4.8 Red de FO de Transelectric S.A

4.7 SERVICIOS

TRANSELECTRIC S.A. cuenta con una red de telecomunicaciones muy robusta, la disponibilidad anual se ha mantenido sobre el 99.8% y una latencia menor a 165 ms entre el enrutador del cliente con los demás nadas ubicados en los Estados Unidos.

Además posee una alta confiabilidad con pérdidas de paquetes menores al 0.1 %, y un rehúso 1: 1 garantizado.

Existen dos tipos de servicios que TRANSELECTRIC S.A. ofrece como empresa.

- Portador de Portadores (Nacional)
- Servicios al MEM (Mercado Eléctrico Mayorista)

4.7.1 Servicios como Portador de Portadores (Nacional)

Existen tres tipos de servicios que TRANSELECTRIC S.A. ofrece como portador:

- Clear Channel
- Valor Agregado
- Collocation

4.7.1.1 Clear Channel

Es un servicio que conecta dos sitios mediante un enlace digital dedicado que le asegura la disponibilidad de un canal exclusivo para enviar y recibir grandes volúmenes de información con una máxima velocidad, al tener garantizado el 100 % del ancho de banda contratado. Debido a sus características es ideal cuando se necesita realizar transmisiones en tiempo real, sin demoras.

Las Características del Servicio son:

- Transmisión digital dedicada de extremo a extremo.

- Le permite contratar el ancho de banda que se ajusta a sus necesidades de Transmisión: que varían entre 9.6 Kbps y 2 Mbps.

- Supervisión y mantenimiento constante.

- Por sus redes IP's remotas, es apropiado para aplicaciones como videoconferencias, acceso a redes LAN's remotas, etc.

Los Beneficios del Servicio son:

- Controlar sus costos.
- Optimizar el Trabajo.
- Instalación, configuración y mantenimiento del sistema.

4.7.1.2 Valor Agregado

Son aquellos que utilizan servicios finales de telecomunicaciones e incorporan aplicaciones que permiten transformar el contenido de la información transmitida. Esta Transformación puede incluir un cambio neto entre los puntos extremos de la transmisión en el código, protocolo o formato de la información.

Se entiende que ha habido transformación en la información cuando la aplicación direcciona, empaqueta datos, interactúa con base de datos o almacena la información para su posterior retrasmisión.

- **Ubicación**

Facilidades físicas de espacio, energía y ambiente controlado para la instalación de Equipos en los puntos de Presencia de TRANSELECTRIC S.A.

Características/servicio	PORTADOR DE PORTADORES
DISPONIBILIDAD	99,98%
CAPACIDADES OFRECIDAS	N X E1, n x DS3, n x STM-1
LATENCIA	< 165ms
PERDIDA DE PAQUETES	>0,1%
REHÚSO	1:1 GARANTIZADO

Tabla 4.5 Características Portador de Portadores TRANSELECTRIC

4.7.1.3 Servicios al Mercado Eléctrico Mayorista

Establece canales de comunicación para la trasmisión de datos, voz, datos y video para el sector eléctrico, el cual se beneficia de este servicio ya que utiliza sistema de

comunicaciones SCADA, Datos de contadores, Registradores de Falla y redes Inteligentes, voz dedicada, Voz Conmutada, Servicios de Respaldo, Video conferencia e internet, todo esto complementa los servicios de valor Agregado.

Características/servicio	PORTADOR DE PORTADORES
DISPONIBILIDAD	99,98%
CAPACIDADES OFRECIDAS	N X E1, n x DS3, n x STM-1
LATENCIA	< 165ms
PERDIDA DE PAQUETES	>0,1%
REUSO	1:1 GARANTIZADO

Tabla 4.6 Características Servicios al MEM

El servicio al MEM Mercado Eléctrico Mayorista se lo realiza en todos los nodos ubicados en el país, para garantizar las comunicaciones necesarias y el normal monitoreo, operación y funcionamiento.

CAPÍTULO V

DISEÑO DE LA RED

5.1 DESCRIPCIÓN ACTUAL DE LA RED.

Según el análisis realizado en los capítulos anteriores el objetivo fundamental de esta tesis es diseñar una red de multiservicios basados en MPLS. Para cumplir este objetivo es necesario tomar como bases, la topología y capacidades de red que posee actualmente la empresa Transelectric S.A.

5.1.1 SDH

Es la tecnología utilizada en la actual red de fibra óptica de banda ancha que pertenece a Transelectric. Permite el transporte y gestión de una gran cantidad de tipos de tráfico diferentes sobre la infraestructura física.

Es considerado un protocolo basado en la existencia de una referencia temporal común (Reloj primario), que multiplexa diferentes señales dentro de una jerarquía común flexible, y gestiona su transmisión de forma eficiente a través de la estructura de fibra óptica, con mecanismos internos de protección. El sistema de sincronismo con el que cuenta Transelectric se basa en un equipo de estrato 1 del tipo PRC (Primary Referente Clock), ubicado en su nodo principal en Quito con redundancia a través de un sistema similar en proveniente de Colombia.

Se considera red de transporte a los enlaces y equipos asociados que permiten el transporte de tráfico entre dos clientes o nodos en una red.

Los tributarios de un elemento de red **SDH** son las interfaces de tráfico en la red **SDH**. Estos elementos de red soportan diferentes tipos de tributario no **SDH** permitiendo el transporte eficiente de tráficos de diverso origen, como por ejemplo:

- Interfaces de tráfico **PDH**, tales como 2 Mbps, 34 Mbps, y 140 Mbps.
- Interfaces de voz analógicos.
- Interfaces Ethernet que toman datos IP o datos provenientes de LAN.
- Interfaces RDSI/ADSL

5.1.2 Módulo de transporte síncrono

Para lograr la convergencia de las señales tributarias en tráfico SDH la información es empaquetada en un módulo de transporte síncrono de modo que esta pueda ser transportada y gestionada a través de la red.

Un **Contenedor** (C) es el elemento básico de una señal **SDH**. Este está formado por los bits de información de una señal **PDH** la cual será empaquetada dentro del contenedor.

La **Cabecera de Ruta** (**Path Overhead**) sirve para tener algún tipo de control sobre la información asociada a un contenedor. Esta información es generada en el nodo originario de la ruta y es terminada en el nodo final del camino. Esta información permite al operador etiquetar el tráfico así como trazar la señal a través de la red (envío de trazas) e identificarla para propósitos de protecciones y monitorización de cuentas de errores.

El **Contenedor Virtual** (VC) se refiere al conjunto de un contenedor y a su cabecera de ruta asociada. Hay diferentes tipos de **contenedores virtuales**. Un **VC-12** es construido de un contenedor **C-12**, el cual contiene una señal PDH de 2 Mbps. Un **VC-3** porta un contenedor **C-3** que contiene una señal PDH de 34 Mbps y un **VC-4** porta una señal PDH de 140 Mbps en un contenedor **C-4**.

El **módulo de transporte síncrono** (STM - Synchronous Transport Module) se utiliza para que una señal introducida en un contenedor virtual pueda ser transportada en un enlace óptico, el contenedor virtual es portado sobre la red junto a algunos otros contenedores ubicados dentro de el **STM**. El contenedor virtual está ubicado en el área de carga útil del **STM** (Payload Area).

La unidad básica de **SDH** es la estructura **STM-1** y la capacidad máxima soportada por esta tecnología es STM-64, constituido por 64 tramas STM-1, equivalente a 10 Gbps.

La Cabecera de Sección (**Section Overhead**): Los bytes de información son añadidos a la estructura **STM** para habilitar el control de la transmisión sobre el enlace, provisionando un canal de comunicación entre nodos adyacentes.

La estructura de multiplexión **SDH** define cómo la información es estructurada para construir una trama **STM-1**.

La construcción del área de carga **STM** es definida por la estructura mapeada **SDH**. Las tasas de transmisión de los clientes son mapeadas en contenedores y una **cabecera de camino** (POH) añadida para dar lugar a un contenedor virtual. Estos formarán **Unidades Tributarias** (TU - Tributary Units) las cuales consisten en contenedores virtuales más el puntero. El puntero indica la posición de contenedor virtual dentro de la unidad tributaria.

La unidad tributaria es empaquetada en Grupos de Unidades Tributarias (Tributary Units Groups o TUGs) y finalmente en Grupos de Unidades Administrativas (Administrative Unit Groups o AUGs) de acuerdo a las reglas de estructura de multiplexión **SDH**.

Siguiendo estas reglas de multiplexión, una señal **STM-1** puede ser constituida de diferentes modos.

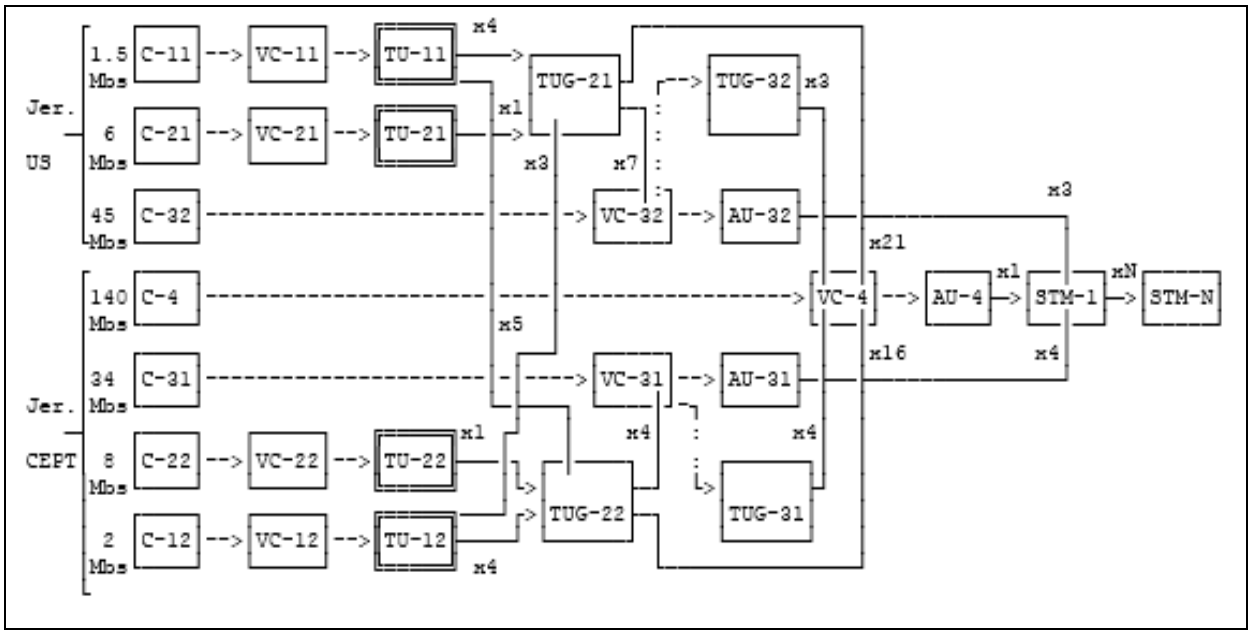


Figura 5.1 Estructura del módulo de transporte síncrono

5.1.2.1 Elementos de red de un sistema de transmisión síncrona

La recomendación de la ITU-T G.782 identifica equipos **SDH** a través de combinaciones de funciones **SDH**. Están clasificados en: Sistemas de línea, multiplexores add-drop (ADM) y cross-conectores digitales. Los equipos de fibra óptica con los que cuenta Transelectric correspondes a los multiplexores ADM, que corresponden a tarjetas eléctricas y ópticas de diferentes capacidades, además que ofrecen características de protección de tráfico del tipo lineal y en anillo.

Multiplexores Add-Drop (ADM): Estos equipos ofrecen la función de cross-conexiones junto con la de terminal de línea y multiplexión. En **SDH** es posible extraer (**Drop**) un contenedor virtual e insertar en sentido contrario (**Add**) otro contenedor virtual a la señal **STM** directamente. Esta ventaja fundamental de los sistemas síncronos significa que es posible conectar flexiblemente señales entre interfaces de elementos de red (agregados o tributarios). Esta capacidad de enrutamiento permite que la función de cross-conexión sea

distribuida por la red, resultando mejor que concentrarla en un enorme cross-conector dedicado.

En el caso del terminal de línea, los enlaces establecidos eran circuitos fijos punto a punto. La funcionalidad añadida a un **ADM** permite que sea establecida una red más flexible en la cual los circuitos de cliente que transiten la red puedan ser mas fácilmente variados. Esta flexibilidad puede ser demostrada por una red de **ADMs** encadenados.

Cross-Conectores Dedicados: Como se describió anteriormente, la cross-conectividad de los **ADM's** permite que la función de cross-conexión sea distribuida a lo largo de red, pero también es posible tener un único equipo cross-conector.

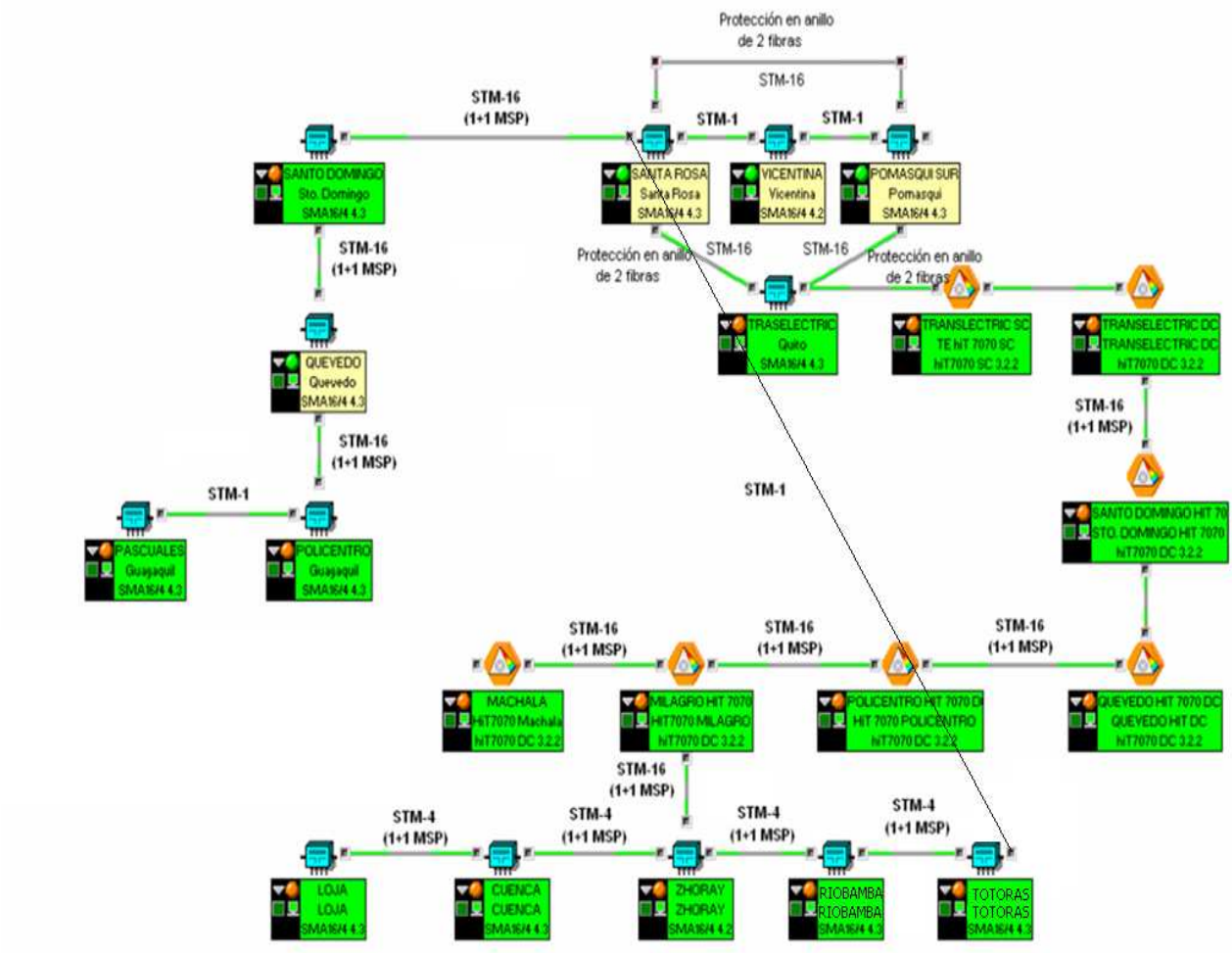


Figura 5.2 Mapa del anillo de fibra

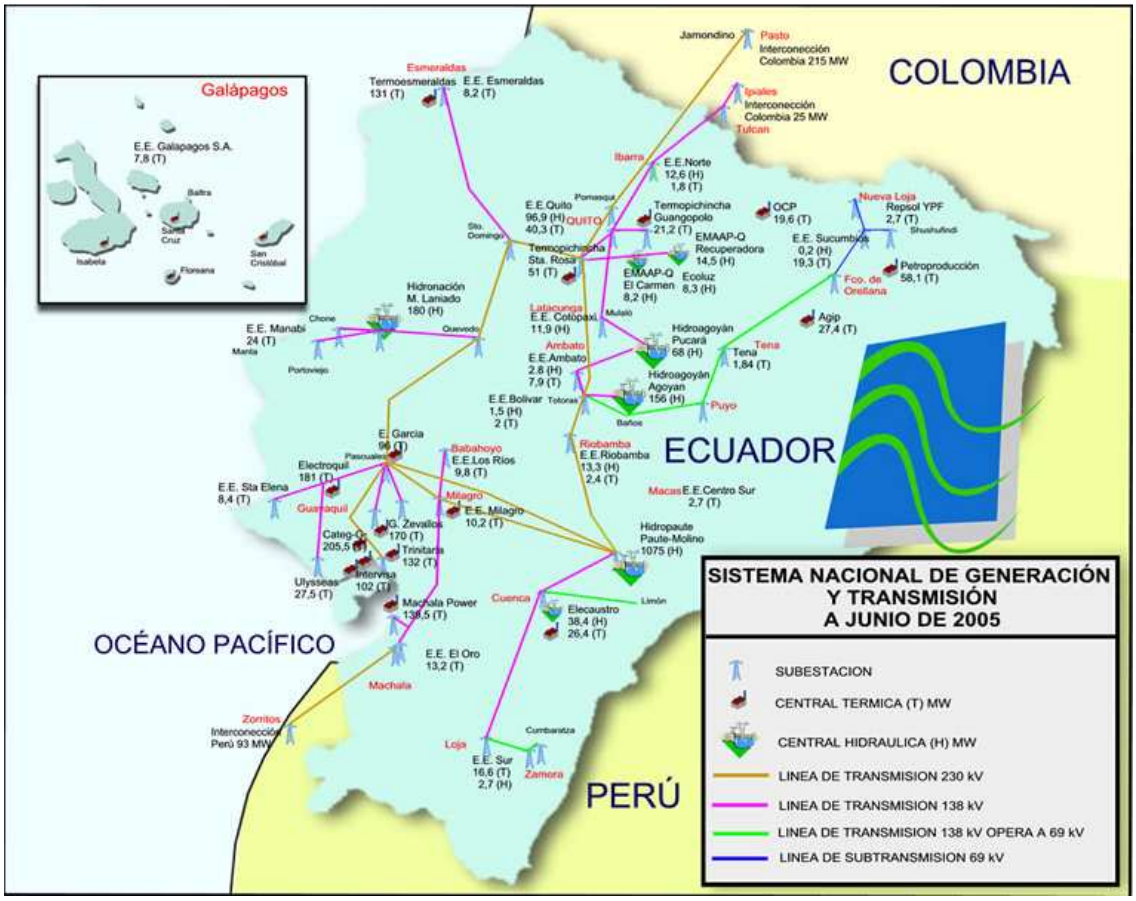


Figura 5.3. Mapa del anillo de fibra

5.2 SUBESTACIONES DE TRANSELECTRIC

TRANSELECTRIC administra y opera un conjunto de subestaciones cubriendo las principales ciudades del país como son: Quito, Santo Domingo, Quevedo, Portoviejo, Manta, Ciudad Alfaro, Guayaquil, Milagro, Machala, Cuenca y Loja.

Las subestaciones que Transelectric administra y opera son:

- Ambato

- Babahoyo
- Chone
- Cuenca
- Dos Cerritos
- Esmeraldas
- Ibarra
- Loja
- Machala
- Milagro
- Molino (Paute)
- Mulaló
- Pascuales
- Policentro (Guayaquil)
- Pomasqui
- Portoviejo
- Pucará
- Quevedo
- Riobamba
- Salitral (Guayaquil)
- San Idelfonso
- Santa Elena
- Santa Rosa
- Santo Domingo
- Totoras (Ambato)
- Trinitaria
- Tulcán
- Vicentina (Quito)
- Francisco de Orellana
- Tena

5.3 ESTRUCTURA DEL SISTEMA NACIONAL DE TRANSMISIÓN

La red de transporte óptico de TRANSELECTRIC S.A. cubre actualmente las ciudades de: Quito, Santo Domingo, Quevedo, Portoviejo, Manta, Ciudad Alfaro, Guayaquil, Milagro, Machala, Cuenca, Loja, Riobamba, Ambato y Santa Elena.

Las rutas internas del país tienen una capacidad de STM-16 (red TRANSELECTRIC) y la ruta de salida internacional hacia Colombia es de STM-64 (red TRANSNEXA). También esta puesta en marcha la integración a la red regional que une los países de Venezuela, Colombia, Ecuador y Perú. Para esto la red de existe una interconexión con Perú con una CAPACIDAD de STM-16 (red TRANSNEXA).

5.4 ESTRUCTURA DE LA RED

La red de transporte óptico que opera TRANSELECTRIC y TRANSNEXA opera a nivel SDH.

La red actual presenta una topología de línea con radiales cubriendo las ciudades antes mencionadas.

En esta red cabe señalar que existen dos tipos de nodos en las ciudades antes mencionadas. Un nodo corresponde propiamente a la red de transporte de TRANELECTRIC que opera dentro del SNT y en las Subestaciones. Y el otro nodo conocido como el nodo comercial, que es en el cual los clientes se conectan para recibir el servicio. La conexión entre el nodo operativo y el nodo comercial consta de una conexión de fibra óptica para garantizar al cliente el servicio prestado.

5.5 CAPACIDADES

5.5.1 Tráfico Internacional

En la ruta hacia Quito - Colombia existe una capacidad física máxima de 1 STM-64. La capacidad operativa y total que se encuentra operando esta ruta se la indica en la tabla 5.1

RUTA QUITO – JAMONDINO		
Capacidad	**Valor**	**Porcentaje**
Total	64 STM-1 (STM-64)	100%
Operativa	28 STM-1 + 22 E1	44,30%
Disponible	35 STM-1 + 41 E1	55,70%

Tabla 5.1 - Capacidades de trafico ruta Quito – Jamondino**.**

Existe otra ruta hacia Perú con el fin de conformar la Red Regional. Esta ruta se encuentra en fase de prueba y gestión, por lo que no existen canales contratados al momento. Consta con una capacidad de 1 STM-16 de forma inicial y existen proyectos para su expansión. Esta en fase de prueba con una capacidad de 2 STM-1 del Proyecto “Red Clara” hacia Perú, desde Machala hasta Zorritos.

5.5.2 Tráfico Interno (Nacional)

En las rutas internas entre las principales ciudades, se encuentra operando una capacidad física máxima de 1 STM-16. Las capacidades tanto operativa, disponible y total se encuentra detallada en las siguientes tablas:

RUTA QUITO – SANTO DOMINGO		
Capacidad	**Valor**	**Porcentaje**
Total	16 STM-1 (1 STM-16)	100%
Operativa	8 STM-1 + 55 E1	55,46%
Disponible	7 STM-1 + 8 E1	44,54%

Tabla 5.2 – Capacidades de trafico ruta Quito – Santo Domingo.

RUTA SANTO DOMINGO – QUEVEDO		
Capacidad	**Valor**	**Porcentaje**
Total	16 STM-1 (1 STM-16)	100%
Operativa	8 STM-1 + 41 E1	54,07%
Disponible	7 STM-1 + 22 E1	45,93%

Tabla 5.3 – Capacidades de trafico ruta Santo Domingo – Quevedo.

RUTA QUEVEDO – MANTA		
Capacidad	**Valor**	**Porcentaje**
Total	16 STM-1 (1 STM-16)	100%
Operativa	21 E1	2,08%
Disponible	15 STM-1 + 42 E1	97,92%

Tabla 5.4 – Capacidades de trafico ruta Quevedo – Manta.

RUTA QUEVEDO – GUAYAQUIL		
Capacidad	**Valor**	**Porcentaje**
Total	16 STM-1 (1 STM-16)	100%
Operativa	8 STM-1 + 22 E1	52,18%
Disponible	7 STM-1 + 41 E1	47,82%

Tabla 5.5 – Capacidades de trafico ruta Quevedo – Guayaquil.

RUTA GUAYAQUIL – MILAGRO		
Capacidad	**Valor**	**Porcentaje**
Total	16 STM-1 (1 STM-16)	100%
Operativa	1 STM-1 + 7 E1	6,94%
Disponible	14 STM-1 + 56 E1	93,06%

Tabla 5.6 – Capacidades de trafico ruta Guayaquil – Milagro.

RUTA MILAGRO – MACHALA		
Capacidad	**Valor**	**Porcentaje**
Total	16 STM-1 (1 STM-16)	100%
Operativa	1 E1	0,01%
Disponible	15 STM-1 + 62 E1	34,8%

Tabla 5.7 – Capacidades de trafico ruta Milagro – Machala.

RUTA MILAGRO – CUENCA		
Capacidad	**Valor**	**Porcentaje**
Total	16 STM-1 (1 STM-16)	100%
Operativa	1 STM-1 + 6 E1	6,85%
Disponible	14 STM-1 + 57 E1	93,15%

Tabla 5.8 – Capacidades de trafico ruta Milagro – Cuenca.

RUTA CUENCA – LOJA		
Capacidad	**Valor**	**Porcentaje**
Total	16 STM-1 (1 STM-16)	100%
Operativa	0 STM-1	0,00%
Disponible	16 STM-1	100%

Tabla 5.9 – Capacidades de trafico ruta Cuenca – Loja.

**Valores de las capacidades de tráfico hasta abril de 2008.

5.6 EQUIPOS DE LA RED DE TRANSPORTE ÓPTICO

5.6.1 Core

Se define como el núcleo de la red de transporte, donde la multiplexación se realiza a través de circuitos y/o paquetes. Esta red será utilizada para transportar información de cualquier tipo de un nodo a otro nodo de la red. También existe la opción de interconexión entre otros operadores a este nivel de transporte.

5.6.2 Metro Access

Es una red de acceso a los clientes de un operador que soporta multiplexación de circuitos y/o paquetes y a su vez maneja el direccionamiento de la red. Esta red de acceso tiene como función principal el interconectar al cliente con la red núcleo de transporte del operador.

Las tecnologías que se utilizan en esta red de acceso son: SDH (baja capacidad), PDH, Ethernet.

5.6.2.1 Descripción de los equipos del Core

Siemens Surpass hiT7070

Figura 5.4 – Fotografía Siemens Surpass hiT7070.

- Unidad de conmutación de 160G@VC-4 y 10G@VC-12.
- Funcionalidad (Resilient Packet Ring RPR, Multiprotocol Label Switching MPLS) realiza conmutación de capa 2.
- Plataforma Multiservicios: 2Mbps, 34/45Mbps, 155Mbps, STM-1/4/16, GFP para 10/100, Gigabit Ethernet, interfaces SAN (FICON, Fiber Channel); STM-16, GFP para 10 Gigabit Ethernet.
- Variedad de interfaces STM-64 incluyendo DWDM.
- Conserva las funciones de protección SDH (SNCP, MSP, BSHR, Hardware)
- Puede soportar tráfico de baja prioridad sobre líneas de reserva.
- Integrable con el sistema de gestión de altas prestaciones TNMS-Core de Siemens.
- Es posible la interconexión para anillos en todos los puertos de tráfico.

- Parada automática en caso de una interrupción del enlace de acuerdo con UIT-T G.664 y UIT-T G.958.
- Equipamiento sencillo y modular.
- Posee dos núcleos de operación, llamados single y dual core. Cada una de estas capas maneja sistemas tributarios de alto y bajo orden SDH.
- Permite cross-conectar servicios del mismo orden y de diferente orden.

Siemens SMA16

Figura 5.5 – Fotografía Siemens SMA16.

- Alto desempeño de conmutación no bloqueante, permitiendo la conexión de varios tipos de tráfico en combinaciones línea a línea, tributaria a línea y tributaria a tributaria.

- Interfaces ópticas aplicables a todos los rangos de distancias apoyadas por pre-amplificadores y amplificadores.

- Protección 1+1 para interfaces ópticas STM-1/4/16.

- Habilita la multiplexación de señales tributarias PDH y SDH en tasas de bits superiores hasta de nivel STM-16.

- Matriz de conmutación no bloqueante con capacidad VC-4, VC-3, VC-2, VC-12 y 64xSTM-1 para conexiones bidireccionales, de difusión y accesos separados.
- Interfaces para tributaria óptica STM-4/1 y eléctrica de 140/45/34/2 Mbps.

Huawei OSN 3500

- Compatibilidad con STM-64/16/4/1.
- Provee cross-conexión de alto orden de 80G para VC-4, y cross-conexión de bajo orden de 20G para VC-12, o equivalencias de VC-3.
- Provisión multiservicio en interfaces: STM-1 (Óptico/Eléctrico); STM-4/16/64 estándar o concatenados; E1/T1/E3/T3/E4; ATM; y otros.
- Provisto de protocolo GMPLS para servicios *end-to-end.*
- Tecnología WDM incorporada.
- Provee dos canales ópticos para tarjetas ADM
- Completos mecanismos de protección de red: Protección SDH (1+N).
- Soporta 2F/4F MSP, SNCP, DNI, también comparte fibra para protección virtual.
- Soporta protección en anillo RPR y STP (*spanning tree protection).*

5.6.2.2 Descripción de los equipos del metro Access

Siemens Surpass hiT7030

- STM-1 o STM-4 para el enlace.
- 4 slot modulares. (Tarjetas Ethernet, PDH, STM-1)
- Soporte para conmutación a Nivel de Capa 2 (MPLS).
- GFP, VCAT y LCAS
- Amplia los mecanismos de protección (SNCP, MSP, hardware).

Siemens Surpass hiT7020

- STM-1 o STM-4 para el enlace.
- 8 x 2 Mbit/s, 4 Fast Ethernet, STM-1/4
- Soporte para conmutación a Nivel de Capa 2 (MPLS).
- GFP, LCAS y VCAT
- Amplia los mecanismos de protección (SNCP, MSP, hardware).

Huawei Optix Metro 1000

- Capacidad cross-conexión hasta una matriz de 26 ×26 VC-4.
- Provisión multiservicio en interfaces: 6xSTM-1, 3xSTM-4; 80xE1, 64xT1, 6xE3 y DS3; 12x 10/100 Ethernet, Giga bit Ethernet transmisión transparente y 4xATM STM-1.
- GFP, LCAS y VCAT.
- Soporte para conmutación a nivel de capa 2 (MPLS).
- Amplios mecanismos de protección (SNCP, MSP, PP, hardware).
- Protección de la Sección de Multiplexación MSP (Multiplex Section Protection), protección de ruta del anillo PP (Ring Path Protection), protección de la conexión de subred SNCP (SubNetwork Connection Protection), protección de la cola virtual de la fibra compartida y protección del anillo de ruta virtual (VP-Ring protection) de una red con anillo ATM.

RAD FCD 155E

- Soporte para multiplexar tráfico Ethernet sobre SDH.
- Tráfico Ethernet mapeado en 1 VC-3/VC-4/STS-1, hasta 3 VC-3, hasta 63 VC-12.
- Protección del enlace con redundancia 1+1 MSP/APS.
- Soporte para interfaces PDH 8/21 E1, 1 E3/T3.
- Soporte VLAN para interfaces 10/100 y Gigabit Ethernet y capacidad de conmutación punto-multipunto.

RAD Optimux 45L

- Capacidad de multiplexar 21 canales E1 en una trama de 45 Mbps.
- Suporte y combinación de canales T1 y E1.
- Transmisión sobre cable coaxial y fibra óptica.
- Canales E1 eléctricos BNC.
- Varias Interfaces ópticas para el enlace principal de fibra óptica:
    - 850 nm VCSEL para fibra multimodo.
    - 1310 nm LED para fibra multimodo.
    - 1310 y 1550 nm laser para largo alcance de cobertura en fibra monomodo.
    - 1310 y 1550 nm laser para una fibra en operación WDM.
    - 1310 nm laser para una fibra en una sola longitud de de onda.

5.6.2.3 Equipos de sincronización para la red de transporte

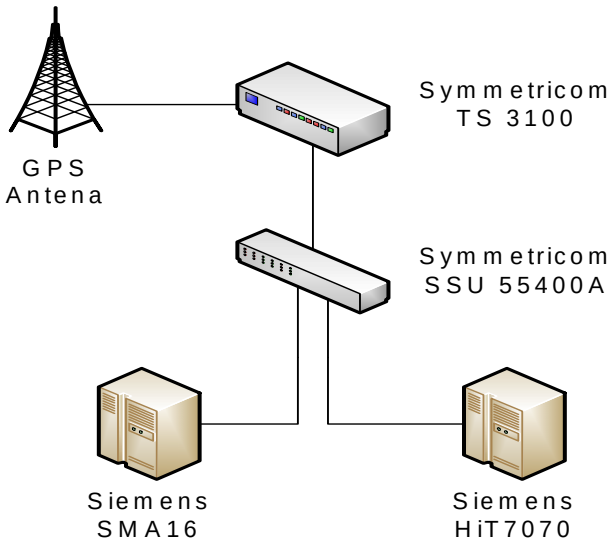


Figura 5.6 – Diagrama de la red de sincronismo actual de TRANSELECTRIC

Symmetricom TS 3100 (PRC)

Figura 5.7 – Fotografía Symmetricom TimeSource 3100.

- Especificaciones: UIT-T G.811 y G.812.
- Oscilador Interno: con oscilador de cuarzo con temperatura controlada digitalmente DCOCXO (Controlled Ovenized Crystal Oscillator).
- Señales de entrada: GPS, E1/2,048 MHz (opcional) u oscilador remoto (opcional).
- Señales de de salida para sincronización: E1/2,048 MHz, 10 MHz, 1 PPS (Pulso Por Segundo), TOD (Tiempo Real), ESCIU (Unidad de Inserción Sincronizada de Reloj a nivel E1).
- Mensaje de estado de las señales de entrada y salida.
- Puertos de comunicación: RS-232, Ethernet.
- Gestión: TimeScan/Craft, TimeScan/NMS, TimePictra/TMN.

Symmetricom SSU 55400A (SSU)

Figura 5.8 – Fotografía Symmetricom SSU 55400A.

- Número máximo de entradas de referencia 9, con protección 1:1.
- Número de entradas de referencia y monitoreo: 1 a 5 o 10 MHz PRC, hasta 8 señales en cualquier combinación de 2048 kHz o 2048 kbps.
- Tolerancia al Jitter/Wander en las señales de entrada según lo establecido en la recomendación de la UIT-T G.823.
- Monitoreo permanente de los siguientes parámetros: TDEV (desviación en el tiempo), MRTIE (máximo error relativo en el intervalo de tiempo), LMRTIE (último máximo error relativo en el intervalo de tiempo), FFOFF (frecuencia de offset fraccional).
- Reloj Oscilador Interno: Oscilador de Cristal de Cuarzo.
- Estabilidad en funcionamiento de régimen libre: 1×10^{-10} por día.
- Número de salidas: hasta 80 salidas, con protección 1:1.

- Tipo de salidas: 2048 kHz, 2048 kbps.
- Puertos para la gestión: RS-232.

En el cuadro siguiente podemos observar en resumen como se encuentran conectados los Enrutadores que están involucrados para la interconexión entre las Estaciones de Transelectric S.A.

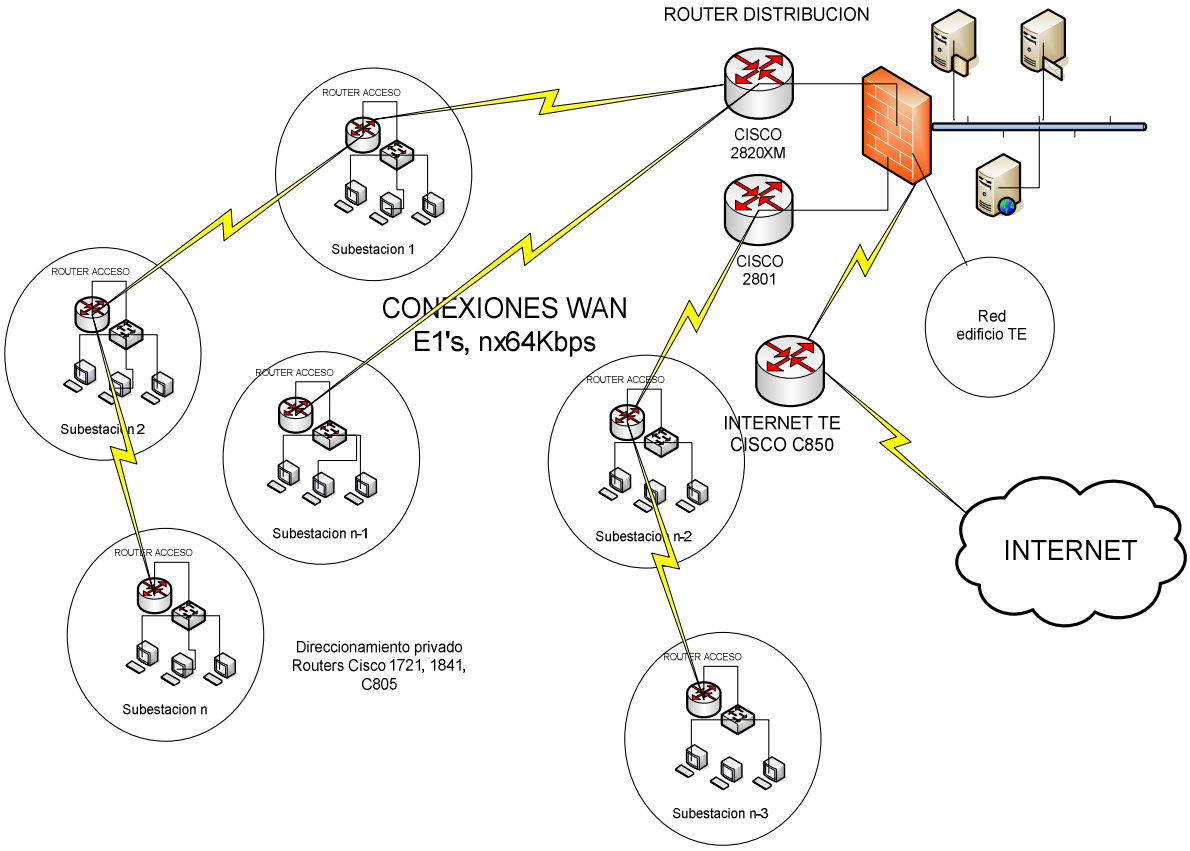


Figura 5.9 Descripción general de la red

5.7 TOPOLOGÍA ACTUAL

En la Actualidad la red de Transelectric S.A. esta conformada por una topología en mallada como podemos apreciar en el diagrama img-01.

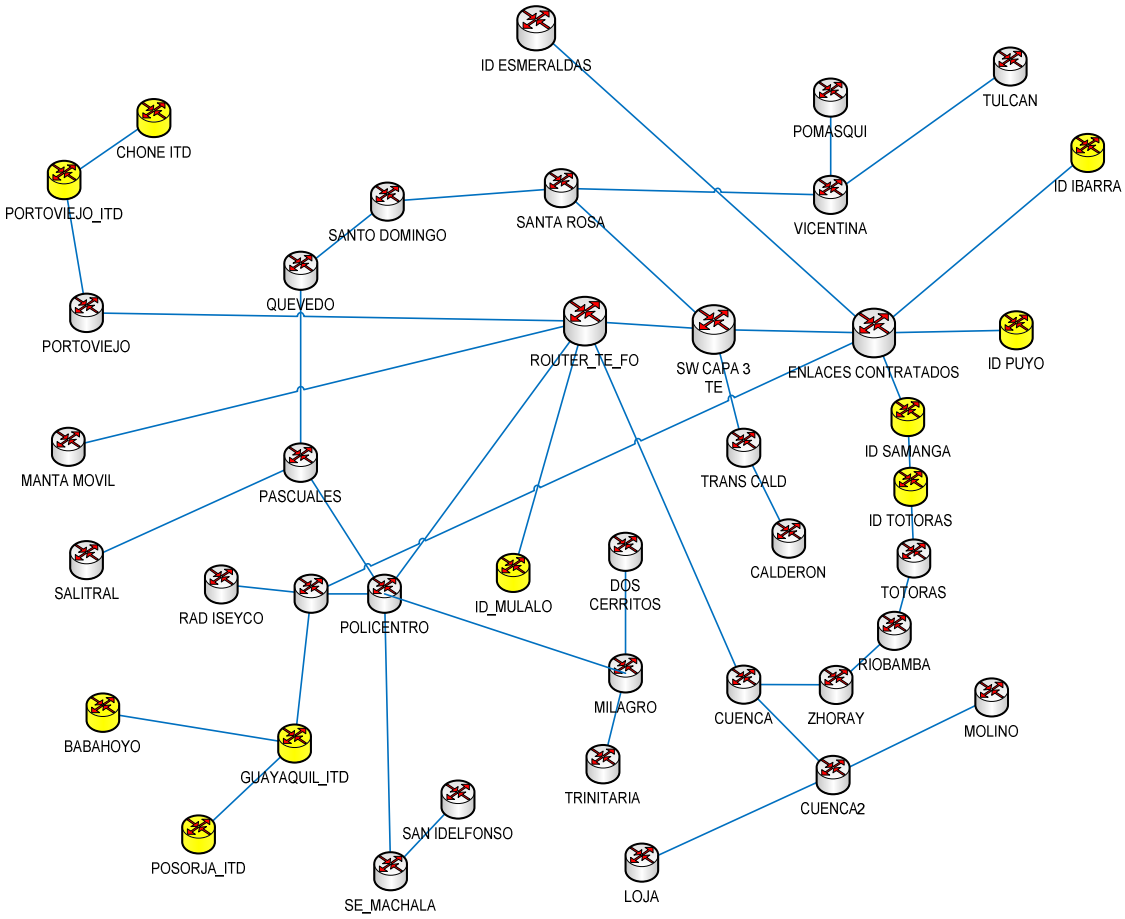


Figura 5.10 Red actual de Transelectric S.A

TRANSELECTRIC S.A ocupa equipos marca CISCO modelos 1605, 1601, 1721 , 1841, C805, C2801, 2620M, analizando las características de estos llegaremos a la conclusión si soportan MPLS y si es necesario una reestructuración y un cambio de alguno de los Enrutadores para poder llegar a MultiProtocol Label Switching MPLS, a continuación describimos los equipos que actualmente están en funcionamiento y forman parte activa de la red de Transelectric S.A.

NUM	SOPORTAS MPLS	ROUTER	MODELO	NOMBRE
1	NO	Cisco	1605	TRANSELEC_TERMOESM
2	NO	Cisco	1721	TULCAN
3	NO	Cisco	1601	TRANS-IBARRA
4	NO	cisco	1721	POMASQUI
5	SI	cisco	1841	VIECENTINA
6	SI	cisco	1841	STA_ROSA
7	SI	cisco	1841	STO_DOMINGO
8	SI	cisco	1841	QUEVEDO
9	NO	cisco	C805	TRANS-CHONE
10	NO	cisco	1601	ID_PORTOVIEJO
11	SI	cisco	1841	PORTOVIEJO
12	SI	cisco	2620XM	ROUTER_TE_FO
13	NO	cisco	WS-C3560-24TS	SWITCH CAPA 3
14	SI	cisco	c2801	TRANSELECTRIC-9
15	NO	cisco	C805	TRANS_PUYO
16	SI	cisco	1841	PASCUALES
17	NO	cisco	C870	TRANS_CALD
18	NO	cisco	1721	TRANSELECTRIC_AMBATO
19	NO	cisco	C805	TOTORAS-ID
20	SI	cisco	1841	DOS_CERRITOS
21	SI	cisco	1841	SALITRAL
22	NO	cisco	c870	CALDERON>
23	NO	cisco	1605	POLICENTRO_RAD_ISEYCO
24	NO	cisco	1721	POLICENTRO
25	NO	cisco	1721	TOTORAS-TE>
26	SI	cisco	1841	SANTA_ELENA
27	NO	cisco	1721	MILAGRO
28	NO	cisco	1721	RIOBAMBA
29	NO	cisco	c805	TRANS_MULALO
30	SI	cisco	1841	Trinitaria
31	NO	cisco	1601	trans_gye
32	NO	cisco	1601	transele_babahoyo

33	NO	cisco	c805	trans_poso
34	NO	cisco	1721	ZHORAY
35	SI	cisco	1841	SAN_IDELFONSO
36	SI	cisco	1841	MOLINO
37	NO	CISCO	1721	WAN_LOJA_CUENCA
38	NO	cisco	1721	CUENCA
39	SI	cisco	2801	SE_MACHALA
40	NO	cisco	1721	LOJA

Tabla 5.10 Equipos Activos en la red de Transelectric S.A

5.7.1 Características principales

5.7.1.1 CISCO 1605

General	
Tipo de dispositivo	Encaminador
Anchura	28.3 cm
Profundidad	22 cm
Altura	5.6 cm
Peso	0.8 kg
Procesador	
Tipo	1 x Motorola 68360 33 MHz RISC
Memoria	
Memoria RAM	8 MB (instalados) / 24 MB (máx.) – integrado
Memoria Flash	4 MB (instalados) / 16 MB (máx.)
Conexión de redes	
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet

Protocolo de conmutación	SMDS, PPP, X.25, Frame Relay, Ethernet
Red / Protocolo de transporte	TCP/IP, IPX/SPX, SNA, AppleTalk, X.25
Características	Soporte de DHCP, soporte de NAT, activable
Cumplimiento de normas	IEEE 802.3
Expansión / Conectividad	
Total ranuras de expansión (libres)	1 (1) x Ranura de expansión
Interfaces	2 x red - Ethernet 10Base-T - RJ-45 - 2 1 x red - Ethernet AUI - D-Sub de 15 espigas (DB-15) - 1 1 x gestión - consola - RJ-45 – 1

5.7.1.2 CISCO 1601

General	
Tipo de dispositivo	Encaminador
Factor de forma	Externo – modular
Anchura	28.3 cm
Profundidad	22 cm
Altura	5.6 cm
Peso	0.8 kg
Procesador	
Tipo	1 x Motorola 68360 33 MHz
Cantidad máxima soportada	1
Memoria	
Memoria RAM	8 MB (instalados) / 24 MB (máx.)
Memoria Flash	4 MB (instalados) / 16 MB (máx.)

Conexión de redes	
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet
Protocolo de conmutación	SMDS, PPP, X.25, Frame Relay, Ethernet
Red / Protocolo de transporte	IPX/SPX, AppleTalk
Cumplimiento de normas	IEEE 802.3
Comunicaciones	
Tipo	Adaptador terminal ISDN
Protocolo de señalización digital	ISDN BRI
Expansión / Conectividad	
Total ranuras de expansión (libres)	1 (1)
Interfaces	1 x red - Ethernet 10Base-T - RJ-45 - 1 1 x red - Ethernet AUI - D-Sub de 15 espigas (DB-15) - 1 1 x serial - HD D-Sub de 60 espigas (HD-60) - 1 1 x gestión - consola - RJ-45 – 1

5.7.1.3 CISCO 1841

Tipo de dispositivo	Encaminador
Factor de forma	Externo - modular - 1U
Dimensiones (Ancho x Profundidad x Altura)	34.3 cm x 27.4 cm x 4.4 cm
Peso	2.7 kg
Memoria RAM	128 MB (instalados) / 384 MB (máx.) – SDRAM
Memoria Flash	32 MB (instalados) / 128 MB (máx.)
Protocolo de interconexión de	Ethernet, Fast Ethernet

datos	
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP, HTTP, SSH-2
Características	Cisco IOS IP Base , protección firewall, compresión del hardware, asistencia técnica VPN, soporte VLAN, Intrusion Detection System (IDS), Sistema de prevención de intrusiones (IPS), montable en pared, Dynamic Multipoint VPN (DMVPN), Network Admissions Control (NAC)

5.7.1.4 CISCO 1721

Tipo de dispositivo	Encaminador
Factor de forma	Externo – modular
Dimensiones (Ancho x Profundidad x Altura)	28.4 cm x 22.1 cm x 7.9 cm
Peso	1.2 kg
Memoria RAM	64 MB (instalados) / 128 MB (máx.)
Memoria Flash	32 MB (instalados) / 32 MB (máx.)
Protocolo de direccionamiento	OSPF, HSRP, NHRP
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte	TCP/IP, L2TP, RSVP, IPSec, L2F
Protocolo de gestión remota	SNMP, RMON, Telnet
Características	Cisco IOS , diseño modular, capacidad duplex, protección firewall, auto-sensor

	por dispositivo, Encaminamiento IP, soporte de DHCP, soporte de NAT, asistencia técnica VPN, negociación automática, soporte VLAN, limitación de tráfico, Stateful Packet Inspection (SPI), prevención contra ataque de DoS (denegación de servicio), activable, Low-latency queuing (LLQ), Weighted Fair Queuing (WFQ), soporte de Access Control List (ACL)
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.1Q

5.7.1.5 CISCO 2801

Tipo de dispositivo	Encaminador
Dimensiones (Ancho x Profundidad x Altura)	43.8 cm X 41.7 cm X 4.5 cm
Peso	6.4 kg
Memoria RAM	128 MB (instalados) / 384 MB (máx.)
Memoria Flash	64 MB (instalados) / 128 MB (máx.)
Conexión de redes	
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP 3
Indicadores de estado	Actividad de enlace, alimentación
	Protección firewall, cifrado del hardware, alimentación mediante Ethernet (PoE),

Características	asistencia técnica VPN, soporte de MPLS, filtrado de URL
Cumplimiento de normas	IEEE 802.3af
Algoritmo de cifrado	DES, Triple DES, AES
Cumplimiento de normas	CISPR 22 Class A, CISPR 24, EN 61000-3-2, VCCI Class A ITE, IEC 60950, EN 61000-3-3, EN55024, EN55022 Class A, UL 60950, EN50082-1, CSA 22.2 No. 60950, AS/NZ 3548 Class A, JATE, FCC Part 15, ICES-003 Class A, CS-03, EN 61000-6-2

5.7.1.6 CISCO 2621 M

Tipo de dispositivo	Encaminador
Dimensiones (Ancho x Profundidad x Altura)	44.5 cm X 30 cm X 4.3 cm
Peso	4.7 kg
Procesador	
Tipo	1 x Motorola MPC860P 50 MHz RISC
Memoria RAM	128 MB (instalados) / 256 MB (máx.) - SDRAM - DIMM 100-PIN
Memoria Flash	32 MB (instalados) / 48 MB (máx.)
Tecnología de conectividad	Cableado
Velocidad de transferencia de datos	100 Mbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet

Protocolo de direccionamiento	OSPF, BGP
Protocolo de gestión remota	RMON
Indicadores de estado	Estado puerto, actividad de enlace, alimentación
Características	Diseño modular
Total ranuras de expansión (libres)	4 (4) x Ranura de expansión ¦ 2 (1) x memoria – DIMM 100-PIN ¦ 1 (1) x memoria - SIMM 80-PIN
Interfaces	2 x red - Ethernet 10Base-T/100Base-TX - RJ-45 - 2 ¦ 1 x gestión - consola - RJ-45 - 1 ¦ 1 x red - auxiliar - RJ-45 – 1
Método de autentificación	RADIUS
Cumplimiento de normas	Certificado FCC Clase A, UL, VCCI, EN 60950, EN 61000-3-2, EN55022, NOM, EN 61000-3-3, EN55024

5.8 DISEÑOS DE LA RED

5.8.1 Servicios a prestarse

La red a ser diseñada permitirá brindar servicios con aplicaciones de transmisión y de datos y voz IP. La transmisión de datos no presenta parámetros críticos como la transmisión de voz, para la voz existe un parámetro crítico a ser considerado que es el retardo. El retardo en la transmisión de voz es manejable al utilizar una arquitectura basada en paquetes como

lo es MPLS debido a que a la voz se le puede dar una mayor prioridad que los datos al utilizar calidad de servicio.

El camino a utilizar para transmitir voz sobre MPLS consiste en enviar voz sobre IP (VoIP), para que luego sean encapsuladas sobre la red MPLS. La transmisión de VoIP es más económica que la telefonía mediante conmutación de circuitos. La VoIP es muy apropiada para dar un servicio de larga distancia ya que todas las llamadas son facturadas como locales, el costo no depende de la distancia.

En la transmisión de VoIP; si el terminal es IP como por ejemplo un teléfono IP, un computador multimedia, etc. se tiene a la salida una comunicación con paquetes IP; si el terminal no es IP como puede ser un teléfono convencional se necesita de un dispositivo intermedio que transforme la VoIP en voz analógica.

5.8.2 Área de cobertura

La red propuesta en este proyecto cubrirá a distintas ciudades estratégicas del Ecuador.
En el diseño propuesto se utilizarán 42 nodos con el fin de cubrir todos las subestaciones distribuidas en diferentes locaciones del Ecuador.

Se define como locaciones de los nodos principales a las 3 ciudades mas importanes del Ecuador, Quito, Guayaquil, Cuenca (Ver FIGURA 5.11).

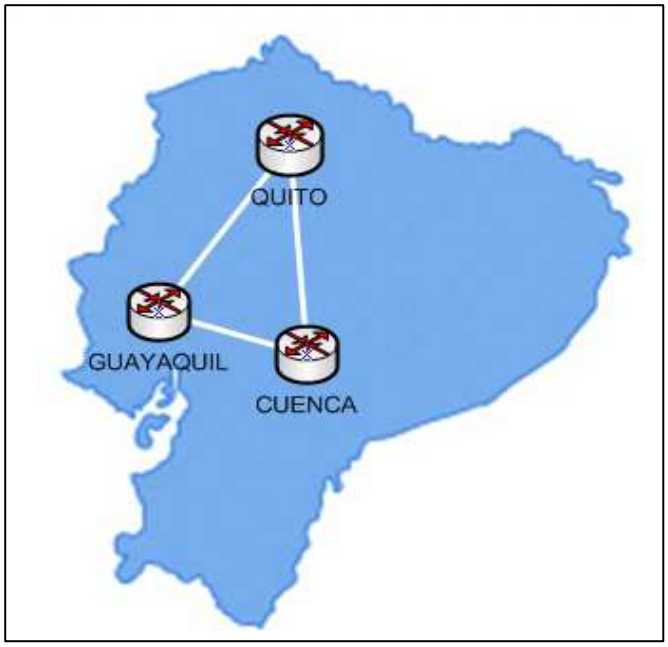


Figura 5.11 Distribución Core MPLS.

5.8.3 Equipos a utilizarse en core MPLS

Los routers con capacidad de conmutación MPLS son los Cisco 2801 y 1841 con los IOS (Internetworking Operating System) SPSERVICES Versión 12.3(14)T4 y ADVENTERPRISE Versión 12.4(9)T respectivamente, que permiten soportar los protocolos y servicios sobre los que se desea realizar el diseño (Ver Anexo 1 Catalogo de equipos)**.**

En la red MPLS de Transelectric S.A se ha descrito la utilización de 3 Routers que formarían el núcleo principal de la red, distribuidos geográficamente en las principales ciudades del Ecuador: Quito, Guayaquil, y Cuenca.

En estos tres nodos principales utilizaremos mencionados routers distribuidos de la siguiente manera:

Quito: Cisco 2800 (P)

Guayaquil: Cisco 1800 (PE)

Cuenca: Cisco 1800 (PE)

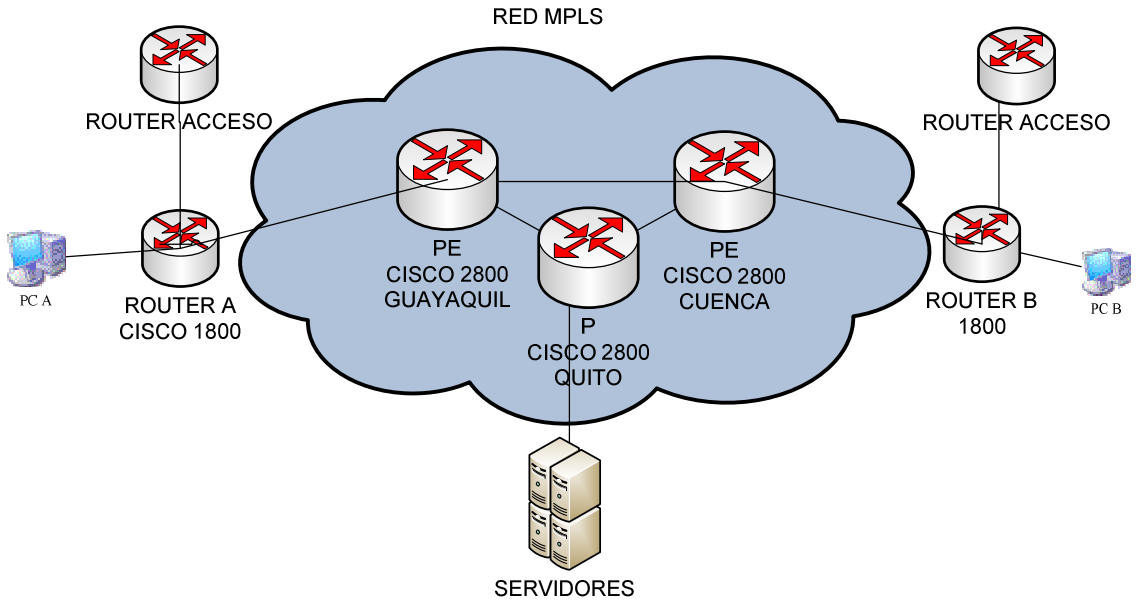


Figura 5.12 Descripción General de la Red

En resumen la red troncal la integran tres routers: Cisco 1841 con funcionalidad PE (Cisco 1841 Guayaquil y Cuenca y un Cisco 2801 Quito con funcionalidad P), capaces "hablar" MPLS.

Cada router PE tiene interconectado un router de acceso con funcionalidad CE (Client-Edge) que a su vez tienen interconectada varias PC. (Ver Anexo 2 Catalogo de Equipos)

5.8.4 Cambios en equipos activos TRANSELECTRIC S.A

NUM	ROUTER	MODELO	NOMBRE
1	cisco	1841	TRANSELEC_TERMOESM
2	cisco	1841	TULCAN
3	cisco	1841	TRANS-IBARRA
4	cisco	1841	POMASQUI
5	cisco	1841	VIECENTINA
6	cisco	1841	STA_ROSA
7	cisco	1841	STO_DOMINGO
8	cisco	1841	QUEVEDO
9	cisco	1841	TRANS-CHONE
10	cisco	1841	ID_PORTOVIEJO
11	cisco	1841	PORTOVIEJO
12	cisco	2801	ROUTER_TE_FO
13	cisco	WS-C3560-24TS	SWITCH CAPA 3
14	cisco	2801	TRANSELECTRIC-9
15	cisco	1841	TRANS_PUYO
16	cisco	1841	PASCUALES
17	cisco	1841	TRANS_CALD
18	cisco	1841	TRANSELECTRIC_AMBATO
19	cisco	1841	TOTORAS-ID
20	cisco	1841	DOS_CERRITOS
21	cisco	1841	SALITRAL
22	cisco	1841	CALDERON>
23	cisco	1841	POLICENTRO_RAD_ISEYCO
24	cisco	2801	POLICENTRO
25	cisco	1841	TOTORAS-TE>
26	cisco	1841	SANTA_ELENA
27	cisco	1841	MILAGRO
28	cisco	1841	RIOBAMBA
29	cisco	1841	TRANS_MULALO

30	cisco	1841	Trinitaria
31	cisco	1841	trans_gye
32	cisco	1841	transele_babahoyo
33	cisco	1841	trans_poso
34	cisco	1841	ZHORAY
35	cisco	1841	SAN_IDELFONSO
36	cisco	1841	MOLINO
37	cisco	1841	WAN_LOJA_CUENCA
38	cisco	2801	CUENCA
39	cisco	2801	SE_MACHALA
40	cisco	1841	LOJA

Tabla 5.11 Cambios en Equipos Activos

5.8.5 Configuración de Equipos.

La primera parte del diseño tiene dos fases. En la primera se configurarán OSPF y BGP. La configuración de OSPF se ha de realizar para que el proceso MPLS pueda conocer la estructura de la red extraída de la base de datos de topología OSPF. La configuración de BGP se hará de cara a la 2ª parte de la práctica, dado que se utilizará en la creación de las VPN implementadas en dicha parte. La segunda fase de este diseño permitirá aprender cómo se configura una red MPLS en routers Cisco.

5.8.5.1 Configuración de una interfaz Loopback

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

cisco# configure terminal cisco(config)# interface loopback<número de la interfaz> cisco(config-if)# ip address <dirección IP> <máscara>

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

5.8.5.2 Configuración de una subinterfaz

La creación y configuración de subinterfaces se realiza siguiendo los siguientes pasos:

cisco# configure terminal cisco(config)# interface fastethernet<nº interfaz>.<nº subinterfaz> cisco(config-subif)# encapsulation dot1Q <VLAN ID>

cisco(config-subif)# ip address <dir IP> <máscara>

NOTA: Levantar la interfaz física (no shutdown).

Ejemplo: *cisco# configure terminal cisco(config)# interface fastethernet0/0.100 cisco(config-subif)# encapsulation dot1Q 2 cisco(config-subif)# ip address 192.168.1.1 255.255.255.0*

5.8.5.3 Configuración básica de OSPF:

Vamos a configurar OSPF como protocolo de routing dinámico en el futuro backbone MPLS.

Recordar que OSPF es un protocolo de routing interno (IGP) del tipo estado de enlace. Los equipos anuncian toda la información al arrancar el protocolo.
Se enviarán entre sí paquetes link state cuando se detectan fallos en algún enlace.

Entonces, todos los routers actualizan la base de datos topológica, se copian los link state e inundan a los vecinos. Por tanto, sólo se van enviando las nuevas actualizaciones de rutas (y no la tabla completa).

Un comando de gran importancia para comprobar las adyacencias OSPF es: *show ip route* Permite ver la tabla de rutas del router donde se ejecuta el comando y si el router aprende las rutas por OSPF.

5.8.5.4 Verificación del estado de OSPF

Podremos comprobar el estado de OSPF por interfaz así como los vecinos OSPF que tendremos en un interfaz, mediante los comandos siguientes:

show ip ospf interface show ip ospf neighbors

5.8.5.5 Configuración Básica de BGP

Antes de configurar MPLS en la red, debemos establecer un full-mesh de sesiones BGP en nuestro backbone y así dejar preparado el escenario de red para la configuración final de MPLS en los routers. El uso de BGP en un dominio MPLS no es “del todo necesario”, ya que se puede implementar una red con funcionalidad MPLS sobre OSPF directamente, el hecho de configurar BGP en un dominio MPLS es para dejarlo preparado por si se quieren crear servicios de redes privadas virtuales sobre MPLS (VPN-MPLS) que sí necesitan la

configuración de un protocolo del tipo de BGP para poder ofrecer servicio. La configuración de BGP requiere los siguientes pasos:

5.8.5.6 Configurar el proceso de routing BGP

cisco# configure terminal cisco(config)# router bgp <número de proceso BGP>
El número de proceso BGP que generalmente se pone es el 65000, para entorno de pruebas, ya que hay otras numeraciones que están reservadas, lo que realmente estamos configurando con el comando *router bgp <numero de proceso BGP>* es el sistema autónomo en el que queremos que se "hable" BGP.

Para cada pareja de routers que estén enfrentados hay que configurar lo siguiente: En uno de los routers especificamos al router vecino y le indicamos que actualice el encaminamiento a través de la interfaz de loopback configurada anteriormente:

cisco(config-router)# neighbor <dir IP de la interfaz del vecino que tiene enfrentada> remote-as <número de proceso BGP > cisco(config-router)# neighbor <dir IP de la interfaz del vecino que tiene
enfrentada > update-source loopback<número de la interfaz>

NOTA: En el caso de que los routers no estén directamente conectados, la dirección IP que hay que indicar es la de la interfaz de loopback configurada en el otro router para que establezcan relaciones de vecindad. En el otro router debemos especificar al router vecino con la interfaz de loopback con la que le hemos indicado que actualice el encaminamiento:

cisco(config-router)# neighbor <dir IP de la interfaz de loopback del vecino> remote-as <número de proceso BGP >

5.8.5.7 Verificación del estado de BGP

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

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

2. *show ip bgp summary* Muestra los routers que mantienen una relación de vecindad con el router en el que se ejecuta el comando, así como el estado en el que se encuentran. **3.** *clear ip bgp* *

Permite resetear las sesiones BGP establecidas.

5.8.5.8 Configuración básica de MPLS

Una vez establecidos los protocolos de routing pasamos a establecer las funcionalidades MPLS en los routers. Para ello hay que arrancar el protocolo de distribución de etiquetas en las distintas interfaces por las que queremos “hablar MPLS”. La configuración de MPLS requiere los siguientes pasos:

Configurar el CEF (*Cisco Express Forwarding*) en todos los routers con funcionalidad “PE” y “P”, CEF es el conjunto de funcionalidades que reúnen los equipos Cisco para poder trabajar en un entorno MPLS entre otras funciones. Los comandos que hay que

ejecutar para activar CEF en un router que soporte estas funcionalidades son: *cisco# configure terminal cisco(config)# ip cef* .

Para comprobar si se ha activado CEF correctamente utilizaremos el siguiente comando: *show ip cef summary* En caso de que no se hubiese habilitado CEF no saldría nada a la salida de este comando.

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

cisco(config)# interface <nombre de la interfaz> cisco(config-if # mpls ip cisco(config-if)# mpls label protocol ldp

5.8.5.9 Verificación del funcionamiento de MPLS en la red

Para realizar la verificación del funcionamiento de MPLS, algunos comandos de interés son los siguientes:

1. *show mpls interfaces* Muestra las interfaces en las que está funcionando MPLS-LDP. **2**. *show mpls ldp parameters* Muestra los parámetros que está utilizando el protocolo en el equipo donde se ejecuta el comando.

2. *show mpls ldp neighbor* Muestra los routers que mantienen una relación de vecindad con el router en el que se ejecuta el comando.

3. *show mpls ldp binding* Muestra la tabla de etiquetas que está utilizando el router donde se ejecuta el comando.

4. *show mpls forwarding-table* Muestra la tabla de *forwarding* del router donde se ejecuta el comando.

5.8.5.10 Configuración de VPNs sobre MPLS

La configuración que se detalla a continuación es para crear VPNs en las que el encaminamiento entre los equipos de cliente (CE) y los equipos del proveedor (PE) se realiza de forma dinámica mediante OSPF y la topología que se generará será totalmente mallada (Full-Mesh).

Hay una configuración distinta según estemos trabajando en un equipo de cliente (CE) o en un equipo de proveedor (PE). Los routers con funcionalidad “CE” van a tener configurado el proceso 255 de OSPF en el área 0 en los enlaces que les unen al backbone MPLS, ya que es el proceso configurado en el backbone. Además, tendrán configurado otro proceso OSPF para las áreas distintas de la cero.

5.8.5.11 Configuración de equipos con funcionalidad PE

La configuración de VPNs sobre MPLS requiere los siguientes pasos en cada uno de los routers con funcionalidad “PE”:

1. Configuración de la VRF asociada a la VPN que vamos a configurar en los routers con funcionalidad “PE”: Una VRF (*VPN routing and forwarding)* incluye las tablas de envío y encaminamiento de los sitios pertenecientes a una VPN. Los parámetros necesarios para crearla son:

Route Distinguisher (RD) que permite identificar unívocamente un prefijo de VPN-IPv4. Route-Target (RT) que identifica los routers que deben recibir la ruta.

cisco# configure terminal cisco (config)# ip vrf <nombre de la VRF> cisco(config-vrf)# rd <valor del rd> cisco(config-vrf)# route-target export <valor que tiene que exportar> cisco(config-vrf)# route-target import <valor que tiene que importar>

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

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

En una topología *Hub & Spoke*, el sitio que hace de “Hub” debe tener un conocimiento de enrutamiento completo de todos los sitios que pertenecen a la misma VPN. Todo el tráfico destinado a la VPN fluirá a través del sitio Hub. Con este tipo de topología, las sedes que hacen de Spoke exportan sus rutas al Hub, por lo que el route-target debe cambiar con respecto a una topología Full-Mesh:

En el sitio que hace de Hub:

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

En el sitio que hace de Spoke:
cisco(config-vrf)# route-target export <valor que importa el Hub > cisco(config-vrf)# route-target import <valor que exportar el Hub>

Configuración del "forwarding" en las interfaces de los routers "PE" que están enfrentadas a los routers "CE":

cisco# configure terminal cisco(config)# interface <nombre de la interfaz> cisco(config-if)# ip vrf forwarding <nombre de la VRF>

Asignación de la dirección IP a la interfaz donde acabamos de configurar el "forwarding" dentro de la VPN, ya que pierde el direccionamiento de dicha interfaz. Después de ejecutar este último comando se mostrará un mensaje indicando que en la interfaz anterior se le ha quitado la configuración IP, por lo que habrá que volver a configurarla: *cisco(config-if)# ip*

address <dirección IP> <máscara>

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

cisco# configure terminal cisco(config)# router ospf <identificador del proceso> vrf <nombre VRF> -

Definir el área en la que se encuentran las interfaces pertenecientes a la VPN:
cisco(config-router)# network <red> <wildcard> area 0

Por ejemplo:

cisco(config-router)# network 192.168.43.0 0.0.0.255 area 0

Configuración de iMBGP: Para que los prefijos aprendidos puedan ser transmitidos a los otros equipos PE, hay que configurar iMBGP siguiendo los siguientes pasos:

Comprobar que los vecinos iBGP siguen activos y operativos. Utilizar el comando *show ip bgp summary*.

Nos metemos en la configuración de BGP del router:

cisco# configure terminal cisco(config)# router bgp <número de proceso BGP que esté configurado>

Entramos a configurar iMBGP para la VPN:

cisco(config-router)# address-family vpnv4

Hay que activar los vecinos existentes con la nueva funcionalidad. Según se vayan ejecutando los comandos siguientes se irán reseteando las sesiones BGP, este comportamiento es normal porque los vecinos renegocian sus "capabilities".

Configurar para cada vecino iBGP mostrado con el comando ***show ip bgp summary*** lo siguiente:

cisco(config-router-af)# neighbor <dir IP del vecino iBGP> activate cisco(config-router-af)# neighbor <dir IP del vecino iBGP> send-community both

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

cisco# Configure terminal cisco(config)# router bgp <número de proceso BGP que esté configurado> cisco(config-router)# address-family ipv4 vrf <nombre del VRF> cisco(config-router-af)# redistribute ospf <identificador del proceso OSPF> vrf <nombre del VRF>

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

cisco# configure terminal cisco(config)# router ospf <identificador del proceso OSPF> vrf <nombre del VRF> cisco(config-router)# redistribute bgp <número de proceso BGP que esté configurado> subnets metric 20

5.8.5.12 Verificación del funcionamiento de la VPN-MPLS

Con los siguientes comandos podremos verificar que la VPN que hemos configurado está funcionando según lo esperado:

show ip route vrf <nombre VRF> Con este comando podremos comprobar los prefijos que se han exportado y los que se han importado en la tabla de routing de la VRF y por ende los prefijos que formarán parte de la VPN.

traceroute vrf <nombre VRF> <Dirección a la que queremos llegar>

El funcionamiento de este comando es exactamente el mismo que el de un traceroute normal, pero para comprobar el funcionamiento de la VPN y usando direcciones destino de la propia VPN, con origen un equipo que pertenezca a la misma VPN necesitamos añadir el parámetro *vrf* junto al nombre de la vrf que pertenece a nuestra VPN.

ping vrf <nombre VRF> <Dirección a la que queremos llegar>

El funcionamiento es exactamente el mismo que el de un ping normal, la explicación del uso del parámetro vrf se aplica exactamente igual que en el comando anterior

5.8.6 Medición del tráfico

En este proyecto se ha realizado el análisis de tráfico entre los elementos activos de la red, a fin de determinar las conclusiones y las diferencias en la mejora de los niveles de trafico con la futura implementación del Multiprotocol Label Switching.

Los niveles de trafico entre los elementos activos de la Red mencionados en la TABLA 5.10 (Equipos Activos en la red de Transelectric S.A), tienen mediciones tomadas en un lapso de 1 mes (Ver Anexo 3 Niveles de tráfico entre los elementos activos).

5.9 MEJORAS CON LA IMPLEMENTACIÓN DE MPLS

Para poder desarrollar el presente diseño, fue necesario estudiar la red de la empresa Transelectric S.A, a partir de la información proporcionada por dicha empresa, conociendo su estructura, funcionamiento, ventajas y desventajas, para realizar la migración a la tecnología MPLS, de la manera más conveniente.

MPLS se presenta como una alternativa de solución óptima, para el adecuado funcionamiento de las redes de telecomunicaciones, ya que separa el envío de datos, de los procedimientos de enrutamiento estándar IP, produciendo beneficios de rendimiento y flexibilidad.

La implementación de MPLS puede mejorar notablemente el rendimiento de la red, debido a la rapidez en la conmutación de etiquetas y la inteligencia del ruteo, dando a la empresa la oportunidad de ofrecer nuevos servicios, que no son posibles con la red Actual, como son: Ingeniería de Tráfico, Calidad de Servicio (QoS), Clases de Servicio (CoS) y creación de VPNs.

Realizando un breve estudio del tráfico en los nodos más relevantes, con ciertos criterios como la topología de la red y redundancia en los nodos, se pudo segmentar la red, para realizar el diseño jerárquico por capas y distribuir el tráfico de la manera más adecuada.

Realizar el monitoreo de forma permanente es un aspecto importante a considerar, ya que permite conocer el estado de cada uno de los enlaces y observar el comportamiento del tráfico dentro de la red.

La tecnología MPLS facilita la implementación de mecanismos de balanceo de carga, para evitar la congestión, utilizando los recursos de la red de manera óptima.

Uno de los resultados considerables que se obtuvo, luego de haber realizado el presente trabajo, es que varios de los equipos con los que cuenta la red actual se conservarán para

formar parte de capa Acceso, donde no se requiere el manejo de MPLS, optimizando de esta manera los recursos de la red.

La migración a la tecnología MPLS será totalmente trasparente para el cliente, debido que la Actual continuará en funcionamiento, hasta que se implemente totalmente el Core MPLS.

Al realizar el estudio de las redes privadas virtuales VPNs con MPLS, se concluye que es una buena alternativa para establecer niveles de seguridad, indispensable para transmisión de datos.

MPLS permite realizar reservación de recursos, a través de protocolos de señalización como RSVP –TE, garantizado Calidad de Servicio en toda la red, características que no se consigue con Ethernet.

Los equipos seleccionados para la implementación de la red MPLS, que mejor se acoplaron a los son los requerimientos planteados, son de la marca comercial CISCO, que es el líder en el desarrollo de hardware, especializado en redes de internetworking.

La fibra óptica, ofrece ventajas relevantes como mayor capacidad para transportar tráfico, por lo que se concluye que la infraestructura de Transelectric S.A trabaja con un medio de transmisión seguro y confiable en toda su extensión.

La tecnología MPLS brinda la posibilidad de unificar múltiples plataformas y mantener requerimientos de diversos clientes para prestación de multiservicios, ya que utiliza las características de capa red con la rapidez de la conmutación de la capa de enlace.

El monitoreo eficiente y continuo de la infraestructura tecnológica de una empresa permite además de llevar un control adecuado de aplicativos, servicios, servidores y equipos de interconectividad, el tomar medidas correctivas con el fin de mantener constante el rendimiento de la misma, adecuarse de manera rápida a las nuevas necesidades y cambios de la empresa, así como también contribuye a tener el Costo total de propiedad lo más bajo posible.

CONCLUSIONES Y RECOMENDACIONES.

Conclusiones

Hoy en día, los proveedores de servicios de telecomunicaciones como Transelectric S.A se encuentran en una continua evolución de sus redes para el soporte de las aplicaciones dominantes, debiendo dar énfasis al estudio de los diferentes parámetros considerados claves para el desarrollo de las redes de explotación de servicios, proporcionando además, una QoS (Quality of Service) real y aceptable para satisfacer las necesidades del usuario.

IP/MPLS ofrece a Transelectric S.A muchos beneficios, incluidos priorización de tráfico, rendimiento de aplicaciones predecible y calidad de servicio integradas. Dado que se trata de una tecnología altamente escalable y menos compleja que sus predecesores, Transelectric S.A gana además en flexibilidad, en reducción y control de costes y carga de trabajo.

Podemos tomar la tecnología MPLS como una puesta de futuro para Transelectric S.A

Actualmente ya ofrece soluciones de enlace muy satisfactorias en cuanto a resultados de rendimiento y proporcionan una nueva forma de gestionar los recursos de forma fiable y segura a otras empresas.

Todo apunta a que en no mucho tiempo podremos ver este estándar implantado en casi la totalidad de las redes de gran envergadura. Todas las miradas apuntan a esta novedosa tecnología como el paso final a la evolución de las tecnologías de conmutación multinivel.

La idea básica de separar lo que es el envío de los datos (mediante el algoritmo de intercambio de etiquetas) de los procedimientos de encaminamiento estándar IP, ha llevado a un acercamiento de los niveles 2 y 3, con el consiguiente beneficio en cuanto a rendimiento y flexibilidad de esta arquitectura.

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

Recomendaciones

- Se recomienda desarrollar el diseño planteado, ya permite obtener grandes beneficios de la tecnología utilizada, como acceder a nuevos servicios, satisfaciendo los requerimientos de los usuarios.

- La instalación de los equipos debe cumplir con todas las especificaciones y normas técnicas dadas por el fabricante, para obtener los parámetros adecuados y el buen desempeño de la red Se recomienda realizar un estudio de GMPLS que es una extensión de la tecnología MPLS, la misma que forma parte de las redes ópticas de nueva generación, que ofrece servicios como proveer de mayor ancho de banda al usuario final.

- Si se pretende implementar el presente Proyecto, se debería realizar un análisis completo y de costos en base de los requerimientos de la red.

- Se recomienda que los equipos ubicados en cada uno de los nodos de capa Core, estén correctamente etiquetados, para poder identificar con facilidad cualquier tipo de dispositivo que presente inconvenientes.

BIBLIOGRAFÍA

- Manuales de Configuración de CISCO, http://hondo.diatel.upm.es/manuales/cisco

- Resumen, autores E. Rosen, A. Viswanathan, R. Callon, “Multiprotocol Label Switching Architecture”, RFC-3031, January 2001.

- Resumen, autores, D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus, “Requirements for Traffic Engineering Over MPLS”, RFC-2702, September 1999.

- Libro, autores P. Bhaniramka, W. Sun, R. Jain, “Quality of Service using Traffic Engineering over MPLS: An Analysis”, September 2000

- Manual, autor David Allan, Guidelines for MPLS load balancing, draft-allan-mpls-loadbal-04, IETF(April 2003).

- Manual, autores D. Awduche y J. Malcolm, Requirements for traffic engineering over MPLS RFC2702, IETF (1999).

- Manual, autores F. Baccelli and P. Bremaud, Elements of queueing theory - palm martingale calculus and stochastic recurrences, Springer-Verlag, 1994.

- Libro, autores R. Braden, D. Clark, and S Shenker, Integrated services in the internet architecture: An overview RFC 1633, IETF (Jun. 1994).

- Manual, autor Ramon Casellas, MPLS trafic engineering,

- Resumen, introducción a las tecnologías MPLS y GMPLS , autores Xavier Hesselbach, Mónica Huerta, Oscar Calderón

- Resumen, autor Julio Alba Soto, http://isa.uniovi.es/~sirgo/doctorado/VPN.pdf

- Resumen, autor José Luis Ruiz González, VPN redes virtuales http://isa.uniovi.es/~sirgo/doctorado/VPN.pdf

- Manual, autor Munther Louis Antoun, MPLS VPN configuration and Design Guide

- Libro, CONNECTION-ORIENTED NETWORKS SONET/SDH,ATM, MPLS and Optical Networks, autor Harry G. Perros

- Resumen, autor Santiago Felici, Servicios diferenciados y MPLS, http://www.slidefinder.net/D/docto_mpls/7865269

- Síntesis, autor anónimo, Actualidad y futuro de las redes ópticas, http://www.ercoasl.com/index.php/id/2/objeto/11/claves/Actualidad-y-futuro-de-las-redes-opticas

- Libro, autor SonicWALL, MPLS y VPN IPSec Optimización de la seguridad en la WAN de empresa

- Manual, autor anónimo, CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO O MPLS (MultiProtocolLabelSwitching), http://www.idg.es/pcworldtech/mostrarArticulo.asp?id=177545&seccion

- Resumen, autor Pablo Belzarena, Ingeniería de tráfico en línea en redes MPLS aplicando la teoría de grandes desviaciones, http://iie.fing.edu.uy/publicaciones/2003/Bel03/Bel03.pdf

- Monografías, autor Jorge Hernández, MPLS, http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml

- Libro, autores Homero Ortega Boada, Carolina Villabona R., Wilder E. Castellanos H, IP sobre ATM - clave en la convergencia de las comunicaciones.

- Manual, autor María Sol Canalis, MPLS MULTI PROTOCOL LABEL SWITCHING- Una Arquitectura de Backbone para la Internet del Siglo XXI, http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/libmpls.PDF
- Manual Cisco Advanced MPLS Design and Implementation, www.cisco.com/warp/public/cc/pd/hb/vp5000/prodlit/iplsc_wp.htm

- Manual, autor Camilo Andrés Llerena, Karen Villacob Pineda, MPLS conmutación de etiquetas multiprotocolo

- Manual Cisco − Configuring VPN MPLS over ATM with Cisco 7500 Routers and LightStream 1010 Switches, http://docstore.mik.ua/cisco/pdf/other/Configuring%20Vpn%20Mpls%20Over%20Atm%20With%20Cisco%207500%20Routers%20And%20Lightstream%201010%20Switches.pdf

- Manual, Rápido de Configuración MPLS y BGP de un Router Cisco, http://hondo.diatel.upm.es/manuales/cisco

- Libro, autor Daniel Monoli, Voice over MPLS Planning and Designing Networks

- Síntesis, autor Miguel Rodríguez, Conectividad segura virtual MPLS, http://www.seguridadinformatica.es/profiles/blog/list?user=seguridad0

- Resumen, autor Hugo Zamora, Implementación de redes MPLS- VPN , Casos de estudio, http://www.cudi.edu.mx/primavera2002/presentaciones/MPLSVPN.pdf

- Libro, autores Xavier Hesselbach, Mónica Huerta, Oscar Calderón, Problemas abiertos en MPLS, Migración, Protección, Gestión de Recursos y Balanceo de Carga

ANEXOS

6.1 ANEXO 1
Catálogos equipos

6.1.1 Cisco 2801 Integrated Services Router

- Tipo de dispositivo: Encaminador

- Factor de forma: Externo - modular - 1U

- Dimensiones (Ancho x Profundidad x Altura): 43.8 cm x 41.9 cm x 4.5 cm

- Peso: 6.2 kg

- Memoria RAM: 128 MB (instalados) / 384 MB (máx.)

- Memoria Flash: 64 MB (instalados) / 128 MB (máx.)

- Protocolo de interconexión de datos: Ethernet, Fast Ethernet

- Red / Protocolo de transporte: IPSec

- Protocolo de gestión remota: SNMP 3

- Características: Cisco IOS , cifrado del hardware, soporte de MPLS

- Alimentación: CA 120/230 V (50/60 Hz)

- Requisitos del sistema: Microsoft Windows 98 Second Edition

General

- Tipo de dispositivo Encaminador
- Factor de forma Externo - modular - 1U
- Anchura 43.8 cm
- Profundidad 41.9 cm
- Altura 4.5 cm
- Peso 6.2 kg

Memoria

- Memoria RAM 128 MB (instalados) / 384 MB (máx.)
- Memoria Flash 64 MB (instalados) / 128 MB (máx.)

Conexión de redes

- Tecnología de conectividad Cableado
- Protocolo de interconexión de datos Ethernet, Fast Ethernet
- Red / Protocolo de transporte IPSec
- Protocolo de gestión remota SNMP 3
- Características Cifradas del hardware, soporte de MPLS

Comunicaciones

- Tipo DSU/CSU

Expansión / Conectividad

- Total ranuras de expansión (libres) 2 (2) x HWIC
- 2 (2) x AIM
- 2 (2) x PVDM
- 1 (1) x WIC
- 1 (1) x VIC
- 1 memoria
- 1 Tarjeta CompactFlash
- Interfaces 2 x red - Ethernet 10Base-T/100Base-TX - RJ-45
- 1 x USB
- 1 x red - auxiliar
- 1 x gestión - consola

Diverso

- Algoritmo de cifrado DES, Triple DES, AES
- Cumplimiento de normas CISPR 22 Class A, CISPR 24, EN 61000-3-2, VCCI Class A ITE, IEC 60950, EN 61000-3-3, EN55024, EN55022 Class A, UL 60950, EN50082-1, CSA 22.2 No. 60950, AS/NZ 3548 Class A, JATE, FCC Part 15, ICES-003 Class A, CS-03, EN 61000-6-2

Alimentación

- Dispositivo de alimentación Fuente de alimentación - interna
- Voltaje necesario CA 120/230 V (50/60 Hz)

Software / Requisitos del sistema

- OS prorporcionado Cisco IOS
- Sistema operativo requerido Microsoft Windows 98 Second Edition

Parámetros de entorno

- Temperatura mínima de funcionamiento 0 °C
- Temperatura máxima de funcionamiento 40 °C
- Ámbito de humedad de funcionamiento 10 - 85%

6.1.2 Cisco 1841 Security Bundle

-Tipo de dispositivo: Encaminador

- Factor de forma: Externo - modular - 1U

- Dimensiones (Ancho x Profundidad x Altura): 34.3 cm x 27.4 cm x 4.8 cm

- Peso: 2.8 kg

- Memoria RAM: 256 MB (instalados) / 384 MB (máx.) - SDRAM

- Memoria Flash: 64 MB (instalados) / 128 MB (máx.)

- Protocolo de interconexión de datos: Ethernet, Fast Ethernet

- Red / Protocolo de transporte: IPSec

- Protocolo de gestión remota: SNMP, HTTP

- Características: Cisco IOS , protección firewall, cifrado del hardware, asistencia técnica VPN, soporte VLAN, Sistema de prevención de intrusiones (IPS), montable en pared, Dynamic Multipoint VPN (DMVPN), Network Admissions Control (NAC)

- Alimentación: CA 120/230 V (50/60 Hz)

General

Tipo de dispositivo Encaminador

Factor de forma Externo - modular - 1U

Cantidad de módulos instalados (máx.) 1 (instalados) / 3 (máx.)

Anchura 34.3 cm

Profundidad 27.4 cm

Altura 4.8 cm

Peso 2.8 kg

Memoria

Memoria RAM 256 MB (instalados) / 384 MB (máx.) - SDRAM

Memoria Flash 64 MB (instalados) / 128 MB (máx.)

Conexión de redes

Tecnología de conectividad Cableado

Protocolo de interconexión de datos Ethernet, Fast Ethernet

Red / Protocolo de transporte IPSec

Protocolo de gestión remota SNMP, HTTP

Capacidad Conexiones SSL concurrentes : 10

Características Protección firewall, cifrado del hardware, asistencia técnica VPN, soporte VLAN, Sistema de prevención de intrusiones (IPS), montable en pared, Dynamic Multipoint VPN (DMVPN), Network Admissions Control (NAC)

Expansión / Conectividad

Total ranuras de expansión (libres) 1 Tarjeta CompactFlash

Memoria

1 (0) x AIM

2 (2) x HWIC

Interfaces 2 x red - Ethernet 10Base-T/100Base-TX - RJ-45

1 x USB

1 x gestión - consola

1 x gestión - auxiliar

Diverso

Kit de montaje en bastidor Opcional

Algoritmo de cifrado DES, Triple DES, AES, SSL

Método de autentificación Secure Shell v.2 (SSH2)

Cumplimiento de normas CSA, CTR 21, CISPR 22 Class A, CISPR 24, EN 60950, EN 61000-3-2, IEC 61000-4-11, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, EN 61000-3-3, EN55024, EN55022 Class A, EN50082-1, EN 61000-4-4, EN 61000-4-2, EN 61000-4-3, EN 61000-4-6, CS-03, EN 61000-4-5, UL 60950-1

Alimentación

Dispositivo de alimentación Fuente de alimentación - interna

Voltaje necesario CA 120/230 V (50/60 Hz)

Potencia suministrada 50 vatios

Software / Requisitos del sistema

OS prorporcionado Cisco IOS

Software incluido Cisco IOS Advanced IP Services

Parámetros de entorno

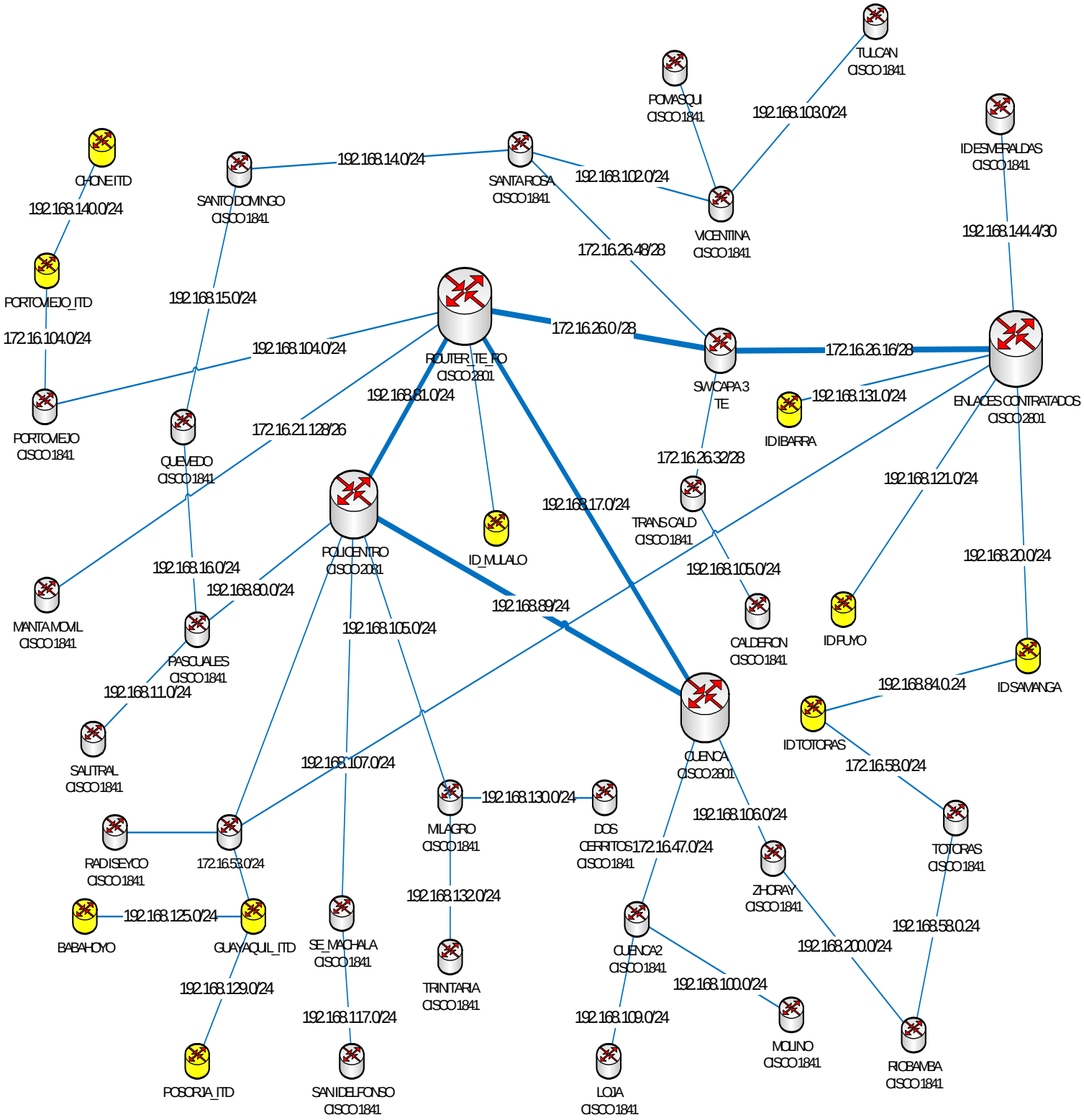
Temperatura mínima de funcionamiento 0 °C

Temperatura máxima de funcionamiento 40 °C

Ámbito de humedad de funcionamiento 10 - 85%

6.2 ANEXO 2

Diseño de la red mpls



6.3 ANEXO 3

Análisis de tráfico entre los elementos activos de la red

Et0 on ENLACE ID BABAHOYO (172.16.125.1)							
	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	9.566,56	1,727	25.334,28	4,535	34.900,84	6,262	53
08/02/2010	17.102,27	1,674	99.416,22	9,594	116.518,48	11,268	98
07/02/2010	7.740,40	0,736	22.464,80	2,132	30.205,21	2,867	100
06/02/2010	17.783,39	1,697	64.480,54	6,142	82.263,93	7,838	99
03/02/2010	10.345,32	1,576	60.930,52	9,38	71.275,84	10,956	62
02/02/2010	22.754,72	2,39	78.234,28	8,146	100.989,00	10,536	91
01/02/2010	19.828,56	1,903	74.572,45	7,109	94.401,01	9,012	99
31/01/2010	14.185,65	1,385	90.608,21	8,692	104.793,86	10,076	98
30/01/2010	7.730,18	0,741	33.032,72	3,151	40.762,90	3,892	99
29/01/2010	8.454,53	0,813	40.454,89	3,882	48.909,42	4,695	99
28/01/2010	21.738,96	2,055	48.731,05	4,619	70.470,02	6,674	100
27/01/2010	27.552,78	2,73	122.347,67	11,809	149.900,45	14,538	97
26/01/2010	19.024,38	2,993	83.630,93	12,785	102.655,31	15,777	61
25/01/2010	10.917,90	1,602	71.335,77	10,317	82.253,66	11,919	65
24/01/2010	20.798,38	2,11	116.483,62	11,733	137.282,00	13,843	94
23/01/2010	15.129,79	1,603	115.985,71	11,834	131.115,49	13,437	91
22/01/2010	8.718,15	0,842	37.880,02	3,603	46.598,18	4,445	99
21/01/2010	7.929,55	0,766	50.802,39	4,846	58.731,94	5,612	99
20/01/2010	21.280,21	2,052	103.871,52	9,893	125.151,73	11,945	99
19/01/2010	14.916,66	1,423	41.482,98	3,956	56.399,64	5,378	99
18/01/2010	15.808,40	1,512	65.932,47	6,279	81.740,87	7,791	99
17/01/2010	22.528,68	2,161	84.013,66	8,198	106.542,34	10,36	98
16/01/2010	15.510,56	1,504	55.011,48	5,308	70.522,04	6,812	98
15/01/2010	26.603,35	2,559	70.329,48	6,678	96.932,82	9,237	99
14/01/2010	13.900,71	1,357	87.330,58	8,434	101.231,29	9,791	98
13/01/2010	12.346,13	1,196	60.989,47	5,882	73.335,60	7,078	98
12/01/2010	17.251,16	1,941	38.910,23	4,346	56.161,38	6,287	85
11/01/2010	17.958,19	1,736	58.086,70	5,563	76.044,89	7,299	99
10/01/2010	19.820,20	1,981	107.219,15	10,488	127.039,35	12,469	96
09/01/2010	20.179,29	1,985	100.714,44	9,745	120.893,73	11,731	97

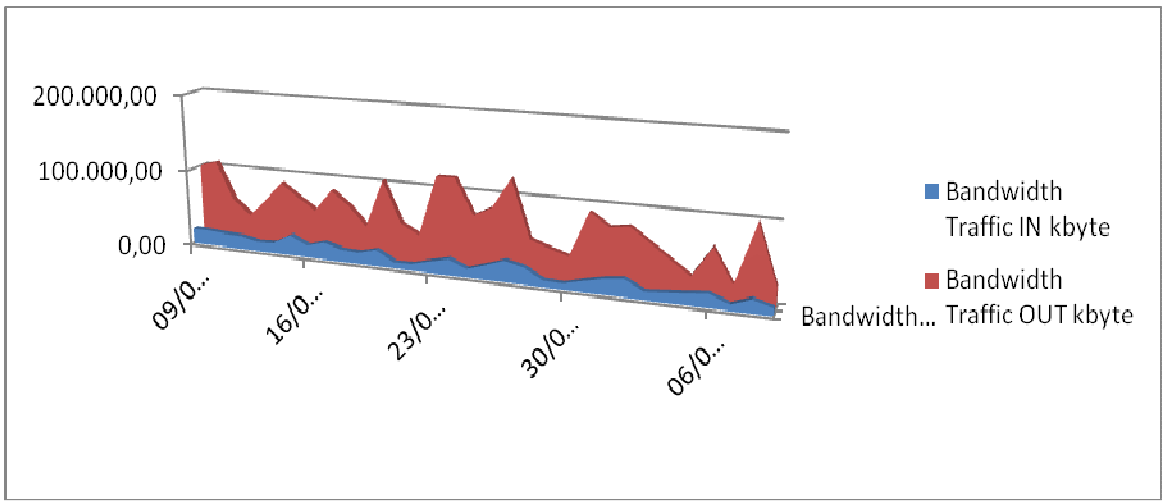


Tabla 5.11 Elemento Babahoyo

Calderon Port Fa4 (172.16.55.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	7.354.656,69	1.300,23	16.132.226,55	2.852,00	23.486.883,24	4.152,24	54
08/02/2010	20.419.145,36	1.936,38	39.564.952,73	3.752,01	59.984.098,09	5.688,38	100
07/02/2010	12.784.786,44	1.212,40	689.879,78	65,422	13.474.666,23	1.277,82	100
06/02/2010	14.717.813,00	1.395,71	4.333.249,28	410,926	19.051.062,27	1.806,63	100
05/02/2010	23.266.792,45	2.981,57	35.755.292,23	4.581,94	59.022.084,69	7.563,51	74
03/02/2010	3.642.459,94	544,687	1.068.233,67	162,33	4.710.693,61	707,017	63
02/02/2010	22.697.780,88	2.152,39	42.299.208,85	4.011,16	64.996.989,73	6.163,55	100
01/02/2010	22.403.661,52	2.124,51	92.716.435,01	8.792,20	115.120.096,52	10.916,72	100
31/01/2010	18.369.767,37	1.741,98	14.355.582,49	1.361,33	32.725.349,86	3.103,31	100
30/01/2010	18.880.225,60	1.790,35	37.925.890,96	3.596,39	56.806.116,56	5.386,74	100
29/01/2010	27.397.335,20	2.598,07	37.630.612,38	3.568,48	65.027.947,58	6.166,54	100
28/01/2010	20.681.750,67	1.961,20	52.510.120,83	4.979,42	73.191.871,50	6.940,62	100
27/01/2010	18.226.455,47	1.728,39	35.901.772,59	3.404,52	54.128.228,06	5.132,91	100
26/01/2010	23.001.272,33	3.444,30	31.299.031,98	4.689,41	54.300.304,31	8.133,71	63
25/01/2010	3.817.805,91	514,111	9.075.148,98	1.222,07	12.892.954,89	1.736,18	70
24/01/2010	11.200.503,99	1.062,12	451.571,25	42,821	11.652.075,24	1.104,94	100
23/01/2010	14.148.811,93	1.341,71	34.574.604,08	3.278,65	48.723.416,01	4.620,35	100
22/01/2010	30.231.825,62	2.866,85	37.433.747,28	3.549,81	67.665.572,90	6.416,65	100
21/01/2010	18.241.184,69	1.729,78	36.382.689,83	3.450,11	54.623.874,52	5.179,88	100
20/01/2010	21.290.188,13	2.018,90	37.961.467,34	3.599,80	59.251.655,46	5.618,71	100
19/01/2010	22.258.409,00	2.110,74	37.820.667,14	3.586,48	60.079.076,14	5.697,22	100
18/01/2010	21.010.389,84	1.992,36	39.795.318,15	3.773,69	60.805.707,98	5.766,05	100
17/01/2010	13.964.154,14	1.324,21	865.002,09	82,027	14.829.156,23	1.406,23	100
16/01/2010	77.070.190,17	7.308,45	40.575.825,44	3.847,74	117.646.015,61	11.156,19	100
15/01/2010	9.369.828,25	888,496	70.941.787,91	6.727,10	80.311.616,15	7.615,59	100
14/01/2010	16.839.955,25	1.596,99	49.379.566,49	4.682,84	66.219.521,74	6.279,83	100
13/01/2010	9.196.917,04	872,12	38.518.231,02	3.652,59	47.715.148,06	4.524,71	100
12/01/2010	7.628.380,79	848,031	37.527.177,71	4.173,49	45.155.558,50	5.021,52	85
11/01/2010	7.231.656,72	685,789	37.116.456,88	3.519,81	44.348.113,60	4.205,60	100
10/01/2010	998.612,54	94,7	560.202,41	53,125	1.558.814,95	147,825	100
09/01/2010	1.808.932,43	171,54	34.572.577,55	3.278,50	36.381.509,98	3.450,04	100

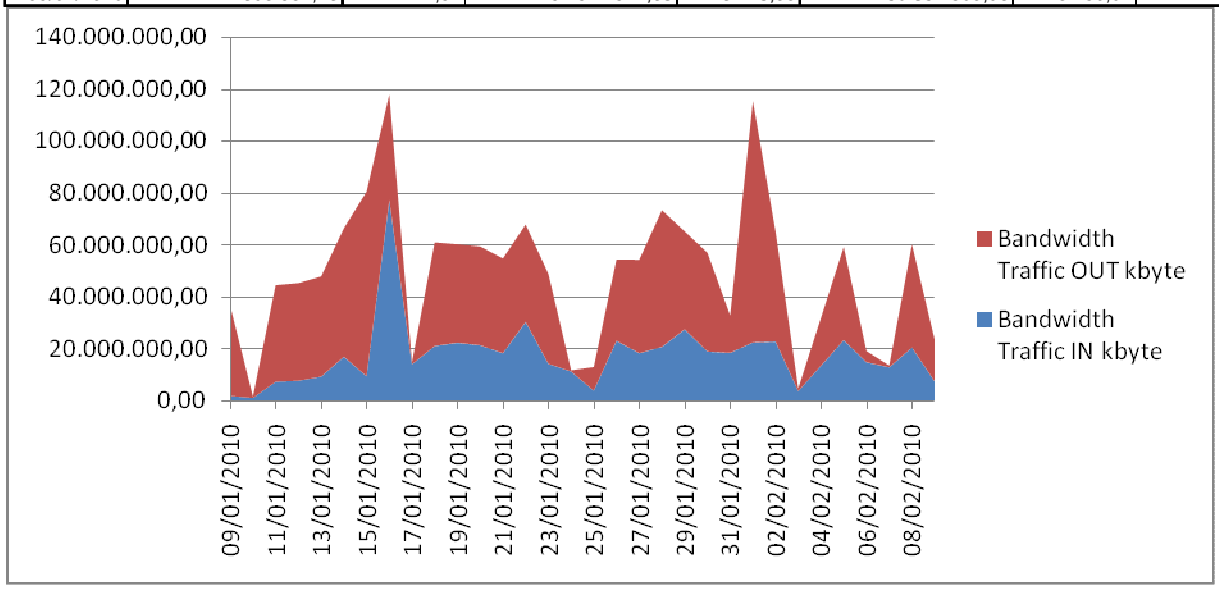


Tabla 5.12 Calderón

FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	79.893,09	14,123	412.125,95	72,851	492.019,05	86,973	54
08/02/2010	153.017,51	14,511	1.116.303,04	105,861	1.269.320,55	120,371	100
07/02/2010	128.755,43	12,21	1.212.916,05	115,022	1.341.671,48	127,232	100
06/02/2010	139.915,55	13,268	1.623.870,94	153,992	1.763.786,49	167,26	100
05/02/2010	134.210,88	17,192	683.942,70	87,613	818.153,58	104,806	74
03/02/2010	115.917,50	17,334	618.591,07	94	734.508,57	111,333	63
02/02/2010	279.577,99	26,512	1.573.659,79	149,227	1.853.237,77	175,739	100
01/02/2010	245.436,53	23,274	728.879,84	69,119	974.316,38	92,393	100
31/01/2010	199.268,73	18,896	981.109,96	93,037	1.180.378,70	111,934	100
30/01/2010	157.810,88	14,965	802.376,96	76,088	960.187,84	91,053	100
29/01/2010	221.769,15	21,03	1.006.316,14	95,427	1.228.085,29	116,457	100
28/01/2010	230.248,06	21,834	670.042,73	63,539	900.290,79	85,373	100
27/01/2010	218.813,39	20,75	693.288,21	65,744	912.101,59	86,493	100
26/01/2010	193.427,36	28,932	733.906,11	109,833	927.333,47	138,765	63
25/01/2010	199.416,34	26,841	1.334.558,17	179,626	1.533.974,52	206,466	70
24/01/2010	219.320,38	20,798	722.941,21	68,555	942.261,60	89,353	100
23/01/2010	198.661,40	18,839	834.944,41	79,176	1.033.605,81	98,015	100
22/01/2010	223.674,81	21,211	639.717,44	60,664	863.392,25	81,874	100
21/01/2010	214.663,07	20,356	976.924,22	92,64	1.191.587,28	112,996	100
20/01/2010	245.566,73	23,337	438.614,24	41,593	684.180,96	64,93	100
19/01/2010	327.195,18	31,028	1.162.860,69	110,273	1.490.055,87	141,3	100
18/01/2010	188.624,25	17,887	761.059,26	72,17	949.683,51	90,056	100
17/01/2010	183.203,12	17,373	1.185.734,64	112,442	1.368.937,76	129,814	100
16/01/2010	163.910,62	15,543	518.242,66	49,144	682.153,28	64,687	100
15/01/2010	168.642,45	16,003	565.959,36	53,669	734.601,81	69,672	100
14/01/2010	235.257,57	22,31	1.590.075,00	150,789	1.825.332,57	173,099	100
13/01/2010	157.956,04	14,979	692.429,48	65,663	850.385,52	80,641	100
12/01/2010	197.948,45	21,878	1.344.407,55	148,651	1.542.356,00	170,529	86
11/01/2010	153.599,63	14,566	548.268,98	51,993	701.868,61	66,559	100
10/01/2010	158.195,85	15,002	785.045,07	74,447	943.240,91	89,449	100
09/01/2010	209.802,46	19,895	1.152.746,36	109,315	1.362.548,82	129,211	100

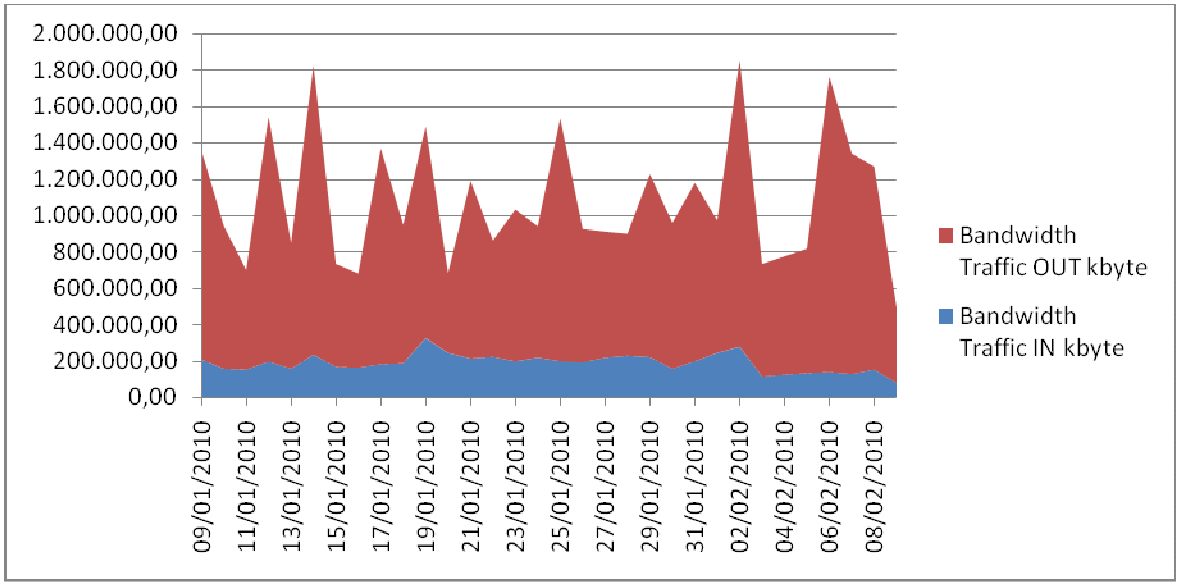


Tabla 5.13 Cuenca Capulispamba

Port Et0 on CHONE - INTEGRAL DATA (172.16.140.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	7.971,83	1,411	74.238,35	13,173	82.210,18	14,584	54
08/02/2010	22.103,82	2,101	185.174,29	17,573	207.278,11	19,673	100
07/02/2010	9.602,37	0,911	42.322,30	4,016	51.924,66	4,927	100
06/02/2010	4.060,26	0,385	21.628,09	2,051	25.688,34	2,436	100
05/02/2010	11.126,42	1,429	62.120,39	7,967	73.246,81	9,395	74
03/02/2010	11.717,08	1,762	171.577,92	26,324	183.295,00	28,086	62
02/02/2010	8.538,49	1,17	109.499,13	10,304	118.037,62	11,474	85
01/02/2010	22.718,83	2,143	224.258,15	20,926	246.976,98	23,069	101
31/01/2010	12.039,46	1,142	102.403,46	9,711	114.442,92	10,853	100
30/01/2010	13.421,66	1,273	91.266,38	8,661	104.688,04	9,933	100
29/01/2010	16.927,10	1,605	152.235,69	14,3	169.162,80	15,905	100
28/01/2010	8.470,02	0,796	51.542,09	4,845	60.012,11	5,641	101
27/01/2010	19.606,62	1,866	200.311,06	19,022	219.917,68	20,888	100
26/01/2010	9.866,04	1,48	118.338,71	17,725	128.204,75	19,205	63
25/01/2010	10.487,81	1,412	39.374,16	5,3	49.861,96	6,711	70
24/01/2010	9.770,05	0,926	63.980,81	6,011	73.750,86	6,937	100
23/01/2010	7.940,23	0,754	41.497,61	3,935	49.437,83	4,689	100
22/01/2010	4.970,42	0,471	25.889,30	2,455	30.859,72	2,926	100
21/01/2010	9.709,53	0,921	70.736,74	6,713	80.446,27	7,633	100
20/01/2010	7.744,23	0,734	39.439,39	3,74	47.183,62	4,474	100
19/01/2010	12.219,74	1,16	91.521,78	8,685	103.741,52	9,845	100
18/01/2010	12.223,59	1,161	112.326,91	10,666	124.550,49	11,827	100
17/01/2010	9.197,40	0,873	80.145,12	7,619	89.342,52	8,492	100
16/01/2010	22.481,35	2,132	168.225,93	15,667	190.707,28	17,799	101
15/01/2010	17.594,47	1,671	101.815,25	9,574	119.409,72	11,245	100
14/01/2010	15.215,55	1,461	119.235,68	11,355	134.451,23	12,816	99
13/01/2010	13.596,88	1,289	114.727,63	10,894	128.324,51	12,184	100
12/01/2010	4.974,71	0,551	20.433,40	2,259	25.408,11	2,81	86
11/01/2010	10.069,64	0,955	42.046,62	3,99	52.116,26	4,945	100
10/01/2010	24.506,90	2,326	165.167,61	15,674	189.674,51	18	100
09/01/2010	15.094,53	1,434	137.753,29	13,072	152.847,82	14,507	100

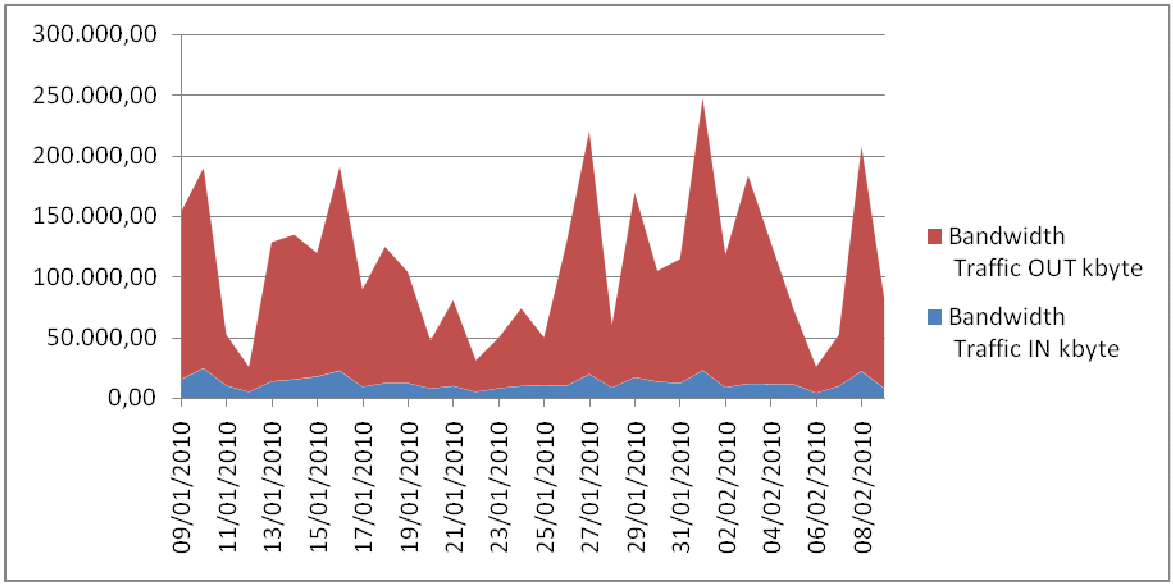


Tabla 5.14 Chone

Port Fa0/0 on DOS CERRITOS (172.16.130.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	7.461,48	1,314	40.623,61	7,153	48.085,09	8,467	54
08/02/2010	38.608,14	3,661	278.973,88	26,455	317.582,02	30,117	100
07/02/2010	32.147,82	3,049	478.935,73	45,481	511.083,55	48,529	100
06/02/2010	21.413,30	2,031	153.334,32	14,541	174.747,63	16,571	100
05/02/2010	18.714,82	2,402	194.377,85	24,899	213.092,67	27,301	74
03/02/2010	11.225,94	1,68	51.711,10	7,858	62.937,04	9,538	63
02/02/2010	14.341,85	1,362	89.338,81	8,478	103.680,66	9,84	100
01/02/2010	24.160,81	2,293	207.202,84	19,649	231.363,66	21,941	100
31/01/2010	24.301,27	2,304	335.676,51	31,875	359.977,78	34,18	100
30/01/2010	18.887,72	1,794	172.361,12	16,345	191.248,84	18,138	100
29/01/2010	16.673,65	1,582	63.356,24	6,008	80.029,88	7,59	100
28/01/2010	25.849,16	2,451	84.614,02	8,024	110.463,18	10,475	100
27/01/2010	29.635,37	2,81	214.260,12	20,347	243.895,49	23,157	100
26/01/2010	11.262,08	1,685	83.139,71	12,459	94.401,79	14,144	63
25/01/2010	6.905,48	0,93	36.452,81	4,909	43.358,29	5,839	70
24/01/2010	23.344,98	2,217	405.897,87	38,491	429.242,85	40,707	100
23/01/2010	17.241,21	1,636	271.475,88	25,78	288.717,09	27,416	100
22/01/2010	18.242,74	1,731	113.273,26	10,742	131.516,00	12,473	100
21/01/2010	53.325,04	5,057	112.160,20	10,636	165.485,25	15,693	100
20/01/2010	24.519,83	2,328	147.244,49	13,992	171.764,32	16,32	100
19/01/2010	17.696,11	1,68	186.739,97	17,721	204.436,08	19,401	100
18/01/2010	17.593,47	1,67	99.022,17	9,39	116.615,64	11,06	100
17/01/2010	39.532,14	3,754	125.286,30	11,889	164.818,44	15,643	100
16/01/2010	11.401,00	1,081	66.303,86	6,292	77.704,86	7,373	100
15/01/2010	17.381,75	1,649	91.396,34	8,594	108.778,09	10,244	100
14/01/2010	16.611,51	1,575	77.319,59	7,348	93.931,10	8,923	100
13/01/2010	12.551,90	1,192	74.761,53	7,103	87.313,43	8,295	100
12/01/2010	24.000,01	2,662	127.611,75	14,16	151.611,75	16,822	85
11/01/2010	24.584,22	2,333	98.316,89	9,343	122.901,10	11,676	100
10/01/2010	15.071,68	1,431	75.697,21	7,198	90.768,89	8,63	100
09/01/2010	17.847,18	1,692	81.732,86	7,751	99.580,04	9,443	100

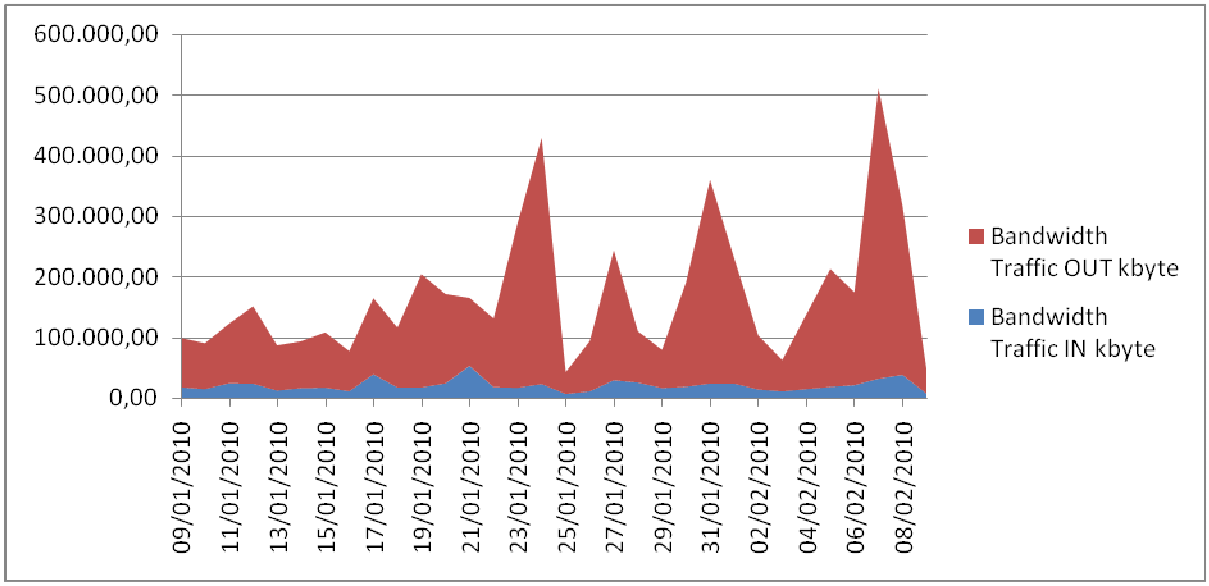


Tabla 5.15 Dos Cerritos

Fa0 on LOJA (172.16.92.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	6.342,32	1,116	35.752,61	6,291	42.094,93	7,407	54
08/02/2010	7.784,88	0,738	47.539,65	4,508	55.324,52	5,246	100
07/02/2010	15.492,76	1,469	202.858,85	19,237	218.351,62	20,706	100
06/02/2010	7.638,78	0,724	46.703,83	4,429	54.342,61	5,153	100
05/02/2010	6.903,56	0,884	33.747,78	4,323	40.651,34	5,208	74
03/02/2010	6.553,69	0,98	52.114,11	7,919	58.667,80	8,899	63
02/02/2010	21.183,28	2,031	62.055,14	5,95	83.238,41	7,981	99
01/02/2010	16.122,12	1,543	141.353,81	13,529	157.475,92	15,072	99
31/01/2010	23.849,30	2,262	216.037,62	20,487	239.886,92	22,748	100
30/01/2010	14.701,56	1,394	149.380,37	14,165	164.081,93	15,56	100
29/01/2010	10.055,55	0,954	61.259,97	5,809	71.315,52	6,763	100
28/01/2010	10.670,70	1,012	65.574,28	6,218	76.244,98	7,23	100
27/01/2010	9.148,29	0,868	53.368,90	5,061	62.517,19	5,928	100
26/01/2010	6.592,76	0,988	44.853,82	6,727	51.446,58	7,715	63
25/01/2010	8.096,43	1,09	79.672,67	10,723	87.769,10	11,813	70
24/01/2010	7.450,95	0,707	53.087,32	5,034	60.538,27	5,741	100
23/01/2010	9.151,68	0,868	72.471,42	6,872	81.623,09	7,74	100
22/01/2010	8.521,04	0,818	42.335,62	4,06	50.856,66	4,877	99
21/01/2010	15.460,05	1,466	132.274,31	12,428	147.734,36	13,894	100
20/01/2010	50.282,45	4,844	37.054,99	3,562	87.337,44	8,407	99
19/01/2010	139.447,68	13,224	44.528,09	4,223	183.975,77	17,446	100
18/01/2010	10.175,91	0,965	150.150,52	14,238	160.326,43	15,203	100
17/01/2010	9.748,94	0,976	122.365,56	12,254	132.114,50	13,23	95
16/01/2010	6.337,31	0,601	30.274,05	2,871	36.611,36	3,472	100
15/01/2010	12.889,51	1,243	122.932,85	11,851	135.822,37	13,094	98
14/01/2010	12.755,84	1,21	189.558,06	17,976	202.313,90	19,186	100
13/01/2010	8.631,25	0,818	34.480,66	3,27	43.111,90	4,088	100
12/01/2010	5.913,84	0,657	33.830,87	3,759	39.744,71	4,415	85
11/01/2010	7.046,48	0,668	56.972,22	5,403	64.018,71	6,071	100
10/01/2010	6.829,40	0,648	32.456,63	3,078	39.286,02	3,726	100
09/01/2010	15.911,85	1,509	317.624,45	30,12	333.536,30	31,629	100

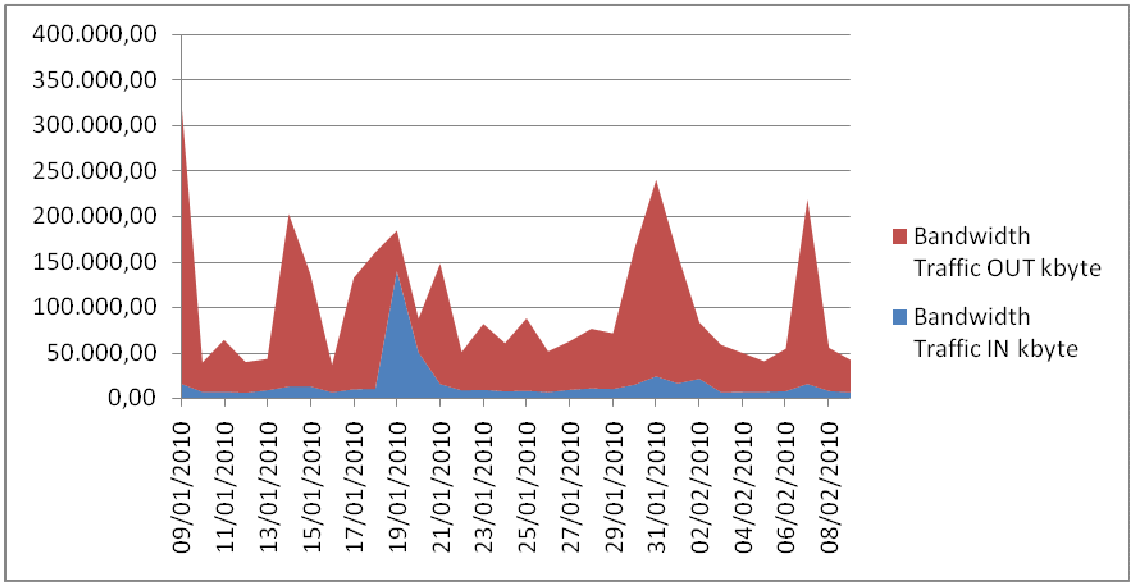


Tabla 5.16 Loja

Fa0/0 RED MACHALA (172.16.48.1)							
FECHA	Bandwidth Traffic IN	Bandwidth T raffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	33.935,68	5,905	87.561,22	15,237	121.496,90	21,143	54
08/02/2010	28.929,33	2,743	88.505,69	8,405	117.435,02	11,148	100
07/02/2010	26.415,44	2,505	93.629,93	8,885	120.045,36	11,39	100
06/02/2010	23.865,94	2,263	29.250,24	2,776	53.116,17	5,039	100
05/02/2010	16.523,06	2,117	31.785,91	4,073	48.308,97	6,19	74
03/02/2010	36.076,31	5,407	58.958,78	8,974	95.035,10	14,381	63
02/02/2010	85.072,96	8,067	41.112,14	3,901	126.185,10	11,969	100
01/02/2010	87.992,74	8,344	111.540,18	10,483	199.532,92	18,827	100
31/01/2010	89.560,06	8,505	88.048,58	8,355	177.608,64	16,86	100
30/01/2010	63.069,62	5,985	36.304,50	3,443	99.374,12	9,428	100
29/01/2010	47.900,10	4,542	83.956,39	7,972	131.856,49	12,515	100
28/01/2010	39.792,21	3,781	101.060,82	9,583	140.853,02	13,365	100
27/01/2010	87.439,42	8,292	160.782,52	15,247	248.221,94	23,539	100
26/01/2010	64.527,48	9,62	73.588,29	10,977	138.115,77	20,597	64
25/01/2010	100.104,35	13,48	113.229,38	15,247	213.333,73	28,727	70
24/01/2010	63.794,80	6,054	286.849,55	27,221	350.644,35	33,274	100
23/01/2010	114.101,68	10,961	131.832,29	12,655	245.933,97	23,616	99
22/01/2010	91.713,68	8,703	58.141,63	5,513	149.855,30	14,217	100
21/01/2010	104.450,65	9,905	37.654,13	3,571	142.104,77	13,476	100
20/01/2010	91.586,66	8,694	181.310,92	17,205	272.897,59	25,899	100
19/01/2010	80.908,99	7,673	45.921,32	4,358	126.830,30	12,03	100
18/01/2010	83.018,10	7,872	176.567,77	16,744	259.585,86	24,616	100
17/01/2010	77.292,95	7,335	97.655,31	9,261	174.948,26	16,595	100
16/01/2010	90.916,18	8,627	312.106,89	29,597	403.023,06	38,224	100
15/01/2010	80.363,76	7,621	270.954,62	25,694	351.318,38	33,315	100
14/01/2010	61.700,39	5,851	54.880,73	5,204	116.581,11	11,056	100
13/01/2010	64.165,14	6,085	37.178,98	3,526	101.344,12	9,61	100
12/01/2010	81.095,70	8,984	81.790,21	9,057	162.885,90	18,041	86
11/01/2010	81.215,06	7,707	61.413,17	5,828	142.628,24	13,535	100
10/01/2010	108.353,33	10,307	1.232.929,34	117,254	1.341.282,67	127,561	100
09/01/2010	61.549,18	5,849	247.001,52	23,44	308.550,69	29,289	100

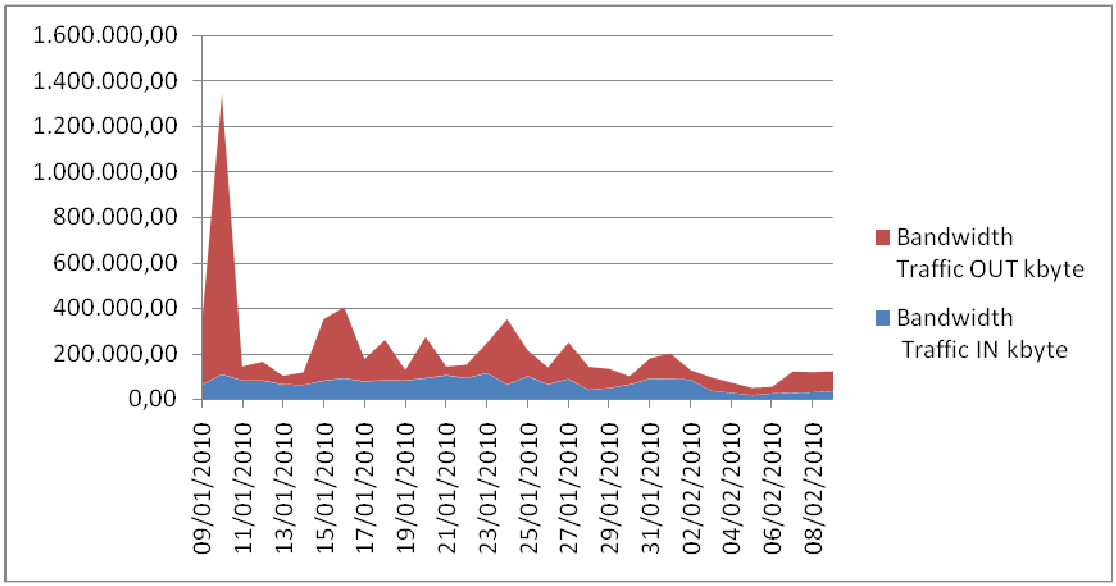


Tabla 5.17 Machala

Port Fa0 on MANTA (192.168.31.2)							
Fecha	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	250.233,22	43,946	374.363,23	65,746	624.596,45	109,693	54
08/02/2010	839.708,91	79,631	694.652,76	65,875	1.534.361,67	145,505	100
07/02/2010	6.917,07	0,668	23.450,52	2,263	30.367,59	2,931	98
06/02/2010	25.756,44	2,446	168.625,77	16,002	194.382,21	18,448	100
05/02/2010	76.662,36	9,821	281.591,02	36,073	358.253,38	45,894	74
03/02/2010	237.888,47	35,611	300.734,22	45,722	538.622,69	81,333	63
02/02/2010	455.503,18	43,194	602.533,75	57,137	1.058.036,93	100,332	100
01/02/2010	41.089,41	3,899	248.197,02	23,585	289.286,43	27,484	100
31/01/2010	241.618,29	25,569	260.982,31	25,883	502.600,59	51,452	93
30/01/2010	573.619,60	56,637	664.209,73	65,58	1.237.829,32	122,218	96
29/01/2010	1.094.322,08	103,771	1.275.801,02	120,982	2.370.123,10	224,753	100
28/01/2010	727.333,30	68,971	873.349,18	82,876	1.600.682,48	151,848	100
27/01/2010	463.447,89	43,948	937.071,28	88,924	1.400.519,17	132,871	100
26/01/2010	391.187,57	58,533	801.073,00	119,929	1.192.260,57	178,462	63
25/01/2010	373.538,81	50,325	825.920,22	111,271	1.199.459,03	161,596	70
24/01/2010	26.946,20	2,558	59.227,40	5,628	86.173,60	8,186	100
23/01/2010	60.562,05	5,743	122.730,26	11,663	183.292,31	17,406	100
22/01/2010	58.820,08	5,578	266.290,57	25,27	325.110,65	30,848	100
21/01/2010	64.315,38	6,103	353.639,28	33,558	417.954,66	39,661	100
20/01/2010	309.644,55	29,363	466.711,42	44,288	776.355,97	73,651	100
19/01/2010	427.546,93	40,571	639.225,99	60,66	1.066.772,92	101,231	100
18/01/2010	407.328,79	38,653	707.723,37	67,112	1.115.052,17	105,765	100
17/01/2010	632.247,64	59,998	935.270,80	88,69	1.567.518,44	148,688	100
16/01/2010	141.570,92	13,425	396.680,47	37,617	538.251,39	51,042	100
15/01/2010	279.405,96	26,513	389.912,83	36,975	669.318,79	63,488	100
14/01/2010	889.432,69	84,347	2.176.254,15	206,668	3.065.686,83	291,016	100
13/01/2010	703.953,94	66,848	1.029.032,53	97,582	1.732.986,48	164,43	100
12/01/2010	41.089,29	4,552	190.666,93	21,13	231.756,23	25,682	86
11/01/2010	57.384,58	5,446	133.652,94	12,692	191.037,52	18,138	100
10/01/2010	20.991,08	1,992	32.530,80	3,087	53.521,88	5,079	100
09/01/2010	33.666,60	3,195	149.615,94	14,198	183.282,54	17,393	100

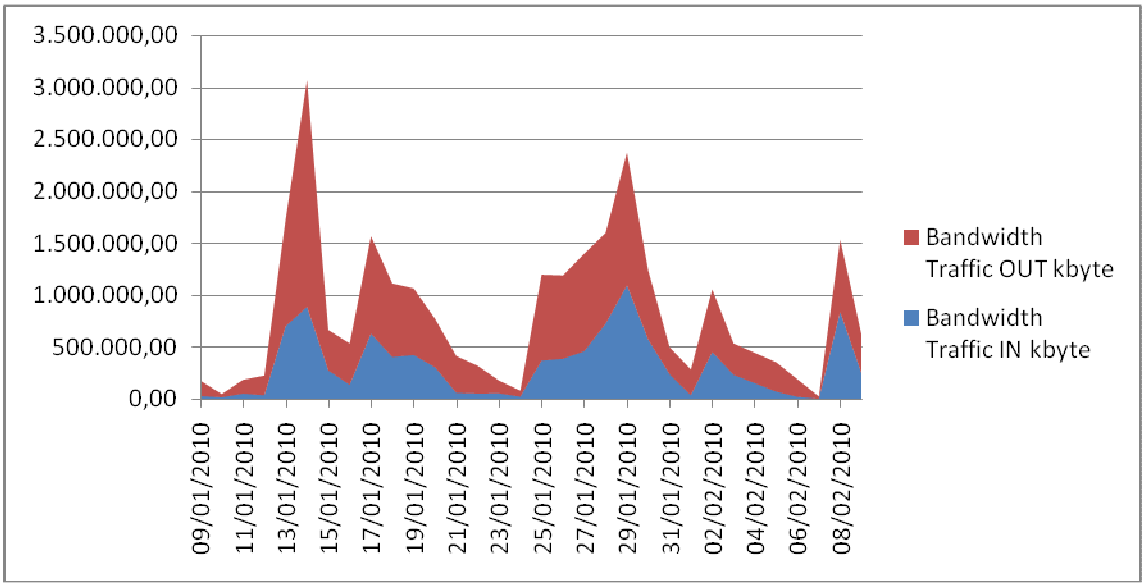


Tabla 5.18 Manta

Port Fa0 on MILAGRO (172.16.105.1)							
	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	49.221,06	8,655	27.726,21	4,869	76.947,26	13,523	54
08/02/2010	98.281,96	9,327	68.707,01	6,525	166.988,97	15,851	100
07/02/2010	95.291,76	9,037	51.298,52	4,868	146.590,28	13,905	100
06/02/2010	116.138,88	11,036	516.888,70	49,017	633.027,58	60,053	100
05/02/2010	54.042,30	6,943	274.687,75	35,193	328.730,05	42,136	74
03/02/2010	82.258,80	12,314	22.523,49	3,423	104.782,28	15,737	63
02/02/2010	233.061,76	22,116	65.034,42	6,12	298.096,18	28,236	100
01/02/2010	200.880,23	19,049	265.474,49	25,192	466.354,72	44,241	100
31/01/2010	177.271,40	16,81	437.085,99	41,477	614.357,39	58,288	100
30/01/2010	194.684,08	18,462	302.055,26	28,643	496.739,33	47,105	100
29/01/2010	200.346,98	18,998	209.944,16	19,937	410.291,14	38,935	100
28/01/2010	171.394,92	16,253	56.804,87	5,387	228.199,79	21,64	100
27/01/2010	172.579,47	16,365	68.812,56	6,525	241.392,04	22,891	100
26/01/2010	110.324,33	16,461	34.428,44	5,134	144.752,76	21,595	64
25/01/2010	171.453,10	23,168	61.555,36	8,301	233.008,47	31,469	70
24/01/2010	179.688,75	17,063	192.210,09	18,265	371.898,85	35,328	100
23/01/2010	161.236,80	15,29	128.082,24	12,162	289.319,04	27,452	100
22/01/2010	180.224,96	17,09	60.138,62	5,703	240.363,58	22,793	100
21/01/2010	155.041,60	14,743	106.694,47	10,125	261.736,07	24,867	100
20/01/2010	129.495,51	12,293	148.167,27	14,07	277.662,77	26,363	100
19/01/2010	168.347,75	15,998	114.519,34	10,875	282.867,09	26,872	100
18/01/2010	151.040,34	14,333	90.283,12	8,573	241.323,47	22,906	100
17/01/2010	196.374,80	18,635	51.670,15	4,907	248.044,95	23,542	100
16/01/2010	246.518,16	23,41	238.384,34	22,621	484.902,51	46,031	100
15/01/2010	228.801,42	21,712	677.043,17	64,203	905.844,59	85,915	100
14/01/2010	158.864,65	15,086	131.833,07	12,502	290.697,72	27,588	100
13/01/2010	165.581,77	15,724	133.465,27	12,665	299.047,05	28,389	100
12/01/2010	151.929,20	16,827	426.710,21	47,28	578.639,41	64,106	86
11/01/2010	150.617,98	14,293	180.309,45	17,111	330.927,42	31,404	100
10/01/2010	170.196,14	16,163	68.829,27	6,532	239.025,41	22,694	100
09/01/2010	184.276,53	17,475	64.362,40	6,104	248.638,93	23,579	100

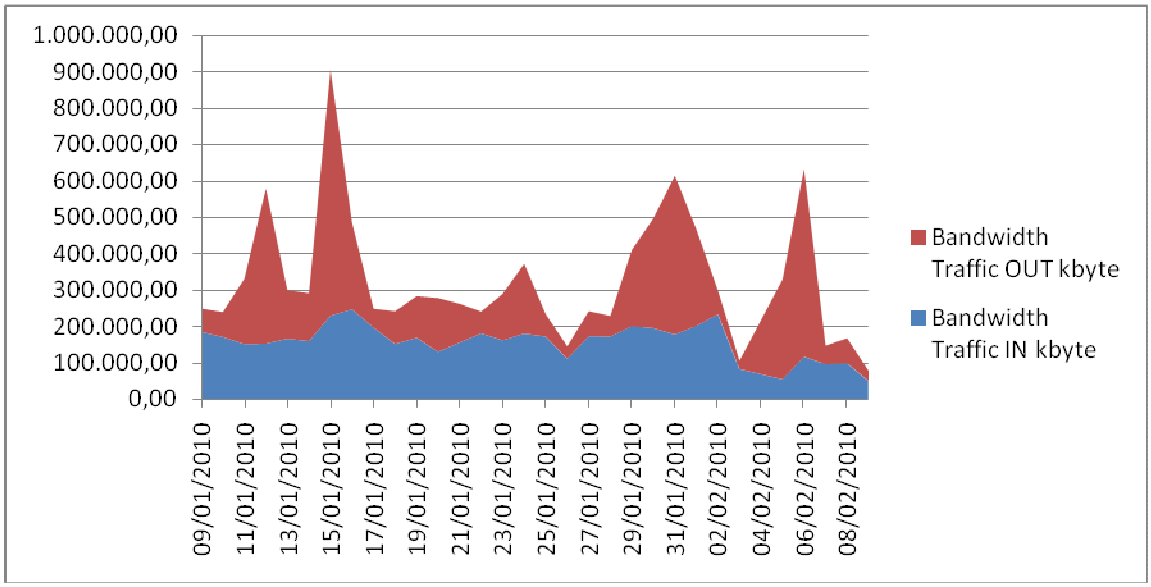


Tabla 5.19 Milagro

Port Fa0/0 on MOLINO (172.16.61.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	34.829,11	6,114	240.776,42	42,269	275.605,54	48,383	54
08/02/2010	66.937,69	6,348	345.054,63	32,722	411.992,32	39,07	100
07/02/2010	60.300,15	5,718	567.401,94	53,807	627.702,09	59,526	100
06/02/2010	97.599,33	9,255	1.231.469,83	116,781	1.329.069,16	126,037	100
05/02/2010	91.141,75	11,679	519.427,80	66,561	610.569,55	78,241	74
03/02/2010	71.310,44	10,663	144.986,95	22,032	216.297,39	32,695	63
02/02/2010	150.699,45	14,153	728.627,60	68,429	879.327,05	82,582	101
01/02/2010	133.606,39	12,67	302.829,84	28,717	436.436,22	41,387	100
31/01/2010	137.758,58	13,063	424.323,07	40,238	562.081,65	53,301	100
30/01/2010	104.478,57	9,907	226.826,17	21,509	331.304,74	31,417	100
29/01/2010	124.077,54	11,766	304.450,35	28,87	428.527,89	40,637	100
28/01/2010	133.107,00	12,622	202.360,82	19,189	335.467,82	31,812	100
27/01/2010	110.718,03	10,499	210.431,14	19,766	321.149,17	30,265	100
26/01/2010	87.327,30	13,014	309.786,99	46,193	397.114,28	59,207	64
25/01/2010	116.823,03	15,723	508.429,78	68,43	625.252,80	84,153	70
24/01/2010	133.431,67	12,653	303.952,09	28,823	437.383,76	41,476	100
23/01/2010	134.520,61	12,756	536.639,02	50,888	671.159,63	63,645	100
22/01/2010	141.984,96	13,464	229.576,00	21,77	371.560,97	35,235	100
21/01/2010	146.367,99	13,88	648.220,77	61,469	794.588,76	75,349	100
20/01/2010	124.417,30	11,824	180.580,76	17,124	304.998,06	28,948	100
19/01/2010	131.654,78	12,485	462.867,93	43,893	594.522,71	56,378	100
18/01/2010	130.523,43	12,377	232.371,61	22,035	362.895,04	34,413	100
17/01/2010	119.092,19	11,293	375.418,22	35,6	494.510,40	46,894	100
16/01/2010	115.740,37	10,975	239.316,31	22,694	355.056,68	33,669	100
15/01/2010	78.690,29	7,462	120.548,65	11,431	199.238,93	18,893	100
14/01/2010	114.504,15	10,859	1.027.266,75	97,418	1.141.770,91	108,276	100
13/01/2010	75.137,42	7,125	208.662,84	19,787	283.800,26	26,912	100
12/01/2010	100.099,91	11,085	408.681,60	45,274	508.781,52	56,358	86
11/01/2010	91.415,88	8,669	239.793,19	22,74	331.209,06	31,409	100
10/01/2010	105.867,43	10,04	472.748,57	44,832	578.616,00	54,871	100
09/01/2010	148.440,68	14,077	442.841,61	41,995	591.282,29	56,071	100

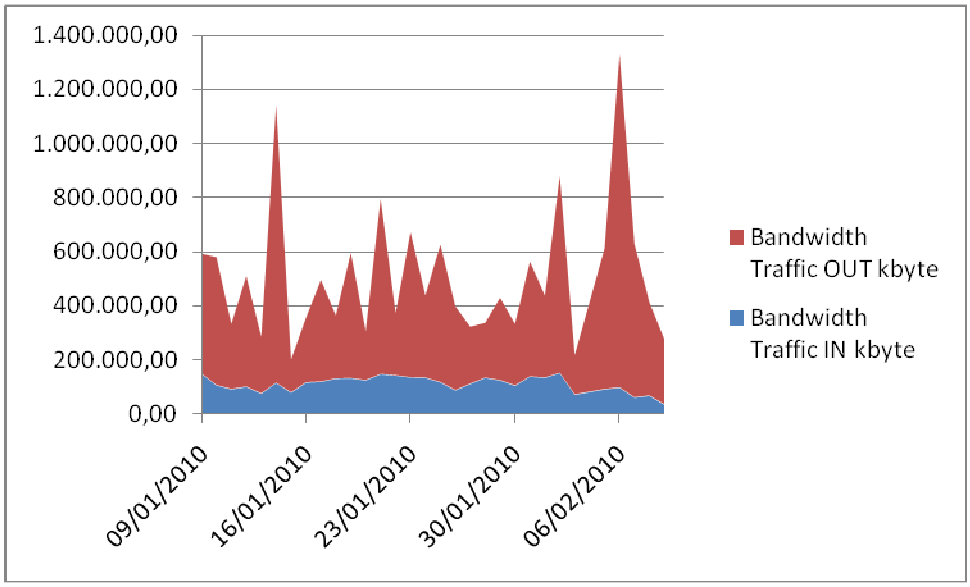


Tabla 5.20 Molino

Et1/1 on MULALO (172.16.26.2)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	4.733,15	0,827	24.724,68	4,321	29.457,84	5,148	54
08/02/2010	18.960,84	1,798	101.369,05	9,613	120.329,89	11,411	100
07/02/2010	12.788,43	1,213	68.640,02	6,509	81.428,45	7,722	100
06/02/2010	22.466,25	2,13	196.630,33	18,647	219.096,58	20,777	100
05/02/2010	12.855,22	1,647	107.243,72	13,742	120.098,94	15,389	74
03/02/2010	8.782,07	1,313	43.148,35	6,557	51.930,42	7,87	63
02/02/2010	18.461,33	1,751	89.737,01	8,51	108.198,35	10,26	100
01/02/2010	18.156,96	1,722	100.869,00	9,565	119.025,96	11,287	100
31/01/2010	10.609,27	1,006	50.091,80	4,75	60.701,06	5,756	100
30/01/2010	9.668,74	0,917	64.156,72	6,084	73.825,46	7,001	100
29/01/2010	17.112,25	1,623	109.587,52	10,392	126.699,77	12,015	100
28/01/2010	12.255,16	1,162	120.377,89	11,415	132.633,05	12,577	100
27/01/2010	15.272,22	1,448	95.381,51	9,045	110.653,73	10,493	100
26/01/2010	10.273,13	1,539	55.073,36	8,256	65.346,49	9,796	63
25/01/2010	10.545,93	1,419	58.040,07	7,812	68.585,99	9,231	70
24/01/2010	9.099,57	0,863	84.093,36	7,974	93.192,94	8,837	100
23/01/2010	10.361,39	0,983	46.490,06	4,409	56.851,44	5,391	100
22/01/2010	16.733,06	1,587	152.949,31	14,504	169.682,38	16,091	100
21/01/2010	15.251,39	1,446	107.096,31	10,156	122.347,70	11,602	100
20/01/2010	13.277,73	1,259	68.360,93	6,483	81.638,66	7,742	100
19/01/2010	16.711,59	1,585	66.534,05	6,309	83.245,65	7,894	100
18/01/2010	18.391,10	1,744	95.270,14	9,034	113.661,24	10,778	100
17/01/2010	8.403,03	0,797	33.813,87	3,207	42.216,90	4,003	100
16/01/2010	14.235,18	1,35	76.956,15	7,298	91.191,33	8,648	100
15/01/2010	11.686,93	1,108	58.958,24	5,591	70.645,17	6,699	100
14/01/2010	36.883,45	3,498	120.448,15	11,423	157.331,60	14,92	100
13/01/2010	15.183,26	1,44	87.267,21	8,275	102.450,47	9,715	100
12/01/2010	10.219,19	1,13	37.447,46	4,143	47.666,65	5,273	86
11/01/2010	9.674,15	0,917	36.747,63	3,485	46.421,78	4,402	100
10/01/2010	10.142,43	0,962	41.155,60	3,903	51.298,03	4,865	100
09/01/2010	15.822,80	1,5	80.510,40	7,635	96.333,20	9,135	100

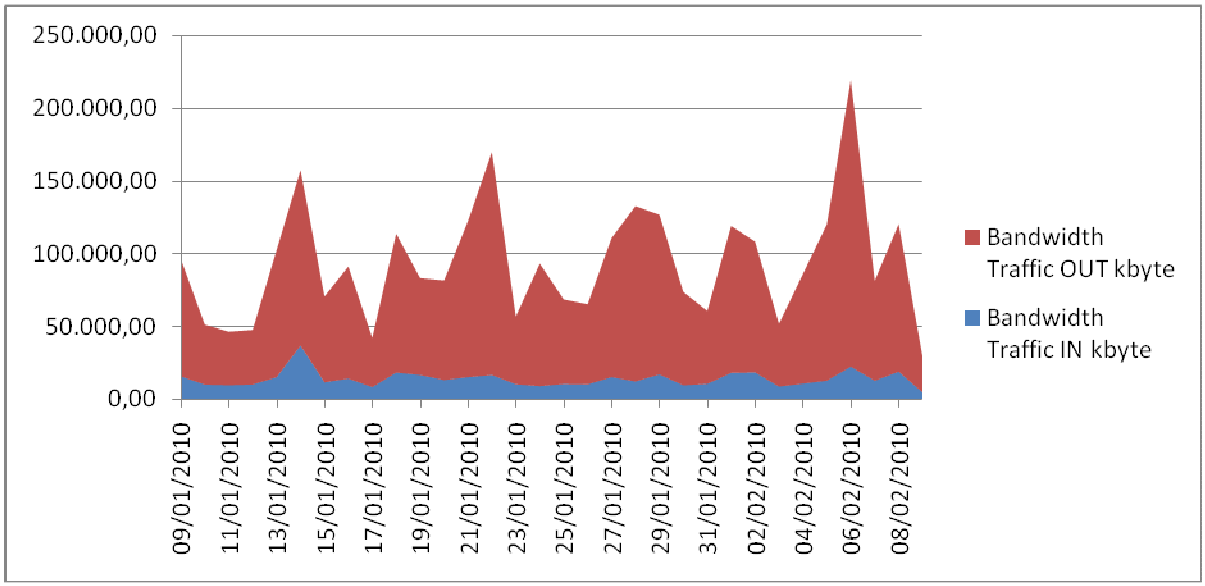


Tabla 5.21 Mulalo

Port Fa0/0 on PASCUALES (172.16.46.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	109.047,37	19,178	869.288,34	152,684	978.335,70	171,862	54
08/02/2010	350.644,00	33,298	1.672.316,63	158,588	2.022.960,63	191,886	100
07/02/2010	17.524.361,81	1.664,15	2.452.291,52	232,552	19.976.653,33	1.896,71	100
06/02/2010	26.982.199,78	2.560,52	2.588.935,93	245,509	29.571.135,71	2.806,03	100
05/02/2010	165.567,95	21,29	676.750,82	86,774	842.318,77	108,063	74
03/02/2010	507.210,13	75,845	1.352.826,37	205,569	1.860.036,50	281,413	63
02/02/2010	332.083,13	31,491	1.120.349,42	106,24	1.452.432,55	137,731	100
01/02/2010	382.286,60	36,252	1.021.553,93	96,873	1.403.840,53	133,124	100
31/01/2010	134.342,57	12,74	425.901,44	40,388	560.244,02	53,127	100
30/01/2010	198.487,11	18,822	792.122,24	75,116	990.609,35	93,938	100
29/01/2010	15.109.259,61	1.434,29	1.446.899,14	137,206	16.556.158,75	1.571,49	100
28/01/2010	17.629.781,25	1.684,69	1.432.452,08	136,358	19.062.233,33	1.821,04	99
27/01/2010	337.298,50	31,683	1.439.824,35	135,243	1.777.122,86	166,926	101
26/01/2010	213.387,66	32,063	989.632,79	148,782	1.203.020,45	180,845	63
25/01/2010	253.292,20	34,142	1.566.980,60	211,005	1.820.272,80	245,146	70
24/01/2010	58.064,17	5,506	865.617,99	82,085	923.682,16	87,591	100
23/01/2010	102.357,52	9,706	973.725,41	92,465	1.076.082,93	102,171	100
22/01/2010	418.733,33	39,735	1.203.596,10	114,215	1.622.329,43	153,95	100
21/01/2010	340.411,76	32,325	1.369.917,46	129,907	1.710.329,23	162,232	100
20/01/2010	776.144,29	73,678	2.087.237,16	198,069	2.863.381,45	271,747	100
19/01/2010	493.275,05	46,81	1.926.603,19	182,697	2.419.878,24	229,507	100
18/01/2010	368.381,64	34,958	1.617.795,79	153,413	1.986.177,43	188,371	100
17/01/2010	77.176,94	7,319	456.824,01	43,32	534.000,95	50,638	100
16/01/2010	108.600,82	10,298	470.885,30	44,684	579.486,12	54,982	100
15/01/2010	461.563,23	43,769	1.281.414,77	121,515	1.742.978,00	165,284	100
14/01/2010	348.053,50	33,007	1.374.563,11	130,352	1.722.616,61	163,359	100
13/01/2010	341.538,40	32,411	1.079.770,71	102,466	1.421.309,11	134,877	100
12/01/2010	303.039,16	33,587	1.382.221,46	153,125	1.685.260,63	186,712	86
11/01/2010	301.399,15	28,602	979.133,97	92,853	1.280.533,11	121,455	100
10/01/2010	96.935,99	9,205	523.732,99	49,805	620.668,97	59,01	100
09/01/2010	174.580,44	16,556	695.970,83	66,046	870.551,26	82,601	100

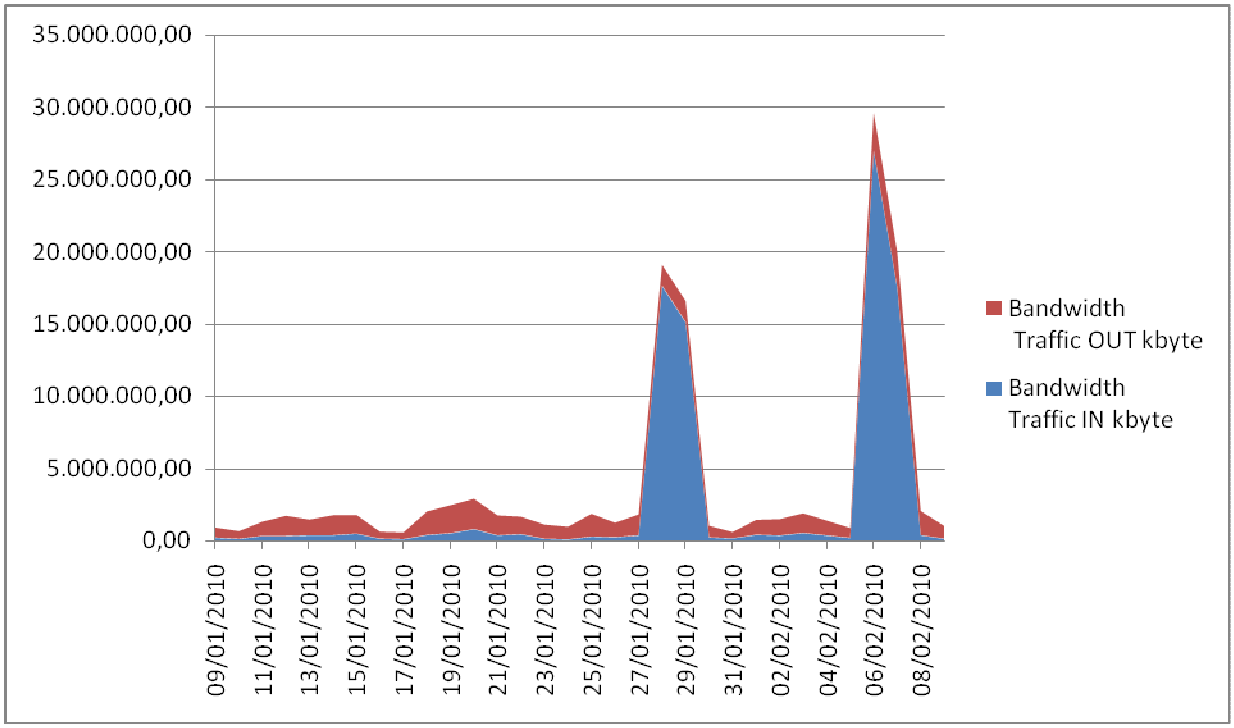


Tabla 5.22 Pascuales

Port Fa0 on POMASQUI (RED LAN POMASQUI)							
FECHA	Bandwidth Tra	Bandwidth Tra	Bandwidth Tra	Bandwidth Tra	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	842.288,98	147,564	75.003,89	13,14	917.292,87	160,704	54
08/02/2010	1.582.559,15	152,513	179.283,20	17,278	1.761.842,35	169,791	98
07/02/2010	1.564.170,23	151,329	182.793,30	17,685	1.746.963,52	169,014	98
06/02/2010	1.626.058,73	156,147	195.858,74	18,777	1.821.917,48	174,924	99
05/02/2010	1.161.385,55	154,405	149.433,51	19,859	1.310.819,06	174,263	71
03/02/2010	1.039.574,94	156,653	95.782,48	14,669	1.135.357,42	171,322	62
02/02/2010	1.634.372,16	159,549	213.687,50	20,825	1.848.059,66	180,374	97
01/02/2010	1.637.645,91	160,363	182.089,42	17,831	1.819.735,33	178,194	97
31/01/2010	1.641.362,46	160,328	202.917,03	19,786	1.844.279,50	180,114	97
30/01/2010	2.780.329,19	267,311	199.235,78	19,155	2.979.564,97	286,467	99
29/01/2010	2.581.986,69	251,799	229.583,24	22,389	2.811.569,93	274,188	97
28/01/2010	5.981.159,87	576,356	255.894,69	24,626	6.237.054,55	600,983	98
27/01/2010	1.660.436,62	159,615	219.611,35	21,126	1.880.047,97	180,741	99
26/01/2010	1.045.478,09	160,47	197.597,29	30,367	1.243.075,38	190,836	62
25/01/2010	1.152.363,83	157,672	133.734,64	18,261	1.286.098,47	175,933	69
24/01/2010	2.881.365,09	273,993	223.441,92	21,233	3.104.807,01	295,226	100
23/01/2010	2.549.363,94	246,364	323.089,75	31,191	2.872.453,69	277,556	98
22/01/2010	2.304.992,97	222,759	276.839,66	26,719	2.581.832,62	249,478	98
21/01/2010	2.366.712,22	228,004	268.615,72	25,897	2.635.327,94	253,9	98
20/01/2010	2.485.544,09	238,177	308.887,76	29,558	2.794.431,85	267,735	99
19/01/2010	2.503.683,81	239,924	376.885,96	36,091	2.880.569,77	276,015	99
18/01/2010	2.491.166,12	241,599	348.229,19	33,752	2.839.395,32	275,351	98
17/01/2010	2.531.627,56	241,663	215.954,70	20,6	2.747.582,25	262,263	99
16/01/2010	2.032.631,39	197,813	248.456,49	24,154	2.281.087,88	221,966	97
15/01/2010	1.641.877,64	158,61	201.578,12	19,454	1.843.455,76	178,063	98
14/01/2010	2.138.446,52	205,364	243.105,02	23,339	2.381.551,54	228,704	99
13/01/2010	1.625.456,93	156,691	189.062,62	18,238	1.814.519,55	174,929	98
12/01/2010	1.393.448,80	157,741	174.682,88	19,767	1.568.131,68	177,508	84
11/01/2010	1.705.230,17	165,037	430.259,21	41,629	2.135.489,38	206,666	98
10/01/2010	1.615.461,98	154,863	238.580,92	22,855	1.854.042,90	177,718	99
09/01/2010	1.645.887,27	157,668	202.485,77	19,397	1.848.373,04	177,065	99

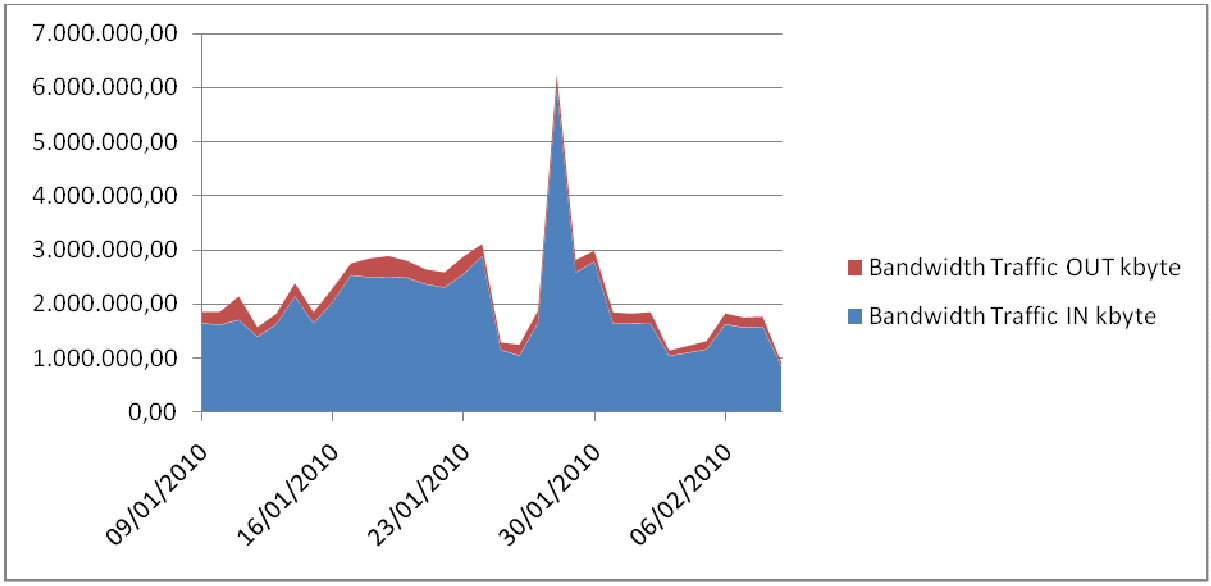


Tabla 5.23 Pomasqui.

Se0/3/1 on PUYO ID (172.16.26.18)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	20.445,42	3,579	225.537,53	39,475	245.982,95	43,054	54
08/02/2010	31.692,40	3,005	190.285,19	18,045	221.977,59	21,05	100
07/02/2010	41.958,80	3,979	257.191,53	24,39	299.150,32	28,369	100
06/02/2010	34.939,24	3,313	195.488,42	18,538	230.427,66	21,852	100
05/02/2010	20.162,36	2,583	88.989,01	11,402	109.151,37	13,985	74
03/02/2010	50.043,22	7,483	110.683,45	16,82	160.726,67	24,303	63
02/02/2010	87.366,45	8,285	112.338,54	10,653	199.704,99	18,938	100
01/02/2010	122.907,90	11,655	313.627,76	29,741	436.535,66	41,396	100
31/01/2010	102.878,81	9,756	276.627,98	26,232	379.506,79	35,988	100
30/01/2010	84.331,24	7,997	139.360,17	13,215	223.691,41	21,212	100
29/01/2010	140.913,29	13,363	464.586,28	44,056	605.499,57	57,419	100
28/01/2010	96.001,22	9,104	238.085,76	22,577	334.086,98	31,681	100
27/01/2010	123.471,71	11,709	251.676,24	23,866	375.147,95	35,575	100
26/01/2010	41.240,78	6,146	8.714,39	1,299	49.955,17	7,445	64
25/01/2010	60.552,66	8,154	112.963,52	15,212	173.516,18	23,366	70
24/01/2010	157.277,80	14,914	374.693,79	35,531	531.971,58	50,446	100
23/01/2010	86.163,90	8,171	187.845,13	17,813	274.009,03	25,984	100
22/01/2010	125.663,12	11,917	187.421,62	17,773	313.084,74	29,689	100
21/01/2010	107.002,00	10,147	193.908,32	18,388	300.910,32	28,535	100
20/01/2010	73.182,30	6,94	95.446,46	9,051	168.628,76	15,991	100
19/01/2010	106.999,91	10,147	264.078,39	25,042	371.078,30	35,189	100
18/01/2010	103.626,86	9,827	115.808,70	10,982	219.435,56	20,808	100
17/01/2010	80.697,34	7,652	173.622,91	16,465	254.320,25	24,117	100
16/01/2010	84.964,84	8,057	284.136,30	26,944	369.101,13	35,001	100
15/01/2010	125.945,36	11,943	258.049,74	24,47	383.995,10	36,412	100
14/01/2010	117.941,13	11,185	176.656,42	16,753	294.597,55	27,938	100
13/01/2010	102.351,82	9,706	210.808,72	19,99	313.160,54	29,696	100
12/01/2010	31.629,73	3,514	98.852,81	10,986	130.482,53	14,499	85
11/01/2010	30.981,74	2,938	73.720,79	6,991	104.702,53	9,929	100
10/01/2010	61.537,99	5,836	113.712,26	10,784	175.250,25	16,619	100
09/01/2010	78.057,16	7,402	189.455,87	17,966	267.513,03	25,368	100

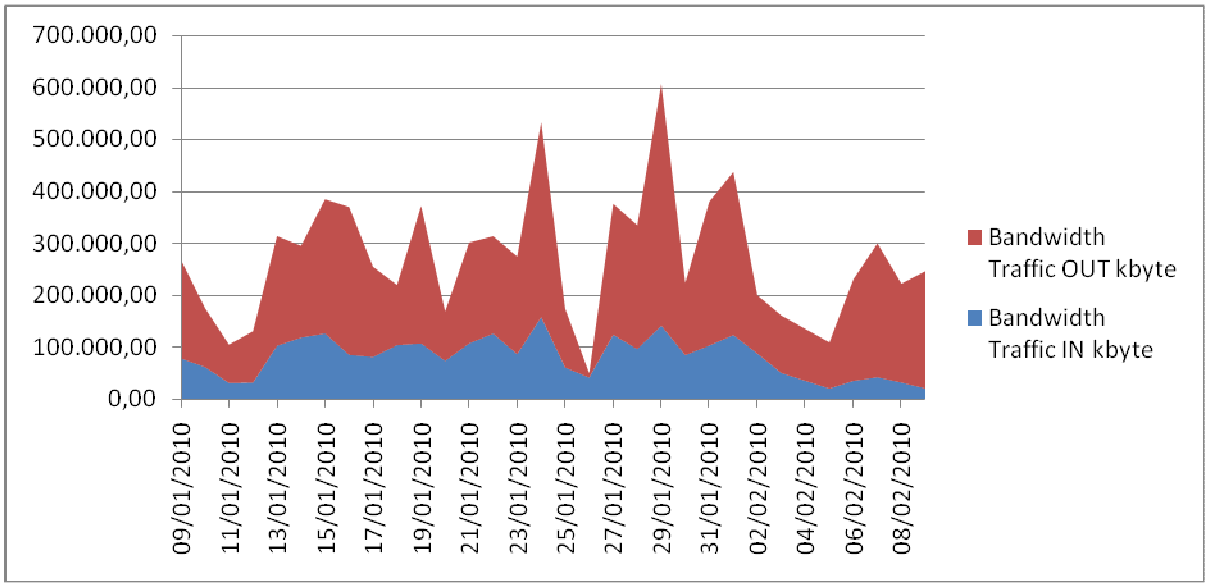


Tabla 5.24 Puyo

Port Fa0/0 on QUEVEDO (172.16.56.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	10.933,75	1,918	25.518,35	4,465	36.452,10	6,383	54
08/02/2010	5.398,87	0,513	6.377,06	0,606	11.775,93	1,119	100
07/02/2010	878,952	0,083	1.636,90	0,155	2.515,86	0,239	100
06/02/2010	2.671,99	0,254	3.334,49	0,316	6.006,48	0,571	100
05/02/2010	1.744,16	0,223	3.876,58	0,498	5.620,73	0,721	74
03/02/2010	18.158,45	2,715	83.516,72	12,691	101.675,17	15,406	63
02/02/2010	14.301,90	1,356	74.612,83	7,075	88.914,73	8,432	100
01/02/2010	6.361,65	0,603	70.222,43	6,664	76.584,08	7,267	100
31/01/2010	11.237,34	1,066	77.827,21	7,38	89.064,55	8,446	100
30/01/2010	22.648,16	2,148	70.085,03	6,646	92.733,19	8,794	100
29/01/2010	7.721,07	0,732	8.791,03	0,834	16.512,10	1,566	100
28/01/2010	15.987,20	1,518	42.964,06	4,077	58.951,27	5,595	100
27/01/2010	6.843,32	0,649	7.606,94	0,721	14.450,26	1,37	100
26/01/2010	1.925,93	0,289	2.405,61	0,362	4.331,54	0,651	63
25/01/2010	5.060,81	0,682	30.466,50	4,107	35.527,31	4,789	70
24/01/2010	525,312	0,05	1.211,77	0,115	1.737,08	0,165	100
23/01/2010	478,609	0,045	1.161,25	0,11	1.639,86	0,156	100
22/01/2010	283,103	0,027	1.182,53	0,112	1.465,63	0,139	100
21/01/2010	16.781,99	1,591	95.253,51	9,058	112.035,50	10,649	100
20/01/2010	1.731,18	0,164	2.462,90	0,234	4.194,07	0,398	100
19/01/2010	3.888,78	0,369	4.768,38	0,452	8.657,16	0,821	100
18/01/2010	5.677,77	0,538	6.598,81	0,626	12.276,58	1,165	100
17/01/2010	409,345	0,039	1.159,49	0,11	1.568,84	0,149	100
16/01/2010	528,505	0,05	1.241,15	0,118	1.769,65	0,168	100
15/01/2010	1.198,50	0,114	2.013,31	0,191	3.211,81	0,305	100
14/01/2010	2.549,62	0,242	3.429,73	0,325	5.979,35	0,568	100
13/01/2010	1.353,03	0,128	1.994,99	0,189	3.348,02	0,318	100
12/01/2010	16.095,66	1,782	153.515,01	17,001	169.610,66	18,783	86
11/01/2010	4.407,59	0,418	5.306,76	0,503	9.714,35	0,922	100
10/01/2010	682,724	0,065	1.221,87	0,116	1.904,60	0,181	100
09/01/2010	476,765	0,045	1.172,96	0,111	1.649,73	0,156	100

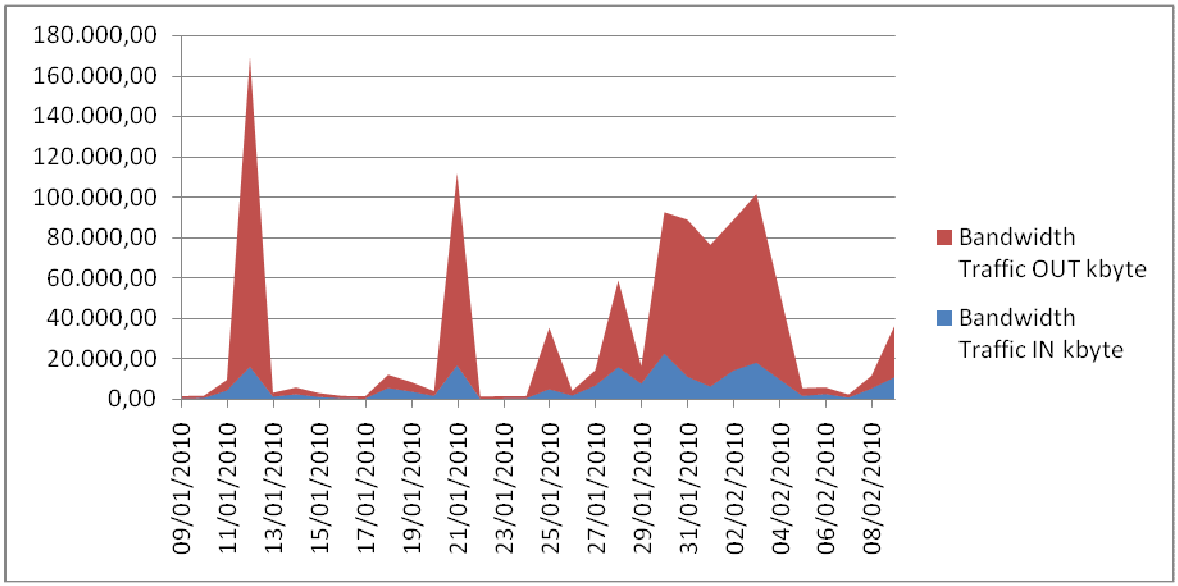


Tabla 5.25 Quevedo

Port Fa0 on RIOBAMBA (172.16.200.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	21.647,52	3,826	224.616,90	39,422	246.264,42	43,248	54
08/02/2010	31.785,91	3,016	188.799,52	17,904	220.585,43	20,921	100
07/02/2010	40.981,38	3,948	251.169,71	23,995	292.151,09	27,943	99
06/02/2010	35.217,97	3,342	193.678,30	18,386	228.896,27	21,728	100
05/02/2010	18.637,45	2,388	86.788,91	11,129	105.426,36	13,517	74
03/02/2010	50.289,28	7,524	109.726,17	16,425	160.015,44	23,949	63
02/02/2010	87.619,53	8,309	110.752,79	10,51	198.372,32	18,819	100
01/02/2010	125.900,31	11,832	311.918,00	29,169	437.818,31	41,001	101
31/01/2010	103.600,26	9,852	274.822,23	26,161	378.422,48	36,013	100
30/01/2010	83.384,94	7,913	137.895,67	13,086	221.280,60	20,998	100
29/01/2010	144.718,09	13,622	463.839,75	43,365	608.557,83	56,987	101
28/01/2010	96.396,39	9,148	235.761,52	22,435	332.157,91	31,582	100
27/01/2010	124.553,76	11,869	251.050,11	23,647	375.603,87	35,516	100
26/01/2010	38.595,00	5,785	6.561,52	0,984	45.156,52	6,769	63
25/01/2010	59.446,75	8,009	111.619,63	15,038	171.066,38	23,046	70
24/01/2010	160.975,37	15,292	375.506,68	35,81	536.482,05	51,101	100
23/01/2010	85.571,72	8,126	186.624,21	17,709	272.195,93	25,835	100
22/01/2010	125.282,89	11,918	187.231,68	17,767	312.514,57	29,685	100
21/01/2010	107.050,51	10,166	192.876,35	18,328	299.926,85	28,494	100
20/01/2010	71.821,37	6,811	94.009,69	8,915	165.831,06	15,726	100
19/01/2010	109.949,66	10,426	264.941,60	25,177	374.891,26	35,603	100
18/01/2010	103.531,99	9,818	115.571,15	10,856	219.103,14	20,674	100
17/01/2010	82.750,45	7,847	174.238,19	16,534	256.988,64	24,381	100
16/01/2010	87.077,70	8,275	281.251,82	26,811	368.329,52	35,086	100
15/01/2010	129.020,90	12,26	260.823,77	24,733	389.844,67	36,994	100
14/01/2010	119.368,21	11,32	177.988,86	16,891	297.357,07	28,211	100
13/01/2010	101.832,10	9,691	209.880,17	19,958	311.712,27	29,648	100
12/01/2010	29.992,73	3,319	97.641,97	10,81	127.634,69	14,129	86
11/01/2010	27.980,11	2,735	71.854,85	6,814	99.834,96	9,549	98
10/01/2010	60.479,13	5,735	114.128,32	10,823	174.607,45	16,558	100
09/01/2010	77.821,99	7,4	188.684,32	17,95	266.506,32	25,35	100

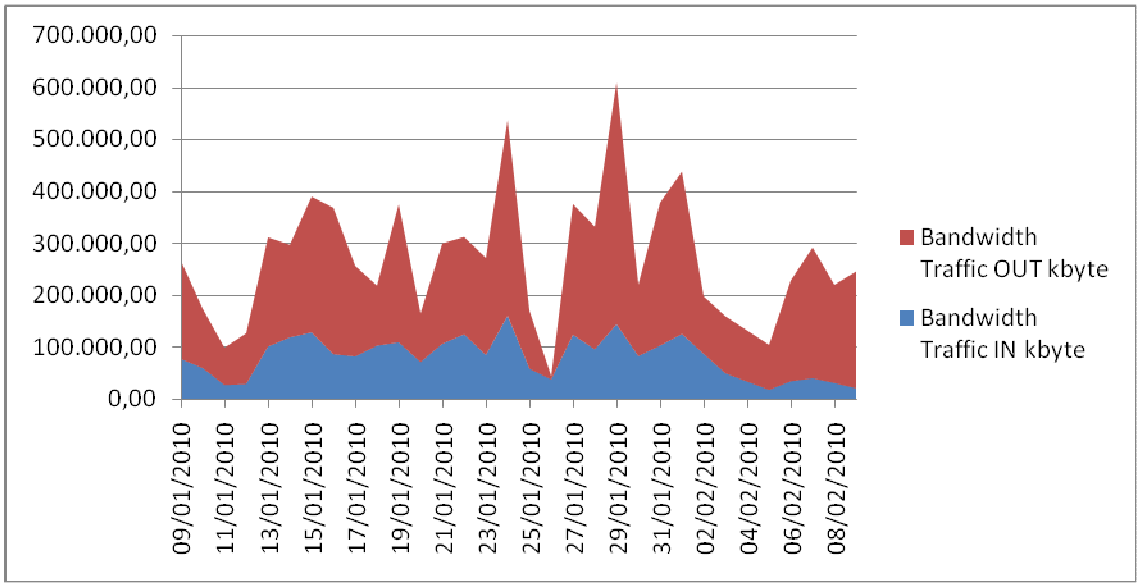


Tabla 5.26 Riobamba

Port Se0/3 on ROUTER_TE_FO IBARRA							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	4.737,30	0,827	24.731,89	4,318	29.469,19	5,146	54
08/02/2010	18.960,87	1,798	101.370,15	9,613	120.331,02	11,411	100
07/02/2010	12.788,47	1,213	68.638,93	6,509	81.427,40	7,722	100
06/02/2010	22.468,81	2,131	196.639,23	18,647	219.108,04	20,778	100
05/02/2010	12.853,24	1,647	107.237,24	13,738	120.090,48	15,384	74
03/02/2010	8.782,07	1,313	43.148,35	6,557	51.930,42	7,87	63
02/02/2010	18.461,33	1,751	89.737,01	8,51	108.198,34	10,26	100
01/02/2010	18.156,96	1,722	100.869,01	9,565	119.025,96	11,287	100
31/01/2010	10.608,99	1,006	50.091,55	4,75	60.700,54	5,756	100
30/01/2010	9.669,01	0,917	64.156,97	6,084	73.825,98	7,001	100
29/01/2010	17.105,50	1,623	109.587,26	10,294	126.692,75	11,917	100
28/01/2010	12.255,69	1,162	120.368,70	11,422	132.624,39	12,584	100
27/01/2010	15.271,69	1,448	95.381,94	9,045	110.653,63	10,493	100
26/01/2010	10.312,82	1,538	55.198,52	8,239	65.511,34	9,778	64
25/01/2010	10.544,87	1,42	58.037,45	7,815	68.582,32	9,235	70
24/01/2010	9.099,57	0,863	84.093,36	7,974	93.192,93	8,837	100
23/01/2010	10.361,39	0,983	46.490,06	4,409	56.851,45	5,391	100
22/01/2010	16.733,05	1,587	152.949,23	14,504	169.682,29	16,091	100
21/01/2010	15.249,77	1,447	107.095,91	10,156	122.345,68	11,603	100
20/01/2010	13.277,74	1,259	68.361,27	6,483	81.639,01	7,742	100
19/01/2010	16.711,61	1,585	66.534,20	6,309	83.245,80	7,894	100
18/01/2010	18.391,11	1,744	95.269,51	8,949	113.660,61	10,693	100
17/01/2010	8.403,03	0,797	33.813,86	3,207	42.216,89	4,003	100
16/01/2010	14.235,19	1,35	76.956,16	7,298	91.191,34	8,648	100
15/01/2010	11.686,22	1,108	58.957,08	5,591	70.643,30	6,699	100
14/01/2010	36.884,13	3,498	120.449,77	11,423	157.333,91	14,921	100
13/01/2010	15.183,33	1,44	87.267,41	8,275	102.450,74	9,715	100
12/01/2010	10.068,64	1,117	36.839,69	4,087	46.908,33	5,203	85
11/01/2010	9.674,37	0,917	36.747,71	3,485	46.422,08	4,402	100
10/01/2010	10.142,33	0,962	41.154,53	3,903	51.296,86	4,865	100
09/01/2010	15.822,83	1,5	80.510,30	7,635	96.333,12	9,135	100

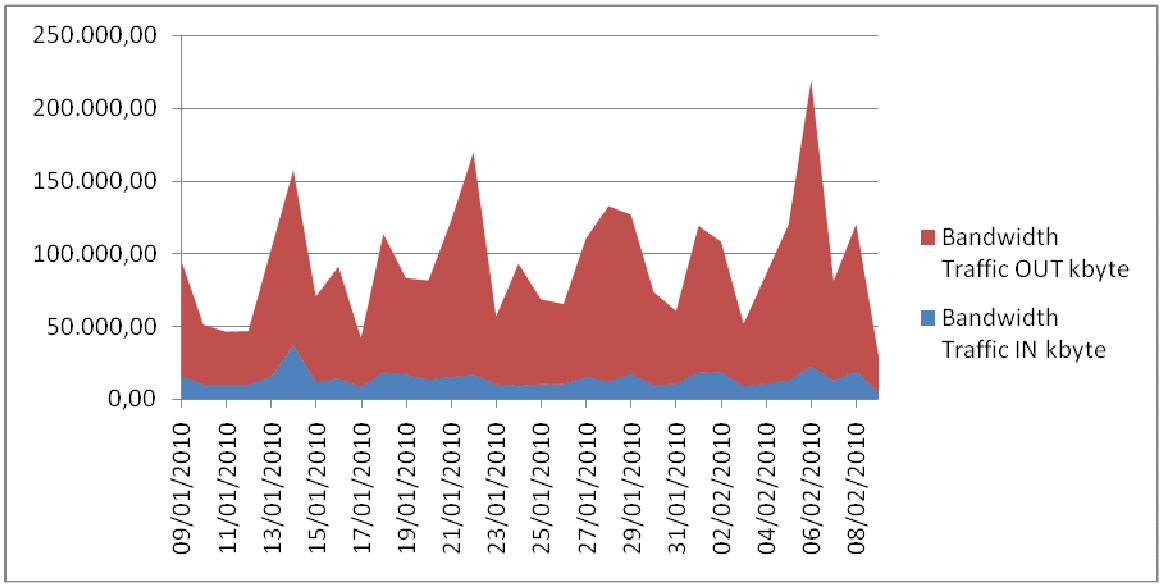


Tabla 5.27 Ibarra

Fa0/0 on Salitral (172.16.66.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	37.763,32	6,592	160.812,94	28,071	198.576,26	34,662	54
08/02/2010	79.053,28	7,497	168.349,10	15,998	247.402,39	23,495	100
07/02/2010	76.379,90	7,248	261.563,99	24,804	337.943,89	32,053	100
06/02/2010	63.023,60	5,985	97.736,07	9,288	160.759,67	15,273	100
05/02/2010	43.132,38	5,532	90.170,07	11,554	133.302,45	17,086	74
03/02/2010	71.433,57	10,682	32.946,80	5,009	104.380,37	15,691	63
02/02/2010	155.962,16	14,79	84.975,62	8,058	240.937,78	22,848	100
01/02/2010	161.513,22	15,316	80.381,18	7,622	241.894,40	22,938	100
31/01/2010	141.275,14	13,397	95.760,34	9,081	237.035,48	22,478	100
30/01/2010	155.529,52	14,749	161.542,13	15,319	317.071,65	30,067	100
29/01/2010	140.520,93	13,325	137.682,10	13,056	278.203,03	26,381	100
28/01/2010	150.524,53	14,299	186.446,44	17,693	336.970,96	31,992	100
27/01/2010	146.478,54	13,89	466.217,92	44,211	612.696,46	58,101	100
26/01/2010	95.232,48	14,276	41.596,49	6,246	136.828,96	20,522	63
25/01/2010	81.464,26	10,964	24.283,82	3,268	105.748,08	14,233	70
24/01/2010	151.280,95	14,346	310.105,36	29,427	461.386,30	43,772	100
23/01/2010	138.085,85	13,104	150.139,55	14,237	288.225,40	27,341	100
22/01/2010	227.694,86	21,622	228.246,18	21,69	455.941,03	43,312	100
21/01/2010	137.101,94	12,882	190.024,31	17,854	327.126,25	30,735	101
20/01/2010	130.393,12	12,386	100.876,30	9,566	231.269,43	21,952	100
19/01/2010	196.745,72	18,683	242.099,89	22,974	438.845,61	41,657	100
18/01/2010	129.577,49	12,412	46.427,22	4,406	176.004,71	16,817	99
17/01/2010	136.522,06	12,946	48.484,75	4,598	185.006,81	17,544	100
16/01/2010	160.825,45	15,261	187.505,12	17,781	348.330,57	33,042	100
15/01/2010	136.727,72	12,975	87.171,38	8,272	223.899,11	21,247	100
14/01/2010	167.439,03	15,89	113.898,31	10,801	281.337,33	26,691	100
13/01/2010	163.384,72	15,717	51.246,69	4,925	214.631,42	20,642	99
12/01/2010	93.628,81	10,413	78.565,80	8,742	172.194,60	19,155	85
11/01/2010	129.196,24	12,269	152.526,53	14,474	281.722,77	26,743	100
10/01/2010	121.971,88	11,591	76.880,35	7,296	198.852,23	18,887	100
09/01/2010	136.330,39	12,928	127.089,87	12,052	263.420,26	24,98	100

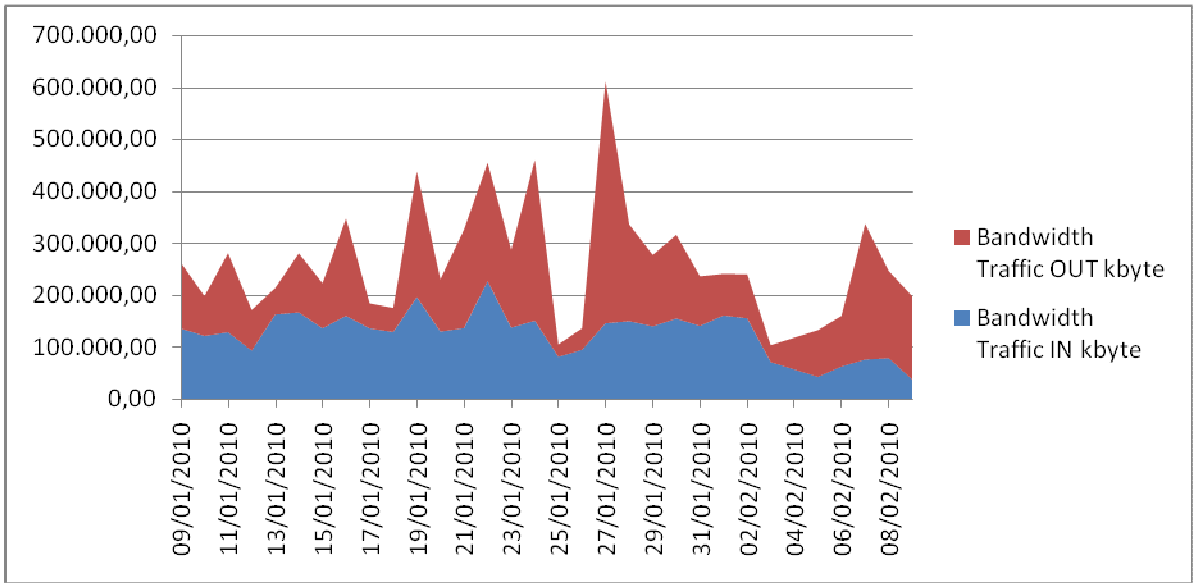


Tabla 5.28 Salitral

Port Fa0/0 on SAN IDELFONSO (172.16.117.1)							
	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	17.002,89	2,969	26.358,48	4,609	43.361,37	7,578	54
08/02/2010	24.055,80	2,284	183.822,55	17,481	207.878,35	19,766	100
07/02/2010	37.123,90	3,523	476.858,80	45,316	513.982,69	48,838	100
06/02/2010	38.132,63	3,621	379.736,61	36,01	417.869,24	39,632	100
05/02/2010	26.024,98	3,34	226.565,74	29,022	252.590,72	32,362	74
03/02/2010	8.340,24	1,254	84.342,86	12,816	92.683,09	14,07	63
02/02/2010	17.751,42	2,315	113.365,52	10,881	131.116,94	13,197	86
01/02/2010	22.456,86	2,137	165.680,12	15,711	188.136,99	17,848	100
31/01/2010	22.958,37	2,183	95.108,31	9,038	118.066,67	11,221	100
30/01/2010	270.860,81	25,793	261.531,09	24,835	532.391,90	50,628	100
29/01/2010	13.222,96	1,254	52.574,50	4,986	65.797,46	6,239	100
28/01/2010	20.225,30	1,921	182.790,59	17,346	203.015,90	19,266	100
27/01/2010	21.833,65	2,076	230.385,94	21,878	252.219,59	23,954	100
26/01/2010	11.907,27	1,787	39.111,46	5,866	51.018,73	7,653	63
25/01/2010	10.843,40	1,464	214.969,49	29,047	225.812,89	30,51	70
24/01/2010	16.663,25	1,582	145.258,33	13,784	161.921,58	15,367	100
23/01/2010	32.012,78	3,081	763.950,39	72,546	795.963,18	75,626	99
22/01/2010	28.268,43	2,682	503.093,13	47,268	531.361,56	49,95	100
21/01/2010	23.391,15	2,244	144.208,22	13,841	167.599,38	16,085	99
20/01/2010	22.987,86	2,19	126.601,05	12,039	149.588,91	14,229	100
19/01/2010	18.628,14	1,773	106.370,50	10,12	124.998,64	11,893	100
18/01/2010	21.427,37	2,032	113.734,49	10,785	135.161,86	12,817	100
17/01/2010	12.712,67	1,206	83.977,55	7,963	96.690,22	9,169	100
16/01/2010	28.987,49	2,756	467.275,55	44,434	496.263,05	47,191	100
15/01/2010	19.853,56	1,888	207.169,44	19,701	227.023,00	21,588	100
14/01/2010	14.423,51	1,374	88.670,45	8,45	103.093,96	9,823	100
13/01/2010	21.963,21	2,092	103.685,31	9,884	125.648,52	11,976	100
12/01/2010	16.962,59	1,878	180.041,03	19,941	197.003,62	21,819	86
11/01/2010	26.947,38	2,564	344.527,14	32,763	371.474,52	35,327	100
10/01/2010	9.324,01	0,888	39.059,14	3,709	48.383,15	4,597	100
09/01/2010	10.890,99	1,04	68.322,21	6,511	79.213,20	7,551	99

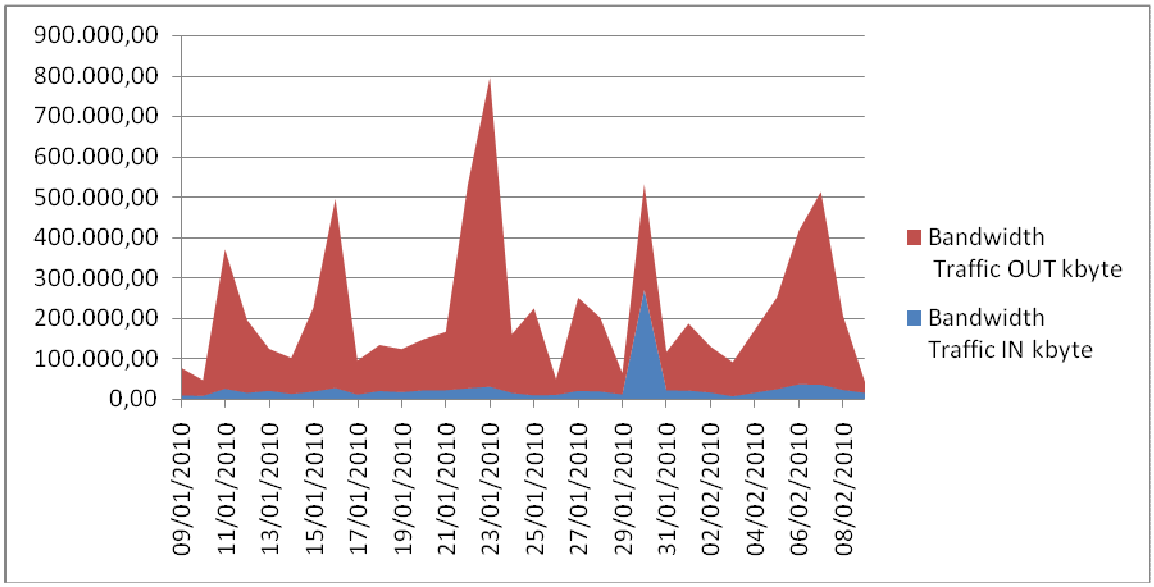


Tabla 5.29 San Idelfonso.

Port Fa0/0 on SANTA ELENA (172.16.118.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	16.192,11	2,822	35.343,35	6,167	51.535,46	8,989	54
08/02/2010	29.203,63	6,089	76.915,35	16,013	106.118,98	22,102	46
07/02/2010	811.059,90	647,696	594.329,90	474,62	1.405.389,81	1.122,32	12
03/02/2010	9.472,85	1,567	41.266,31	6,271	50.739,16	7,837	60
02/02/2010	19.409,73	1,841	154.814,61	14,722	174.224,33	16,562	100
01/02/2010	19.858,07	1,887	227.761,69	21,613	247.619,76	23,5	100
31/01/2010	19.456,96	1,848	205.985,62	19,56	225.442,58	21,408	100
30/01/2010	21.801,29	2,734	91.803,92	8,711	113.605,21	11,445	88
29/01/2010	92.118,50	10,479	38.941,48	3,693	131.059,98	14,172	92
28/01/2010	14.033,75	1,332	70.917,58	6,73	84.951,33	8,061	100
27/01/2010	6.532,52	0,62	79.704,96	7,569	86.237,48	8,189	100
26/01/2010	12.719,02	1,904	114.087,43	17,07	126.806,45	18,974	63
25/01/2010	8.614,35	1,16	53.006,43	7,145	61.620,78	8,305	70
24/01/2010	7.329,59	0,696	32.653,67	3,099	39.983,26	3,795	100
23/01/2010	11.834,59	1,124	189.842,65	18,039	201.677,24	19,163	100
22/01/2010	15.529,92	1,473	172.826,59	16,238	188.356,51	17,711	100
21/01/2010	15.152,01	1,723	140.998,00	13,37	156.150,00	15,094	92
20/01/2010	14.102,76	1,34	170.198,62	16,162	184.301,37	17,502	100
19/01/2010	21.254,52	2,016	409.341,40	38,845	430.595,92	40,86	100
18/01/2010	10.796,29	1,025	85.488,10	8,118	96.284,39	9,143	100
17/01/2010	15.489,74	1,469	135.024,87	12,822	150.514,60	14,291	100
16/01/2010	15.577,13	1,479	185.190,63	17,61	200.767,76	19,089	100
15/01/2010	14.180,25	1,365	56.535,62	5,365	70.715,87	6,729	99
14/01/2010	19.028,08	2,265	136.048,15	12,901	155.076,23	15,167	90
13/01/2010	17.332,87	2,079	104.582,87	9,924	121.915,74	12,003	89
12/01/2010	17.925,68	1,985	60.439,15	6,694	78.364,83	8,678	86
11/01/2010	24.859,20	2,376	90.684,86	8,612	115.544,07	10,988	100
10/01/2010	11.623,65	1,105	42.329,58	4,02	53.953,23	5,125	100
09/01/2010	13.726,41	1,302	61.700,80	5,859	75.427,21	7,161	100

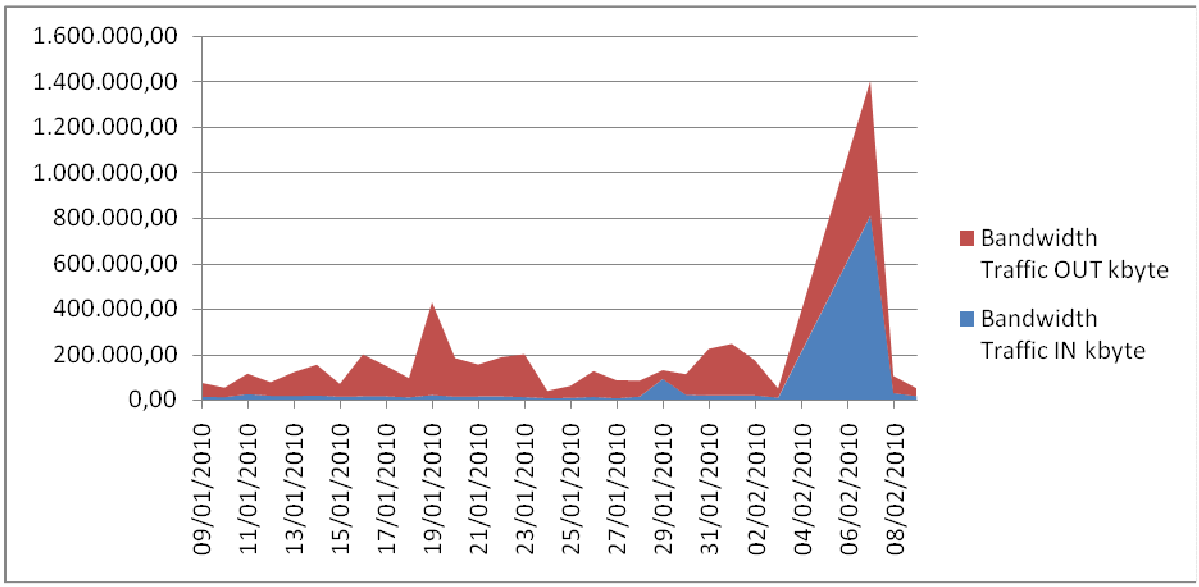


Tabla 5.30 Santa Elena

Port Fa0/0 on SANTA ROSA (172.16.42.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	2.656.142,65	462,473	3.400.214,26	592,024	6.056.356,91	1.054,50	54
08/02/2010	3.690.039,20	349,931	4.804.228,48	455,591	8.494.267,68	805,522	100
07/02/2010	178.260,30	16,905	388.262,61	36,819	566.522,91	53,724	100
06/02/2010	3.198.032,52	303,272	4.682.318,74	444,029	7.880.351,25	747,301	100
05/02/2010	128.041,76	16,407	749.870,87	96,085	877.912,63	112,492	74
03/02/2010	326.752,77	48,861	1.030.988,07	156,668	1.357.740,84	205,529	63
02/02/2010	3.277.869,22	310,834	4.708.286,08	446,479	7.986.155,30	757,314	100
01/02/2010	1.485.708,62	140,888	2.534.009,10	240,298	4.019.717,73	381,186	100
31/01/2010	15.788,24	1,499	76.255,35	7,231	92.043,58	8,73	100
30/01/2010	49.835,35	4,726	145.312,61	13,78	195.147,96	18,505	100
29/01/2010	3.525.521,28	334,323	4.550.835,76	431,551	8.076.357,04	765,875	100
28/01/2010	3.556.315,43	337,238	4.649.408,21	440,892	8.205.723,64	778,13	100
27/01/2010	3.956.239,90	375,165	5.195.199,65	492,654	9.151.439,55	867,819	100
26/01/2010	2.661.727,15	398,914	3.439.556,34	515,77	6.101.283,48	914,684	63
25/01/2010	3.459.776,56	465,891	4.259.247,17	573,549	7.719.023,73	1.039,44	70
24/01/2010	27.624,91	2,62	183.237,08	17,376	210.861,99	19,996	100
23/01/2010	57.643,49	5,466	640.721,23	60,758	698.364,72	66,225	100
22/01/2010	2.601.719,76	246,718	3.595.806,03	337,844	6.197.525,80	584,561	100
21/01/2010	1.416.492,90	134,323	4.137.509,36	392,353	5.554.002,26	526,677	100
20/01/2010	3.308.366,13	313,725	4.850.757,70	459,985	8.159.123,84	773,71	100
19/01/2010	3.182.506,10	301,793	4.922.518,23	466,796	8.105.024,32	768,589	100
18/01/2010	3.461.561,74	328,251	4.615.182,22	437,646	8.076.743,96	765,898	100
17/01/2010	26.214,82	2,486	149.823,63	14,208	176.038,45	16,694	100
16/01/2010	1.653.633,01	156,976	1.881.995,51	178,467	3.535.628,52	335,443	100
15/01/2010	3.304.080,52	313,31	4.230.255,61	401,135	7.534.336,13	714,446	100
14/01/2010	2.995.759,74	284,098	4.034.208,00	382,578	7.029.967,74	666,676	100
13/01/2010	2.866.428,60	271,816	3.632.000,30	344,414	6.498.428,91	616,23	100
12/01/2010	2.855.597,21	315,741	3.405.248,21	376,667	6.260.845,41	692,408	86
11/01/2010	3.196.405,05	303,12	4.670.944,66	442,954	7.867.349,71	746,073	100
10/01/2010	34.921,41	3,312	432.476,75	41,012	467.398,15	44,324	100
09/01/2010	49.605,01	4,704	554.264,39	52,561	603.869,40	57,265	100

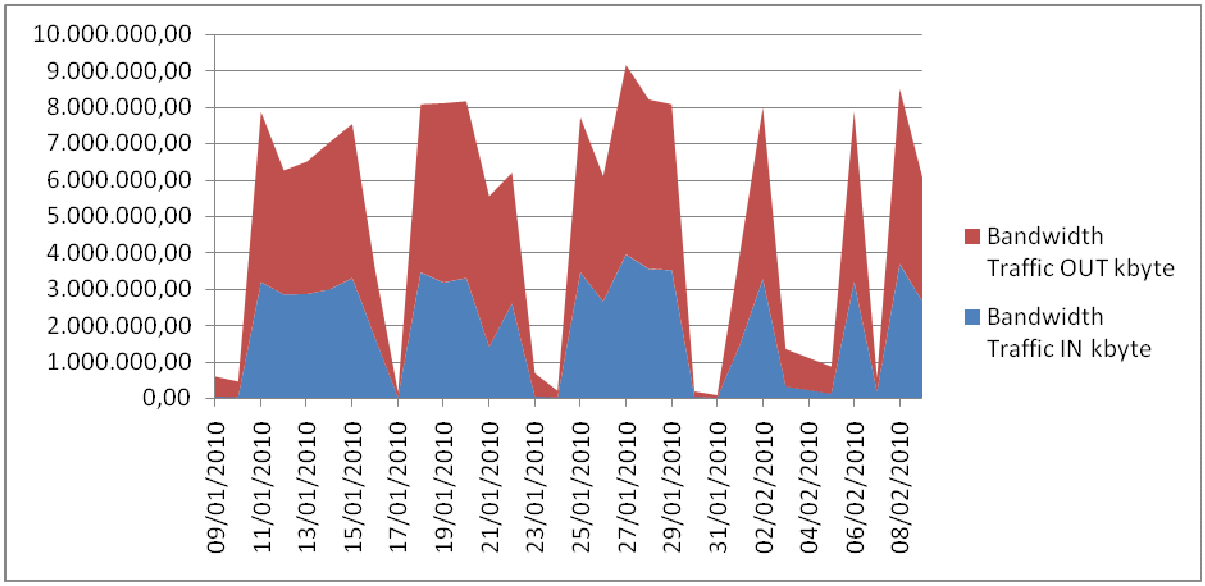


Tabla 5.31 Santa Rosa.

Port Fa0 on SANTO DOMINGO (172.16.45.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	1.289.295,89	224,204	189.758,77	32,998	1.479.054,65	257,202	55
08/02/2010	2.303.514,14	218,446	149.373,39	14,165	2.452.887,53	232,611	100
07/02/2010	2.351.957,55	223,039	86.205,82	8,175	2.438.163,37	231,214	100
06/02/2010	2.432.940,05	230,717	103.567,66	9,821	2.536.507,70	240,539	100
05/02/2010	1.594.965,46	204,365	155.086,21	19,871	1.750.051,67	224,236	74
03/02/2010	1.448.717,08	216,638	149.223,94	22,688	1.597.941,01	239,326	63
02/02/2010	2.412.651,87	228,788	139.574,49	13,236	2.552.226,36	242,024	100
01/02/2010	2.430.640,48	230,495	244.657,55	23,201	2.675.298,03	253,696	100
31/01/2010	2.406.227,12	228,418	242.663,88	23,012	2.648.891,00	251,429	100
30/01/2010	2.477.340,82	234,92	175.312,01	16,624	2.652.652,83	251,544	100
29/01/2010	2.464.995,02	233,752	280.399,55	26,59	2.745.394,56	260,342	100
28/01/2010	2.370.122,23	224,754	273.646,04	25,949	2.643.768,26	250,703	100
27/01/2010	2.500.489,75	237,118	465.983,81	44,189	2.966.473,56	281,307	100
26/01/2010	1.340.183,00	199,747	79.987,47	11,928	1.420.170,47	211,675	64
25/01/2010	1.731.116,00	232,992	153.791,79	20,699	1.884.907,79	253,691	70
24/01/2010	2.456.643,35	232,958	89.237,64	8,462	2.545.880,99	241,42	100
23/01/2010	1.918.100,93	181,891	76.459,58	7,251	1.994.560,51	189,141	100
22/01/2010	1.461.654,45	138,607	172.604,41	16,368	1.634.258,86	154,974	100
21/01/2010	1.950.761,99	184,987	257.002,26	24,371	2.207.764,24	209,358	100
20/01/2010	2.556.894,76	242,466	227.825,74	21,604	2.784.720,50	264,071	100
19/01/2010	2.512.030,27	238,213	252.284,46	23,924	2.764.314,74	262,136	100
18/01/2010	2.456.882,02	232,981	193.567,42	18,356	2.650.449,44	251,337	100
17/01/2010	2.447.115,43	232,057	89.351,36	8,473	2.536.466,79	240,53	100
16/01/2010	2.367.729,66	224,763	104.885,52	9,946	2.472.615,18	234,709	100
15/01/2010	2.369.846,65	224,723	194.393,62	18,434	2.564.240,27	243,157	100
14/01/2010	1.885.658,14	178,823	162.886,63	15,447	2.048.544,77	194,27	100
13/01/2010	1.981.592,85	187,91	127.251,50	12,067	2.108.844,36	199,977	100
12/01/2010	1.858.554,94	205,745	163.409,39	18,097	2.021.964,33	223,843	86
11/01/2010	2.371.539,63	224,896	356.455,53	33,803	2.727.995,17	258,699	100
10/01/2010	2.276.940,71	215,926	81.045,59	7,686	2.357.986,31	223,611	100
09/01/2010	2.317.518,48	219,769	113.891,97	10,8	2.431.410,45	230,57	100

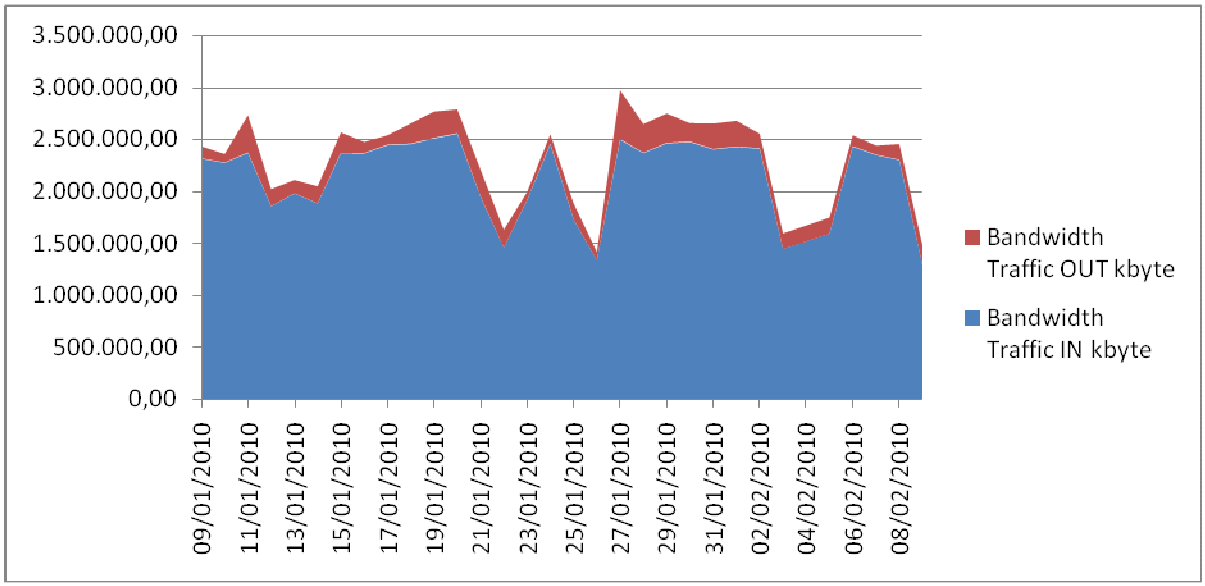


Tabla 5.32 Santo Domingo

Fa4 on TERMOPICHINCHA GUANGOPOLO (192.168.11.2)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	1.386.326,65	240,951	1.161.132,85	201,81	2.547.459,50	442,76	55
08/02/2010	4.017.629,44	380,997	1.818.123,56	172,414	5.835.753,00	553,411	100
07/02/2010	1.844.454,37	174,912	165.716,53	15,715	2.010.170,89	190,627	100
06/02/2010	2.055.700,89	194,944	228.025,75	21,624	2.283.726,64	216,567	100
05/02/2010	2.641.458,96	338,425	1.506.698,16	193,04	4.148.157,12	531,465	74
03/02/2010	1.820.896,57	272,589	1.709.951,30	259,975	3.530.847,87	532,564	63
02/02/2010	4.771.638,06	452,485	4.503.253,11	427,035	9.274.891,17	879,52	100
01/02/2010	3.378.886,86	321,105	3.957.505,71	375,285	7.336.392,56	696,39	100
31/01/2010	807.666,73	76,59	4.300.978,32	407,855	5.108.645,05	484,445	100
30/01/2010	772.023,85	73,21	2.339.557,82	221,856	3.111.581,67	295,066	100
29/01/2010	2.295.802,40	217,705	1.362.346,46	129,189	3.658.148,87	346,894	100
28/01/2010	2.863.277,70	271,519	3.107.566,02	294,685	5.970.843,72	566,204	100
27/01/2010	3.768.907,27	357,398	1.641.014,52	155,614	5.409.921,78	513,012	100
26/01/2010	1.884.965,11	281,804	1.175.167,98	175,785	3.060.133,09	457,589	63
25/01/2010	2.688.942,39	361,916	5.984.160,97	805,434	8.673.103,36	1.167,35	70
24/01/2010	503.038,87	47,702	142.514,92	13,514	645.553,78	61,217	100
23/01/2010	1.404.752,91	133,21	163.212,04	15,477	1.567.964,95	148,687	100
22/01/2010	2.854.046,36	270,645	1.403.619,86	133,103	4.257.666,22	403,748	100
21/01/2010	2.653.930,22	251,666	2.664.624,49	252,681	5.318.554,71	504,347	100
20/01/2010	3.241.683,99	307,405	1.779.757,53	168,772	5.021.441,52	476,177	100
19/01/2010	2.596.343,49	246,466	1.180.720,99	111,966	3.777.064,48	358,432	100
18/01/2010	3.620.057,40	343,762	2.228.637,61	211,338	5.848.695,01	555,1	100
17/01/2010	1.948.644,42	184,788	285.350,19	27,059	2.233.994,61	211,847	100
16/01/2010	1.620.311,49	153,652	309.653,02	29,364	1.929.964,51	183,016	100
15/01/2010	1.852.105,95	175,63	1.368.940,88	129,814	3.221.046,83	305,444	100
14/01/2010	2.597.724,91	246,602	2.304.383,73	218,53	4.902.108,64	465,132	100
13/01/2010	3.720.309,50	352,793	1.289.581,76	122,29	5.009.891,26	475,083	100
12/01/2010	1.546.565,49	171,075	1.131.887,48	125,255	2.678.452,97	296,329	86
11/01/2010	3.982.750,32	377,689	4.862.005,44	461,07	8.844.755,76	838,759	100
10/01/2010	1.106.643,95	104,945	131.989,10	12,517	1.238.633,04	117,462	100
09/01/2010	1.139.159,56	108,026	150.582,34	14,28	1.289.741,90	122,306	100

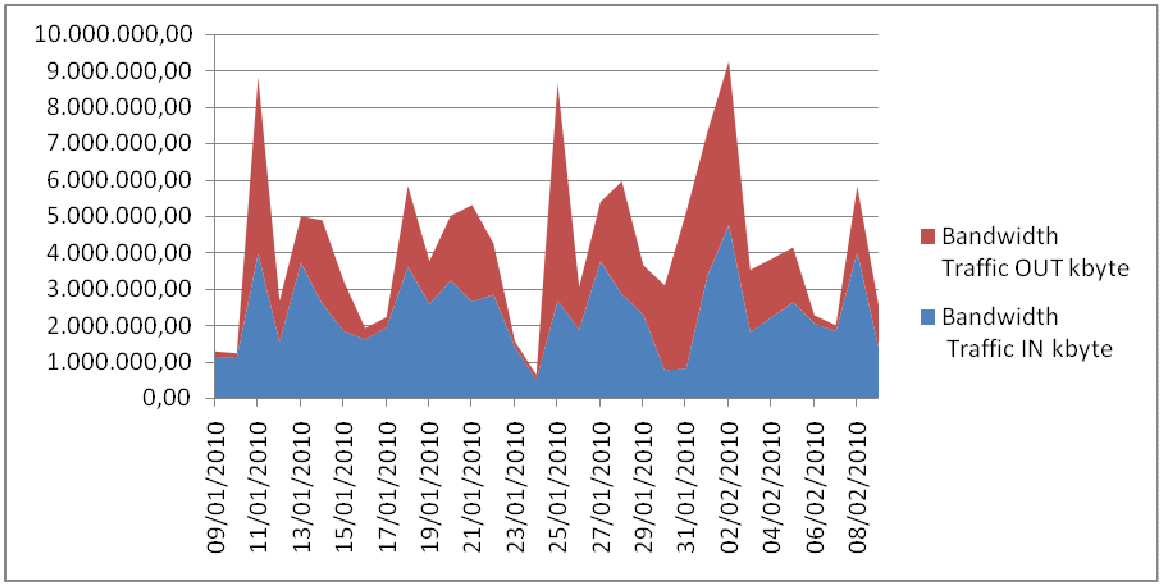


Tabla 5.33 Guangopolo Termo Pichincha

Port Et0 on TOTORAS - LAN TOTORAS							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	27.877,25	4,843	93.475,20	16,24	121.352,45	21,083	55
08/02/2010	72.488,79	6,884	187.819,08	17,823	260.307,86	24,707	100
07/02/2010	90.718,70	8,609	400.428,16	37,973	491.146,85	46,582	100
06/02/2010	42.345,74	4,016	291.510,23	27,644	333.855,97	31,66	100
05/02/2010	46.677,95	5,991	240.812,38	30,877	287.490,32	36,867	74
03/02/2010	45.282,20	6,779	224.986,20	34,207	270.268,40	40,986	63
02/02/2010	72.383,89	6,864	235.337,93	22,317	307.721,81	29,181	100
01/02/2010	111.932,63	10,614	614.859,23	58,306	726.791,86	68,921	100
31/01/2010	44.819,86	4,253	261.745,45	24,838	306.565,31	29,091	100
30/01/2010	37.810,96	3,585	174.864,87	16,582	212.675,83	20,167	100
29/01/2010	67.135,71	6,366	369.825,89	35,094	436.961,60	41,46	100
28/01/2010	91.468,40	8,68	753.037,05	71,409	844.505,45	80,088	100
27/01/2010	88.278,94	8,371	904.071,36	85,732	992.350,29	94,103	100
26/01/2010	58.097,13	8,67	100.552,25	14,998	158.649,39	23,668	64
25/01/2010	83.657,35	11,26	125.149,95	16,844	208.807,30	28,104	70
24/01/2010	47.050,78	4,462	325.611,09	30,877	372.661,87	35,339	100
23/01/2010	44.991,14	4,269	321.943,70	30,551	366.934,84	34,82	100
22/01/2010	178.557,30	16,944	251.382,45	23,847	429.939,75	40,791	100
21/01/2010	126.953,03	12,039	271.797,36	25,774	398.750,38	37,813	100
20/01/2010	88.420,23	8,415	455.551,80	43,199	543.972,03	51,614	100
19/01/2010	150.704,97	14,321	762.419,55	72,351	913.124,53	86,672	100
18/01/2010	169.947,99	16,127	346.504,19	32,904	516.452,18	49,032	100
17/01/2010	33.613,02	3,192	144.528,26	13,715	178.141,27	16,907	100
16/01/2010	45.813,88	4,348	539.827,28	51,191	585.641,16	55,538	100
15/01/2010	137.814,67	13,078	1.224.910,28	116,236	1.362.724,95	129,314	100
14/01/2010	134.508,34	12,783	350.852,31	33,296	485.360,65	46,079	100
13/01/2010	126.589,38	12,012	311.468,71	29,536	438.058,09	41,549	100
12/01/2010	133.670,89	14,793	415.110,13	45,958	548.781,02	60,75	86
11/01/2010	128.075,17	12,146	331.558,30	31,442	459.633,47	43,588	100
10/01/2010	29.596,96	2,813	88.367,77	8,38	117.964,73	11,193	100
09/01/2010	32.841,41	3,116	80.702,20	7,653	113.543,61	10,769	100

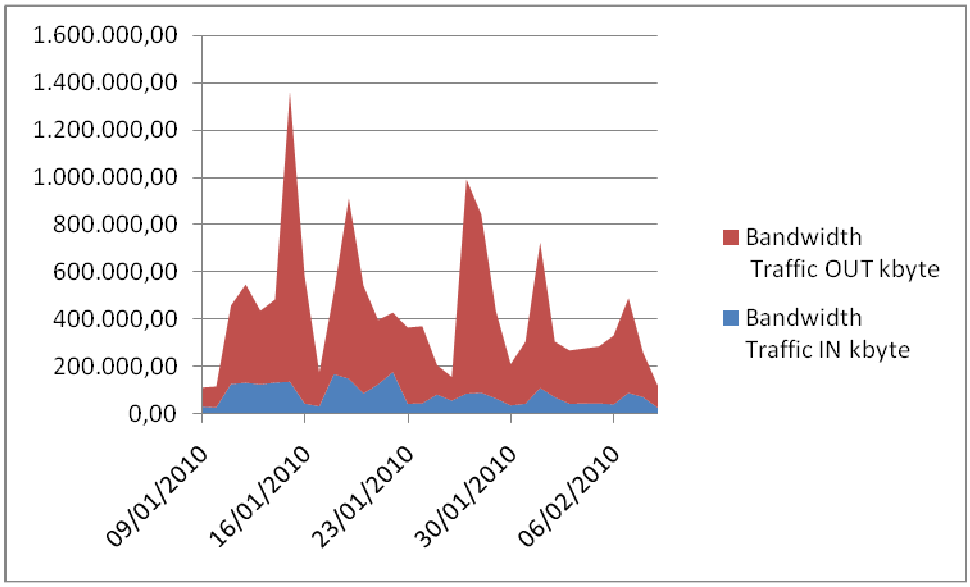


Tabla 5.34 Totoras

Fa0/0 on TRINITARIA (172.16.132.1)							
FECHA	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	4.849,57	0,843	20.039,29	3,483	24.888,86	4,325	55
08/02/2010	7.658,57	0,727	40.905,18	3,882	48.563,75	4,609	100
07/02/2010	11.589,16	1,099	65.468,13	6,213	77.057,29	7,312	100
06/02/2010	12.084,30	1,147	84.737,74	8,036	96.822,03	9,182	100
05/02/2010	8.994,86	1,157	47.175,14	6,062	56.170,00	7,219	74
03/02/2010	5.551,90	0,831	27.093,40	4,117	32.645,29	4,948	63
02/02/2010	13.989,44	1,329	101.730,86	9,654	115.720,30	10,983	100
01/02/2010	11.161,11	1,058	42.273,91	4,02	53.435,02	5,078	100
31/01/2010	12.938,73	1,228	71.443,64	6,789	84.382,38	8,017	100
30/01/2010	10.065,36	0,977	52.948,40	5,025	63.013,76	6,002	99
29/01/2010	10.866,27	1,032	55.246,18	5,239	66.112,45	6,271	100
28/01/2010	15.719,22	1,491	95.927,91	9,103	111.647,13	10,593	100
27/01/2010	7.645,78	0,725	41.312,31	3,918	48.958,09	4,643	100
26/01/2010	3.061,74	0,457	9.794,19	1,465	12.855,92	1,922	63
25/01/2010	4.929,49	0,665	22.340,21	3,007	27.269,69	3,672	70
24/01/2010	14.345,46	1,36	108.614,09	10,321	122.959,55	11,681	100
23/01/2010	8.142,91	0,773	68.226,31	6,474	76.369,22	7,247	100
22/01/2010	15.445,84	1,469	98.905,21	9,379	114.351,05	10,848	100
21/01/2010	13.264,32	1,26	132.457,31	12,587	145.721,63	13,846	100
20/01/2010	7.886,14	0,75	71.159,87	6,826	79.046,00	7,576	99
19/01/2010	8.238,76	0,781	71.185,00	6,755	79.423,76	7,536	100
18/01/2010	5.929,01	0,563	20.032,16	1,9	25.961,18	2,462	100
17/01/2010	6.349,40	0,604	29.485,67	2,796	35.835,07	3,4	100
16/01/2010	6.555,52	0,623	28.906,52	2,741	35.462,04	3,364	100
15/01/2010	8.461,68	0,804	53.004,21	5,03	61.465,90	5,833	100
14/01/2010	9.017,86	0,856	71.743,45	6,804	80.761,31	7,66	100
13/01/2010	9.068,23	0,861	124.278,48	11,794	133.346,71	12,654	100
12/01/2010	6.444,72	0,719	33.172,36	3,69	39.617,08	4,409	85
11/01/2010	6.146,75	0,584	23.957,41	2,273	30.104,17	2,857	100
10/01/2010	4.270,56	0,405	14.276,22	1,355	18.546,78	1,76	100
09/01/2010	9.250,89	0,877	77.397,10	7,365	86.647,99	8,243	100

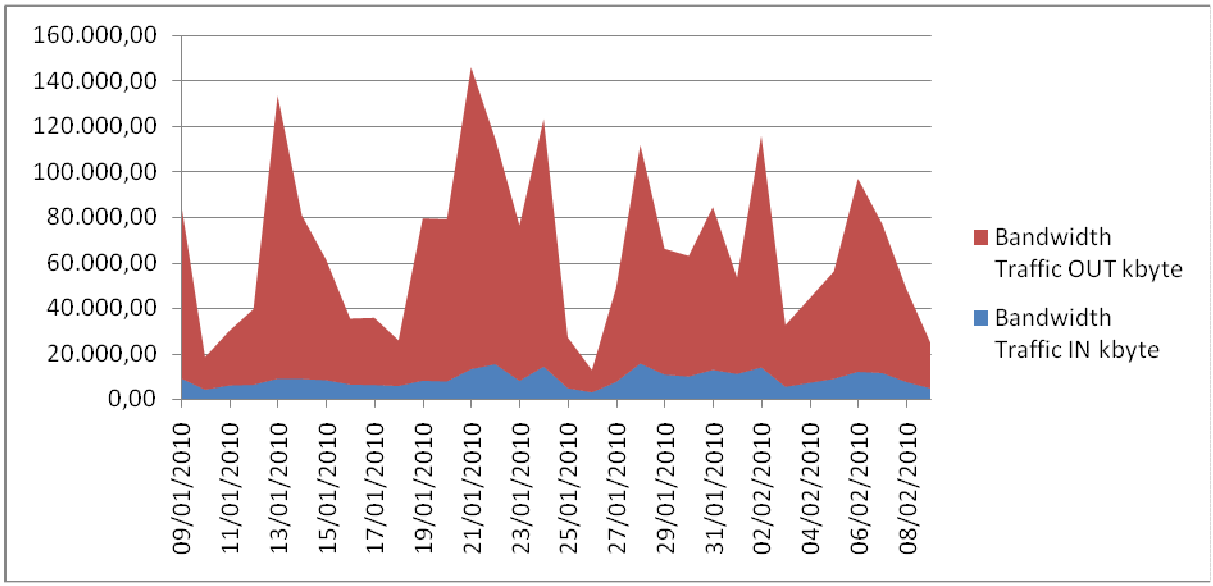


Tabla 5.35 Trinitaria

Fa0/1 on WAN 100megas UIO-SROSA (172.16.26.50)							
	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	3.817.147,16	662,335	4.818.349,03	836,059	8.635.496,19	1.498,40	55
08/02/2010	5.482.884,33	519,95	7.618.565,85	722,479	13.101.450,18	1.242,43	100
07/02/2010	1.408.515,40	133,571	4.227.794,12	400,926	5.636.309,53	534,497	100
06/02/2010	5.404.623,77	512,525	7.357.239,29	697,694	12.761.863,06	1.210,22	100
05/02/2010	1.433.361,97	183,611	3.004.285,54	384,843	4.437.647,51	568,454	74
03/02/2010	1.392.337,56	208,207	2.835.371,26	430,868	4.227.708,81	639,075	63
02/02/2010	5.223.501,52	495,335	7.331.981,38	695,279	12.555.482,90	1.190,61	100
01/02/2010	3.297.751,16	312,723	5.617.635,13	532,715	8.915.386,29	845,438	100
31/01/2010	1.117.338,82	106,067	4.179.499,52	396,337	5.296.838,33	502,403	100
30/01/2010	858.577,48	81,416	5.435.693,88	515,449	6.294.271,35	596,865	100
29/01/2010	5.370.999,49	509,327	8.624.379,64	817,841	13.995.379,12	1.327,17	100
28/01/2010	5.414.597,08	513,454	7.752.282,40	735,133	13.166.879,48	1.248,59	100
27/01/2010	6.259.944,27	593,622	8.147.378,23	772,604	14.407.322,51	1.366,23	100
26/01/2010	4.214.308,17	627,896	5.084.325,07	757,933	9.298.633,24	1.385,83	64
25/01/2010	4.724.545,02	635,887	6.344.591,14	853,932	11.069.136,15	1.489,82	70
24/01/2010	1.076.219,89	102,055	5.511.519,55	522,645	6.587.739,44	624,7	100
23/01/2010	1.280.305,90	121,409	4.604.154,47	436,603	5.884.460,37	558,012	100
22/01/2010	4.575.890,45	433,926	6.467.165,71	613,273	11.043.056,16	1.047,20	100
21/01/2010	5.044.984,00	478,407	5.821.003,01	551,995	10.865.987,01	1.030,40	100
20/01/2010	5.649.876,81	535,765	8.399.537,35	796,511	14.049.414,16	1.332,28	100
19/01/2010	5.862.517,59	555,935	8.275.323,88	784,741	14.137.841,47	1.340,68	100
18/01/2010	5.337.747,04	506,163	8.439.994,68	800,342	13.777.741,72	1.306,51	100
17/01/2010	617.276,96	58,536	5.063.374,32	480,153	5.680.651,28	538,689	100
16/01/2010	2.496.853,91	237,021	6.111.468,11	579,541	8.608.322,02	816,562	100
15/01/2010	4.909.426,30	465,538	7.356.591,67	697,592	12.266.017,97	1.163,13	100
14/01/2010	4.895.919,67	464,297	7.080.847,78	671,503	11.976.767,45	1.135,80	100
13/01/2010	4.165.372,46	394,991	6.517.196,21	618,009	10.682.568,68	1.013,00	100
12/01/2010	3.969.885,64	439,05	6.152.574,80	680,717	10.122.460,44	1.119,77	86
11/01/2010	5.868.679,72	556,536	7.364.017,33	698,341	13.232.697,05	1.254,88	100
10/01/2010	1.016.268,78	96,374	4.019.753,53	381,2	5.036.022,31	477,574	100
09/01/2010	1.039.443,30	98,57	4.068.750,41	385,837	5.108.193,71	484,406	100

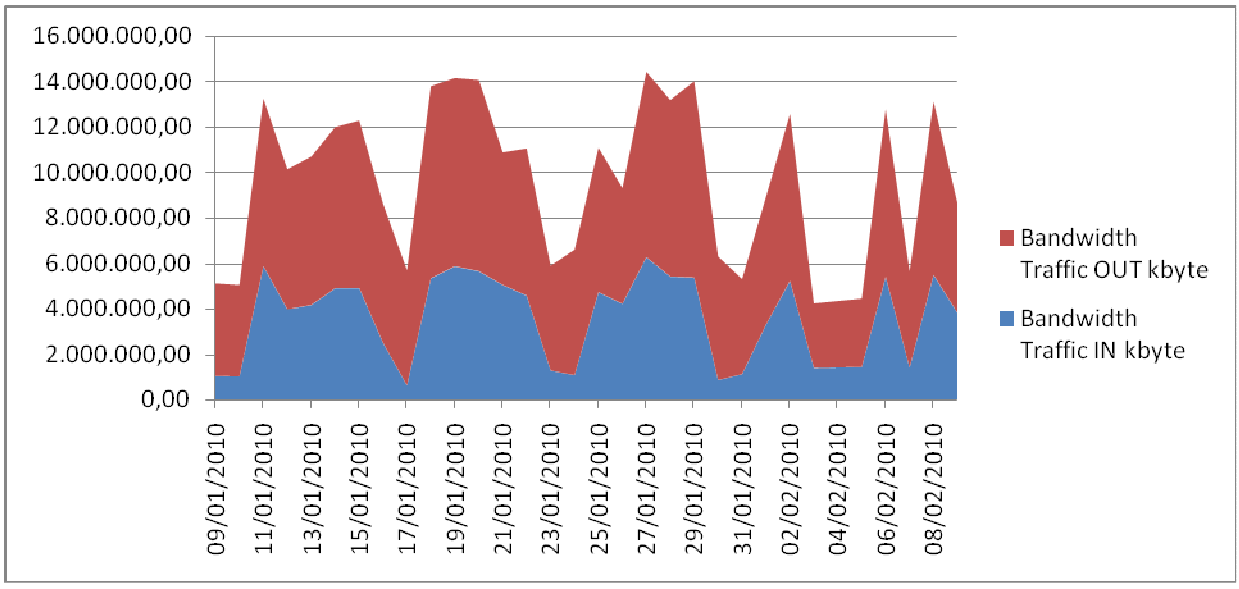


Tabla 5.36 Santa Rosa.

Fa0/0 on VICENTINA (172.16.62.1)							
	Bandwidth Traffic IN	Bandwidth Traffic IN	Bandwidth Traffic OUT	Bandwidth Traffic OUT	SUM	SUM	Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
09/02/2010	28.120,42	4,875	73.092,46	12,672	101.212,88	17,548	55
08/02/2010	50.336,79	4,777	210.489,96	19,989	260.826,75	24,766	100
07/02/2010	97.896,83	9,29	461.518,41	43,796	559.415,24	53,086	100
06/02/2010	101.689,44	9,643	259.383,27	24,649	361.072,71	34,292	100
05/02/2010	92.209,19	11,813	294.362,87	37,711	386.572,07	49,524	74
03/02/2010	8.320,48	1,244	9.108,02	1,384	17.428,50	2,628	63
02/02/2010	16.497,58	1,566	43.426,01	4,118	59.923,59	5,684	100
01/02/2010	36.537,44	3,465	88.714,25	8,413	125.251,69	11,878	100
31/01/2010	54.897,72	5,222	169.250,51	16,061	224.148,22	21,283	100
30/01/2010	107.642,03	10,207	258.990,92	24,559	366.632,95	34,767	100
29/01/2010	54.214,75	5,141	191.335,81	18,144	245.550,57	23,285	100
28/01/2010	24.245,15	2,299	123.436,97	11,705	147.682,12	14,004	100
27/01/2010	51.220,08	4,857	205.220,74	19,461	256.440,82	24,318	100
26/01/2010	14.273,56	2,133	67.579,64	10,102	81.853,20	12,235	63
25/01/2010	17.897,10	2,415	107.634,93	14,523	125.532,03	16,937	70
24/01/2010	117.552,11	11,155	344.787,63	32,718	462.339,74	43,873	100
23/01/2010	39.970,40	3,793	122.673,98	11,641	162.644,37	15,434	100
22/01/2010	74.422,56	7,057	366.754,67	34,779	441.177,23	41,836	100
21/01/2010	70.953,31	6,671	295.083,83	27,725	366.037,14	34,396	101
20/01/2010	25.508,35	2,419	174.791,38	16,599	200.299,73	19,017	100
19/01/2010	63.716,34	6,042	189.182,00	17,94	252.898,34	23,982	100
18/01/2010	38.343,94	3,636	99.917,01	9,475	138.260,94	13,111	100
17/01/2010	40.034,25	3,796	104.081,93	9,87	144.116,19	13,666	100
16/01/2010	49.654,34	4,717	161.419,09	15,318	211.073,44	20,034	100
15/01/2010	42.028,27	3,985	133.254,46	12,636	175.282,73	16,621	100
14/01/2010	43.527,04	4,131	150.797,97	14,31	194.325,02	18,441	100
13/01/2010	35.041,82	3,325	107.695,34	10,22	142.737,16	13,545	100
12/01/2010	54.098,43	5,992	164.510,66	18,199	218.609,09	24,191	86
11/01/2010	92.417,96	8,776	285.028,02	27,03	377.445,99	35,806	100
10/01/2010	64.531,96	6,12	190.113,14	18,041	254.645,10	24,161	100
09/01/2010	26.018,45	2,467	60.024,93	5,692	86.043,37	8,159	100

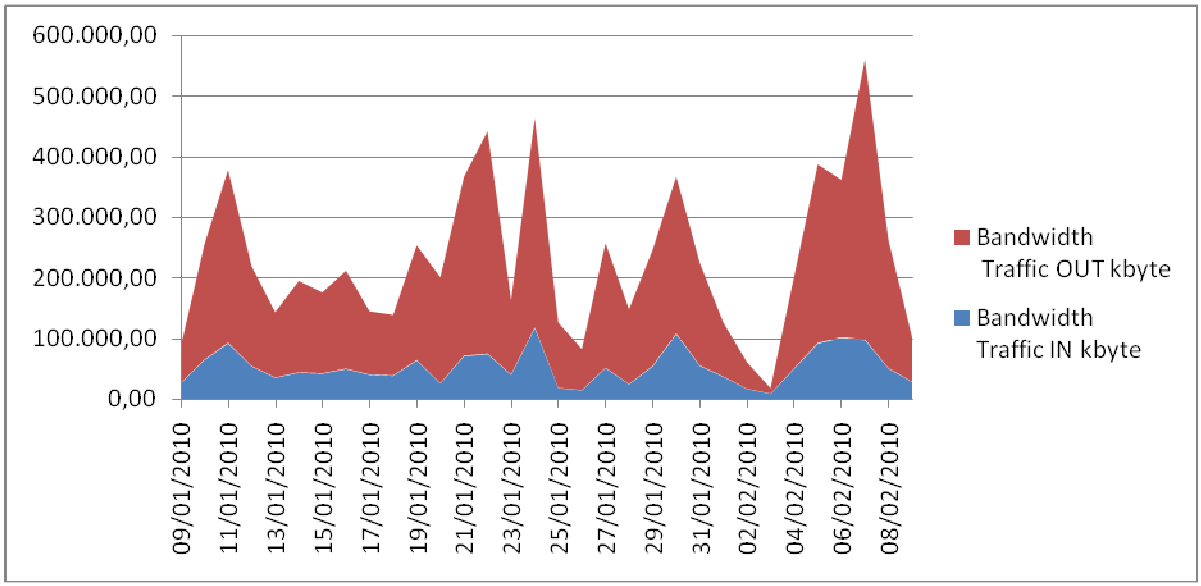


Tabla 5.37 Vicentina