UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

ESCUELA DE INGENIERÍA ELECTRÓNICA

"DISEÑO DE UNA RED DE BACKBONE CON TECNOLOGÍA MPLS PARA EL SOPORTE DE SERVICIOS TRIPLE PLAY EN LA EMPRESA ECUANET-MEGADATOS S.A"

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

SANDRA KARINA NARVÁEZ PUPIALES

DIRECTOR: ING. ROBERTO MARCILLO

Ibarra - 2010

DECLARACIÓN

Yo, Sandra Karina Narváez Pupiales, declaro bajo juramento que el trabajo aquí descrito es de mí autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual, Reglamentos y Normatividad vigente de la Universidad Técnica del Norte.

Sandra Karina Narváez Pupiales

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Sandra Karina Narváez Pupiales, bajo mi supervisión.

Ing. Roberto Marcillo

DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Agradezco, a Dios por guiar mi camino y por darme fortaleza a lo largo de todos estos años, a mis padres y mis hermanos por brindarme el apoyo incondicional en todo momento, a la Universidad Técnica del Norte que aportó a mi formación profesional y personal, a mi Director Ing. Roberto Marcillo por su valiosa colaboración para la culminación del presente Proyecto, a la empresa Ecuanet-MEGADATOS en especial al Ing. Marco Logacho y personal de soporte técnico por su generosa ayuda y finalmente gracias a los ingenieros Francisco Frey, Jorge Caraguay y demás docentes y amigos que contribuyeron con su asesoría durante el desarrollo del presente Proyecto.

Sandra

DEDICATORIA

Dedico este Proyecto de Titulación a mis padres María Oliva y Jesús quienes me han entregado su apoyo, cariño y comprensión en todo momento a lo largo de mi vida en especial para el cumplimiento de este objetivo ayudándome con sus concejos a levantarme tras cada caída y a luchar con más fuerza.

Sandra

CONTENIDO

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

RESUMEN

Con el avance tecnológico, el crecimiento de la demanda y los exigentes requerimientos de los usuarios la tendencia de las Telecomunicaciones gira en torno a la integración de los servicios bajo infraestructuras de redes únicas que permitan ofrecer a los clientes ofertas variadas de servicios y aplicaciones. Es importante para los operadores y proveedores de redes la implementación de nuevas tecnologías para por un lado satisfacer la demanda de los usuarios y por otro permanecer competitivos en este mercado. Una de las tecnologías que se deben implementar y quizá la más importante es MLPS que ofrece los mecanismos para integrar otras tecnologías y servicios con QoS facilitando la migración a las redes NGN.

El presente proyecto propone una alternativa de diseño para la implementación de MPLS en la red de la empresa Ecuanet-MEGADATOS para el soporte de servicios Triple Play considerando la tecnología e infraestructura desplegada en la actualidad tomando como referente un segmento de mercado inicial.

La provisión de servicios Triple Play requiere además del estudio de implementación de otras capas a nivel superior e inferior en especial para los servicios IPTV y VoIP que se ha expuesto conjuntamente con propuestas de equipos y del presupuesto necesario.

ABSTRACT

With the technological advances, the demand growth and the demanding requirements of the users the Telecommunications trend revolves around the integration of services under single network infrastructure to enable customers to offer various service offerings and applications. It is important for operators and network providers to implement new technologies on the one hand meet the demand of users and the other to remain competitive in this market. One of the technologies to be implemented and perhaps the most importantly is MPLS that offer the mechanisms to integrate other technologies and services with QoS to facilitate the migration to NGN networks.

The present project proposes a design alternative to implement MPLS in the network of Ecuanet-MEGADATOS to support Triple Play services considering the technology and infrastructure currently deployed in reference to an initial market segment.

The provision of Triple Play services also requires the study of implementation of other layers to upper and lower level especially for IPTV and VoIP services to be exposed together with proposals for equipment and the budget required.

PRESENTACIÓN

El presente proyecto tiene como objetivo realizar el diseño de una red de Backbone con tecnología MPLS para el soporte de servicios Triple Play en la empresa Ecuanet-MEGADATOS, considerando la tecnología desplegada en la actualidad y la cobertura inicial para las ciudades de Quito, Guayaquil y Cuenca.

En el primer capítulo se presenta un breve análisis de las nuevas tecnologías de redes NGN, características más importantes, modelo referencial por capas, elementos, protocolos y las pautas generales para la migración de una red tradicional a redes convergentes para brindar servicios convergentes.

En el segundo capítulo se analiza la tecnología MPLS, como paso fundamental para la migración de las redes, se presenta las características, los elementos básicos, encabezado MPLS, descripción funcional, aplicaciones y ventajas sobre otras tecnologías de transporte a nivel de enlace además de la importancia de su implementación en las redes troncales para brindar Calidad de Servicio extremo a extremo y servicios Triple Play.

En el tercer capítulo se realiza un breve estudio de la Infraestructura actual de la empresa, las tecnologías y cobertura de las redes a nivel nacional, equipamiento utilizado en los principales nodos, análisis FODA de la empresa, estadísticas de usuarios por servicio y planteamiento de los requerimientos de la red de backbone para el soporte de nuevas aplicaciones.

En el cuarto capítulo se considera los aspectos generales que se deben tomar en cuenta para el diseño de una red de backbone, seguido del desarrollo del diseño que incluye los requerimientos de los servicios Triple Play, cobertura de la red, topología y elementos, se estima además la proyección de la capacidad del backbone para

algunos años, equipos, costos de implementación y también se presenta una simulación de la red de core con características MPLS en el software GNS3.

En el quinto capítulo se exponen las conclusiones y recomendaciones obtenidas en el desarrollo del presente Proyecto.

Finalmente en los Anexos se incluye un glosario de términos, configuración de equipos y comandos Cisco adicionales para la implementación de MPLS en las redes con características de Ingeniería de Tráfico y VPN/MPLS, un análisis de los indicadores de rentabilidad y un manual para la utilización del software GNS3.

CAPÍTULO 1. ANÁLISIS DE LAS TECNOLOGÍAS NGN

1.1 INTRODUCCIÓN

Los proveedores de voz, video y datos distribuyen a los usuarios y clientes sus servicios utilizando diferente infraestructura. Con la evolución de las tecnologías estas redes existentes deben adaptarse a los nuevos requerimientos de los usuarios, basados en el mejoramiento de las prestaciones y costos, que permitan el uso de una sola infraestructura de red. Es inminente para la competitividad de las empresas de Telecomunicaciones la necesidad de migrar sus redes a nuevas tecnologías de convergencia. El modelo de red propuesto por la UIT[1] para cumplir con estas características se denomina NGN[2] o Redes de Próxima Generación.

El éxito rotundo del Internet en el mercado de las Telecomunicaciones ha permitido el acoplamiento de otros servicios al protocolo IP[3] como la voz y video, siendo éste protocolo fundamental para el acceso del usuario a una infraestructura de red NGN.

1.2 GENERALIDADES DE UNA RED NGN

Actualmente la tendencia de las Telecomunicaciones está orientada a la integración de los servicios y de la infraestructura fija y móvil, capaz de soportar tráfico telefónico y nuevas aplicaciones de Internet.

La infraestructura de las redes NGN se acopla a las tecnologías de redes existentes soportadas en ATM[4], Frame Relay, PSTN[5], Ethernet, etc; migrar a NGN no significa reemplazar la infraestructura existente, sino la integración con características de movilidad de las redes inalámbricas, fiabilidad de la red PSTN, alcance geográfico de Internet y la capacidad de transmisión de las redes de fibra óptica.

---

[1] **UIT** Unión Internacional de Telecomunicaciones
[2] **NGN** Next Generation Network
[3] **IP** Internet Protocol
[4] **ATM** Asynchronous Transfer Mode
[5] **PSTN** Public Switched Telephone Network

CAPÍTULO 1

1.2.1 DEFINICIÓN DE NGN

Según la UIT-T se define a NGN como "*una red basada en paquetes que permite prestar servicios de Telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por QoS*[6]*, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes de proveedores de servicios y/o servicios de su elección. Se soporta movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios*". [1]

1.2.2 CARACTERÍSTICAS DE LAS REDES NGN

A continuación se presentan las características de una red de Siguiente Generación:

- Plataforma de red común que permite la prestación de múltiples servicios.
- Capacidad de adaptarse a todo tipo de tecnología existente ya sea de transporte o de acceso.
- Es una red flexible y escalable que permite acoplarse a las necesidades y requerimientos de los usuarios.
- Soporte de servicios de tiempo real y no real, streaming y servicios multimedia.
- Soporte de diversos medios de transmisión como: par trenzado, fibra óptica y radiofrecuencia.
- Garantiza alta disponibilidad de funcionamiento en su infraestructura, basándose en la priorización del tráfico, utilizando Calidad de Servicio.
- Los servicios que brinda una red NGN permiten total transparencia para el usuario.

---

[6] **QoS** Quality of Service

- Interconexión con las redes existentes fijas y móviles por medio de interfaces abiertas.

- Se basa en sistemas inteligentes para controlar y tarifar en tiempo real los servicios que el usuario necesita, dependiendo de sus requerimientos, sin realizar trámites con el proveedor (bajo demanda).

1.2.3 CONVERGENCIA

NGN es una infraestructura de red en donde convergen servicios y redes, la convergencia de servicios se da en torno a la prestación de aplicaciones de distinta naturaleza para el usuario y convergencia de redes porque se integran diferentes redes tradicionales de acceso y de transporte bajo una sola plataforma común de control y gestión.

La convergencia de servicios de voz, datos y video se lo denomina Triple Play, el usuario recibe estos servicios a través de una conexión de banda ancha por medio de cualquier tecnología de acceso y usando cualquier medio de transmisión y por los que también recibe una sola factura. En la figura 1.1 se muestra la convergencia de servicios en una red NGN.

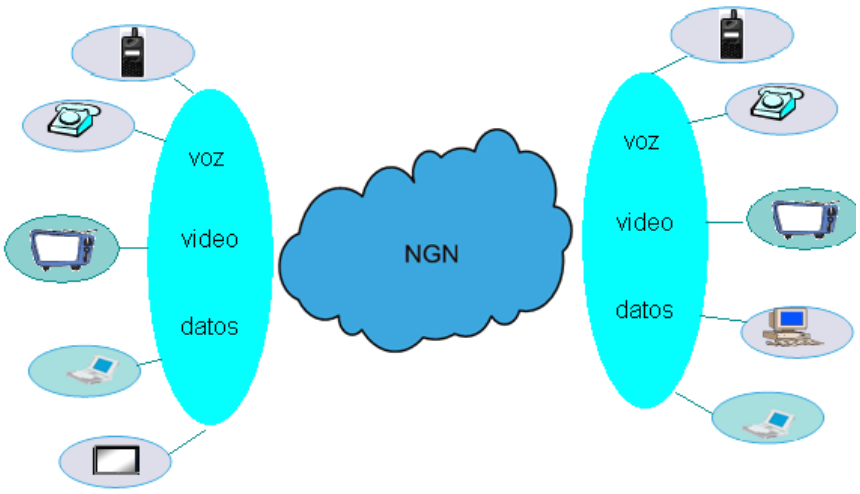


Figura 1.1 Convergencia de Servicios de una red NGN a usuario final

La unión del Triple Play con aplicaciones, bajo una infraestructura de red NGN se denomina Quad Play y ofrece a los usuarios combinaciones de servicios como:

- Servicios de voz que incluyen mensajería y telefonía.
- Servicios de datos (correo electrónico, web, intercambio de archivos).
- Servicios de video (televisión, juegos interactivos, videotelefonía).
- Otros servicios (video bajo demanda, IVR[7], transacciones, conferencias con compartición de archivos y aplicaciones, servicios basados en localización, etc.)

1.3 ESQUEMA DEL MODELO REFERENCIAL DE UNA RED NGN

NGN es una infraestructura de red que para este estudio se explica mediante niveles basados en un modelo jerárquico para facilitar la comprensión. Cada nivel cumple con una función específica y dentro de cada uno existe equipamiento que tiene un propósito y se describe posteriormente.

Los niveles dispuestos jerárquicamente son: Gestión y Servicio, Control de Red, Núcleo y Acceso del Terminal. A continuación en la figura 1.2 se representa una topología general de una red NGN conjuntamente con equipos genéricos en cada nivel.

[7] **IVR** Interactive Voice Response

CAPÍTULO 1

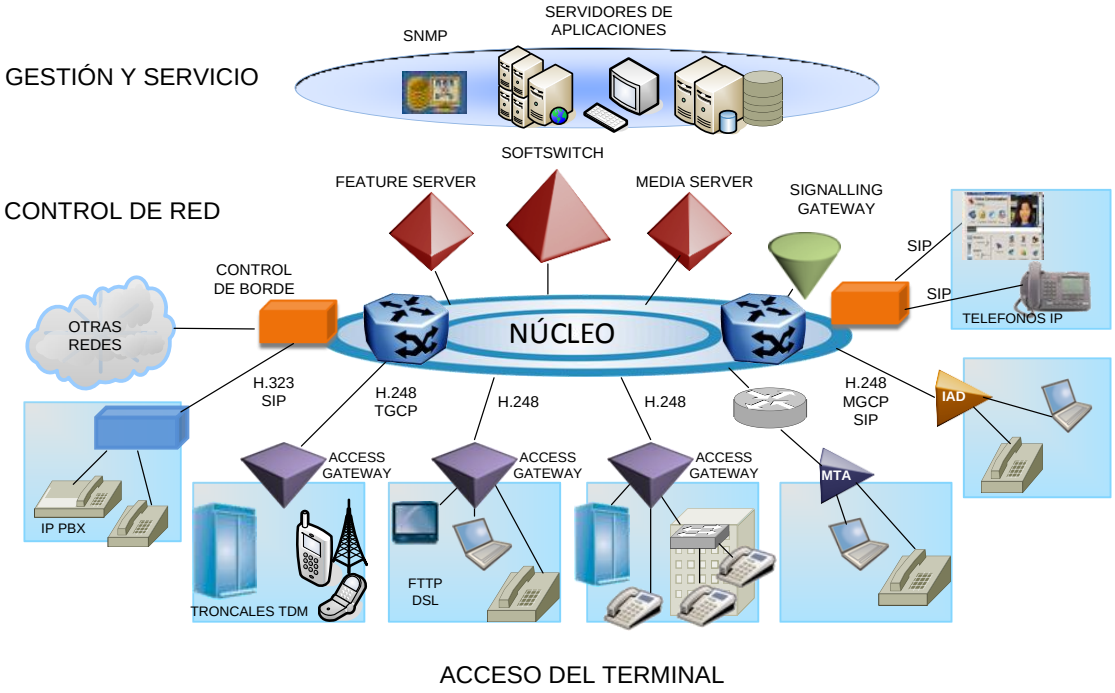


Figura 1.2 Esquema Topológico de una red NGN

1.3.1 GESTIÓN Y SERVICIO

"En este nivel se realizan las funciones relacionadas con la operación y administración de la red y sus servicios. Las tareas incluyen aspectos como la gestión de fallas, configuración de red y elementos, medición de desempeño, tasación, seguridad, gestión de tráfico y QoS". [2]

Los servicios y aplicaciones se ofrecen a toda la red, sin importar la ubicación del usuario, siendo los servicios independientes de la tecnología de acceso que se utilice.

La administración y gestión se basan generalmente en aplicaciones de software sobre plataformas abiertas UNIX, LINUX o Windows en configuración cliente-servidor, para gestionar por una parte los diferentes elementos de red y por otra las interfaces para sistemas informáticos u otros sistemas de jerarquía superior como los sistemas de facturación y los sistemas de distribución de servicios finales.

En este nivel los servidores pueden ser de diferente funcionalidad como:

1. **SERVIDORES DE APLICACIÓN**

   Proveen la ejecución de los servicios como por ejemplo el control de los servidores de llamadas y los recursos especiales de NGN (servidores de video, servidores de mensajes, etc.).

2. **SERVIDORES DE GESTIÓN**

   Son los encargados de administrar todos los elementos de red para adaptarlos a la Calidad de Servicio requerida, además de la implementación de la seguridad mediante Sistemas de Detección de Intrusos, Cortafuegos gestionados y almacenamiento. Permite la provisión, recuperación, supervisión y análisis del desempeño de extremo a extremo de la red.

1.3.2 CONTROL DE RED

En este nivel se encuentran los dispositivos que se encargan de controlar e interconectar a la red con otras redes proporcionando los mecanismos para el manejo de los elementos a nivel del núcleo a través de diferentes protocolos que permiten el funcionamiento de la red en su totalidad y sus servicios en forma homogénea y coordinada. Los equipos y aplicaciones que hacen posible el control de los elementos del núcleo de red e interconexión con otras redes son: el Softswitch, Signalling Gateway, Media Server y Feature Server.

1.3.2.1 Softswitch

El Softswitch es un dispositivo que incorpora una combinación de software y hardware para el control de una red telefónica tradicional y aplicaciones de una red de conmutación de paquetes IP, posibilitando la interconexión de las diferentes redes existentes ATM, Frame Relay, PSTN entre otras, combinando las funciones de señalización, el control de las conexiones y la mediación del servicio con la finalidad de facilitar aplicaciones multimedia en tiempo real.

Mediante software, el Softswitch realiza las conexiones entre los dispositivos para el manejo de voz, datos y enrutamiento de llamadas a través de los diversos tipos de redes utilizando estándares e interfaces abiertas, facilitando la migración a las Redes de Próxima Generación.

1.3.2.1.1 Características

- **Inteligencia:** Permite controlar los servicios de conexión asociados a los Media Gateways y los puntos terminales que utilizan el protocolo IP.

- **Enrutamiento de las llamadas:** En función de la señalización y de la información almacenada en la base de datos de los clientes.

- **Transferencia:** La capacidad para transferir el control de una llamada a otro elemento de la red.

- **Interfaces:** Para las funciones de gestión como los sistemas de facturación y provisión de servicios.

- **Coexistencia:** Puede existir con las redes tradicionales o redes conmutadas así como puede proveer los servicios de la tecnología de conmutación de paquetes en dispositivos finales como son: teléfonos tradicionales, teléfonos IP, computadores, beepers, terminales de videoconferencia y más.

1.3.2.2 Signalling Gateway (Pasarela de Señalización)

El Signalling Gateway es un elemento de red cuya función principal es enrutar y manipular la señalización, sirviendo de puente entre la red de señalización SS7[8] y los nodos que maneja el Softswitch, éste elemento puede estar integrado o ser un dispositivo independiente dentro de la red, en el nivel de Control.

---

[8] **SS7** Signalling System 7

Las funciones que realiza son las siguientes:

- El Signalling Gateway encapsula y transporta protocolos de señalización desde una red telefónica tradicional (SS7) hacia un Softswitch o a otro Signalling Gateway.
- Puede transportar mensajes SS7 entre los distintos medios: SS7 sobre TDM[9], SS7 sobre IP y SS7 sobre ATM.
- El Gateway de señalización establece el protocolo, tiempo y requerimientos de las redes SS7.
- Provee conectividad física para la red SS7 vía T1/E1[10] o T1/V.35[11].
- Ofrece alta disponibilidad de operación para servicios de Telecomunicaciones, ya que no solamente se lo utiliza para servicios de voz, sino también para servicios de datos mediante la interconectividad con redes ATM y Frame Relay.

1.3.2.3 Media Server (Servidor de Medios)

Mejora las características funcionales del Softswitch con el soporte de aplicaciones como:

- Integración de fax y mail box, notificando por e-mail o pregrabación de los mensajes.
- Capacidad de videoconferencia.
- Soporte de múltiples códecs.
- Unificación de los mensajes de lectura para voz, fax y e-mail por una interfaz Ethernet.
- IVR es un dispositivo que tiene como interfaz hacia el usuario un script de voz y recibe comandos a través de tonos DTMF[12].
- Control sobre múltiples servidores de aplicación.
- Funciona bajo el control de un servidor de aplicaciones como el Softswitch por medio de los protocolos MGCP[13] o SIP[14].

---

[9] **TDM** Time Division Multiplexed
[10] **T1/E1** 1.5 Mbps/2Mbps
[11] **T1/V.35** 1.5 Mbps/48-168Kbps
[12] **DTMF** Dual-Tone Multi-Frequency
[13] **MGCP** Media Gateway Control Protocol
[14] **SIP** Session Initial Protocol

1.3.2.4 Feature Server (Servidor de Capacidades)

Es una aplicación a nivel de servidor, el cual aloja un conjunto de servicios de valor agregado y pueden ser parte del Softswitch o pueden ser desarrollados por los proveedores, pero la principal funcionalidad es la tarifación en tiempo real de los servicios y recursos de la red.

Las aplicaciones más comunes del Feature Server son las siguientes:

- Servicios de Facturación: manteniendo información de los detalles de cada sesión.
- Centralización de Llamadas: distribución automática de llamadas a múltiples destinos.
- Utiliza el Signalling Gateway para la autenticación y autorización de la llamada.

1.3.3 NÚCLEO

El núcleo o core permite la conectividad del nivel de acceso con los niveles superiores para que los usuarios puedan acceder a los servicios de la red NGN. La función principal de este nivel es el transporte y enrutamiento del tráfico generado de extremo a extremo de la red mediante la interconexión de switches, routers y dispositivos de control de borde.

La tecnología que se utilice en el núcleo depende de las consideraciones comerciales de los proveedores pero ésta debe garantizar la transparencia y QoS. La tendencia en la actualidad es la utilización de una nueva tecnología de redes de transporte ASON[15] en la implementación del núcleo que de soporte a nuevas aplicaciones con alta Calidad de Servicio. A continuación se da una descripción general de una red de transporte ASON.

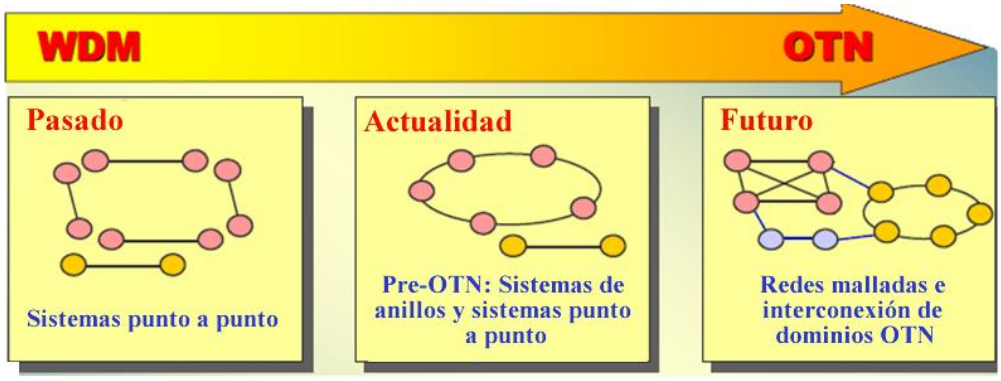
1.3.3.1 ASON

ASON, Red óptica automáticamente conmutada, es un nuevo concepto en la evolución de las redes ópticas de transporte OTN[16] que tiene como objetivo automatizar la gestión de los recursos y componentes de la red de núcleo. Este tipo de red permite la adaptación de los requerimientos de los usuarios mediante la configuración rápida y eficiente de los componentes de la red.

---

[15] **ASON** Automatically Switched Optical Netwok
[16] **OTN** Optical Transport Network

Dentro de las características más importantes: ASON utiliza una topología en malla y garantiza diferentes niveles de Calidad de Servicio además del soporte de OVPN[17] (Redes Privadas Virtuales Ópticas). A continuación en la figura 1.3 se muestra la evolución de las redes de transporte basadas en fibra óptica desde WDM (Wavelength Division Multiplexing) hasta OTN.



Fuente: http://www.eurescom.de

Figura 1.3 Evolución de las Redes Ópticas de Transporte

1.3.4 ACCESO DE TERMINAL

Este nivel provee al usuario el acceso a los servicios de la red NGN (Next Generation Network) independientemente del tipo de terminal y medio empleado por medio de gateways de acceso y gateways de red, usando protocolos e interfaces abiertas para acceder a la NGN.

Los gateways tienen la función de ejecutar mecanismos de QoS tratando directamente con el tráfico generado por el usuario como: filtrado de paquetes y clasificación del tráfico.

1.3.4.1 Access Gateway o Pasarela de Acceso

Permite la conectividad de los terminales con el núcleo de red NGN y su función principal es la conversión de la información a IP para el acceso del usuario, actuando bajo el control del Softswitch.

---

[17]**OVPN** Optical Virtual Private Network

Existe diferentes subtipos de acuerdo a la tecnología de acceso que se utilice, un subtipo muy importante son los MSAN[18] también conocidos como Nodos de Acceso Multiservicio, los cuales brindan servicios de banda ancha y Triple Play soportando una migración fluida a las redes de Siguiente Generación.

1.3.4.2 Media Gateway (Pasarela de Medios)

Se ubican al borde del núcleo y son también conocidos como puntos de control de borde o pasarelas de red, su función principal es dar conectividad entre redes diferentes e incompatibles como la PSTN, ATM, Frame Relay y otras. Además realizan las funciones de procesamiento de voz (codificación y decodificación), cancelación de eco, manejo de jitter, generación de tonos, discriminación del tipo de tráfico y manejo de políticas de Calidad Servicio.

1.3.4.3 MTA (Multimedia Terminal Adapter)

El MTA (Adaptador de Terminal Multimedia) es un dispositivo instalado en las dependencias del cliente que permite la prestación de servicios avanzados de VoIP[19] y datos a través de una conexión de banda ancha. Es utilizado en las redes HFC[20], que es una red híbrida que combina la fibra óptica en la red primaria y el cable coaxial para las acometidas que salen de la red secundaria, típicamente es una infraestructura para televisión por cable pero el MTA es el encargado de modular la señal de datos para ofrecer a los usuarios Internet y VoIP.

Entre las funciones más importantes que realiza un MTA están la encapsulación de voz sobre IP, señalización de llamadas, Calidad de Servicio y seguridad en la transmisión bidireccional y transparente con interfaces para la conexión de líneas telefónicas analógicas (RJ-11), fax, Ethernet 10/100BaseT (RJ-45) y puertos USB[21] para la transmisión de datos con una alta velocidad.

---

[18] **MSAN** Multi-Service Access Node
[19] **VoIP** Voice over Internet Protocol
[20] **HFC** Hybrid Fiber Coaxial
[21] **USB** Universal Serial Bus

1.3.4.4 IAD (Integrated Access Device)

El IAD (Dispositivo de Acceso Integrado) permite el acceso de los usuarios a servicios integrados de voz y datos al cumplir con las funciones de un módem DSL[22] y a la vez encargándose de la conversión de las señales de voz analógicas de los usuarios para el transporte hacia la red del proveedor, proporcionando una interfaz de datos Ethernet y varias interfaces de voz (conectores RJ-11 para la PSTN).

Con un IAD el proveedor de los servicios puede controlar las características del enlace de acceso y gestionar el funcionamiento del mismo durante la conexión con los protocolos H.248 o SIP (Session Initial Protocol) a través del Softswitch y sus componentes.

1.4 ARQUITECTURA Y PROTOCOLOS

Para comprender la arquitectura y protocolos comúnmente utilizados en una red de Siguiente Generación, primeramente hay que establecer la relación existente entre el modelo NGN con las distintas capas del modelo OSI[23].

Basándose en el modelo OSI y caracterizándolo con el esquema referencial del modelo NGN se tiene:

- Física y Enlace: Nivel de Acceso del Terminal
- Red y Transporte: Borde y Núcleo de Red
- Sesión, Presentación y Aplicación: Control de Red y nivel de Gestión y Servicio.

En la figura 1.4 se presenta un esquema de red NGN por capas referenciando al modelo OSI en el que se puede apreciar los protocolos y tecnologías que intervienen para dar soporte a las aplicaciones multimedia.

---

[22] **DSL** Digital Subscriber Line
[23] **OSI** Open System Interconnection

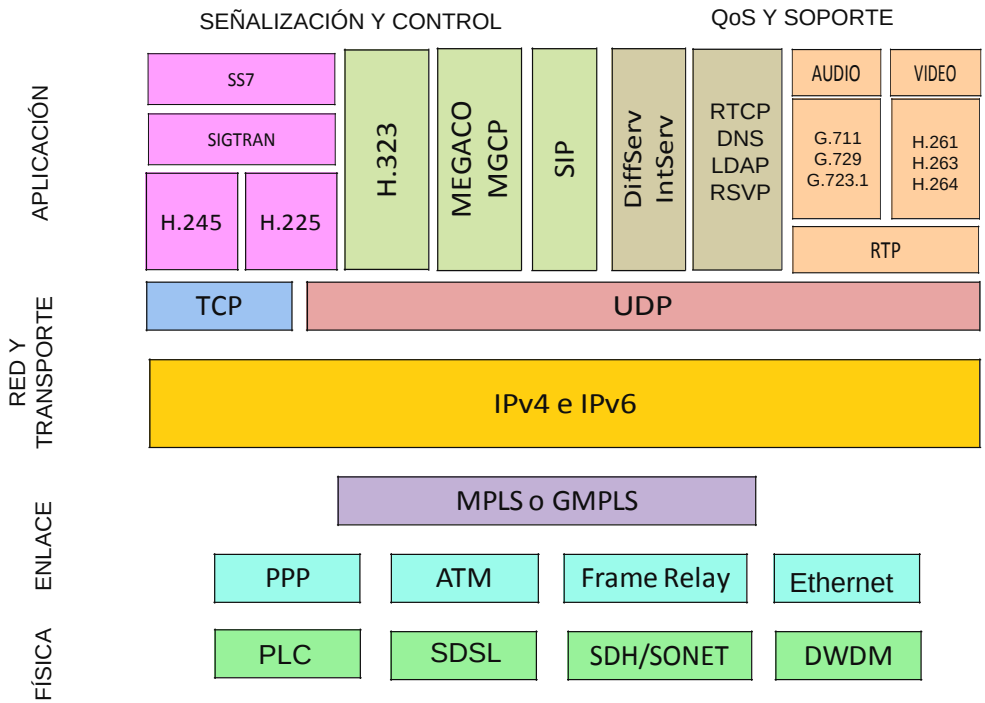


Figura 1.4 Protocolos que intervienen en el modelo de red NGN

Como se observa en la figura 1.4 dentro de una infraestructura de red NGN deben entenderse protocolos y tecnologías tanto tradicionales como nuevas para que sea posible la implementación de una red que proporcione servicios convergentes.

El despliegue en infraestructura de las tecnologías tradicionales de transporte tanto a nivel físico como de enlace (ATM, Frame Relay, SDH/SONET[24], etc.) han requerido de una gran inversión por parte de los proveedores y por tanto estas redes no pueden actualmente dejarse a un lado, por ello uno de los objetivos de las NGN es coexistir con las redes tradicionales a través de la implementación de dispositivos inteligentes en el nivel de control y con el avance tecnológico ir incorporando terminales inteligentes en la parte del acceso del usuario.

Para la integración de las redes tradicionales a nivel físico y de enlace es necesario contar con una tecnología que sea capaz de lograr este objetivo para conformar una plataforma de red

[24]**SDH/SONET** Synchronous Digital Hierarchy/Synchronous Optical Network

común. Con la implementación de MPLS[25] a nivel troncal se obtiene esta integración que proporciona flexibilidad y escalabilidad en cuanto a las aplicaciones que brinda como Ingeniería de Tráfico y Cos[26] (analizadas en el siguiente capítulo).

En la actualidad la tendencia se basa en redes de transporte a nivel de enlace soportadas sobre fibra óptica como OTN (Optical Transport Network) o DWDM[27] para este caso la tecnología adoptada para el núcleo es GMPLS[28]. Esta tecnología es una extensión de MPLS para la integración de redes de conmutación de paquetes IP con las redes ópticas, dando lugar a las redes inteligentes de Siguiente Generación asegurando la provisión de servicios Triple Play y luego Quad Play.

A nivel de red prácticamente el funcionamiento de IPv4[29] ha sido satisfactorio pero el crecimiento de Internet ha provocado la escasez de direccionamiento IP conjuntamente con la dificultad de transmitir aplicaciones en tiempo real sumada la escasez de mecanismos de seguridad, estas y otras desventajas que presenta IPv4 son resueltas con la adopción del nuevo protocolo IPv6[30], definido en la RFC[31] 1883. Esta versión puede ser instalada en el equipo del usuario como una actualización de software y de la misma manera en los equipos de red que lo soporten.

La implementación del Softswitch en el nivel de Control permite distinguir las llamadas de voz de otras aplicaciones y para llevar a cabo esta operación además de comunicarse con otros elementos lo hace por medio de protocolos. A continuación se describe de manera general los protocolos más importantes.

---

[25]**MPLS** Multiprotocol Label Switching
[26]**CoS** Class of Service
[27]**DWDM** Dense Wavelength Division Multiplexing
[28]**GMPLS** Generalized Multiprotocol Label Switching
[29]**IPv4** Internet Protocol version 4
[30]**IPV6** Internet Protocol version 6
[31]**RFC** Request for Comments

1.4.1 PROTOCOLOS DE SEÑALIZACIÓN Y DE CONTROL

Estos protocolos se requieren para establecer, mantener y liberar una conexión así como el control de los demás elementos complementarios del Softswitch, facilitando información de la presencia y ubicación de los usuarios, entre otros.

1.4.1.1 SS7

El SS7 (Sistema de Senalización 7) es un conjunto de protocolos que soportan la señalización de llamadas fuera de banda y características avanzadas de llamadas. Señaliza los circuitos conmutados de los proveedores de servicios de la PSTN permitiendo las variaciones de un país a otro. Además se encarga del establecimiento y desconexión de la llamada, consultas de las bases de datos, estado del enlace troncal y las instrucciones de conmutadores remotos. SS7 no solo permite satisfacer necesidades de voz también fue concebido para utilizarse con datos permitiendo la interconectividad con diferentes redes por ejemplo ATM, Frame Relay permitiendo una gama de servicios suplementarios mediante la separación de la señalización de la parte de conmutación de paquetes.

Algunas de las características de SS7 son las siguientes:

- Señalización estandarizada mediante un canal común.
- Flexibilidad y velocidad en el establecimiento de una llamada.
- Mejor control de las llamadas y la gestión (tasación).
- Señalización bidireccional.
- Admite cambios de información de señalización en tiempo real.
- Permite procedimientos de transmisión de datos como los métodos de detección y corrección de errores.

1.4.1.2 SIGTRAN

SIGTRAN (Signalling Transport), grupo de trabajo del IETF[32], define una arquitectura para el transporte de señalización sobre las redes IP y conjuntamente deduce mecanismos de comunicaciones para transportar mensajes SS7 sobre IP que se describen en la RFC 2719.

---

[32]**IETF** Internet Engineering Task Force

El protocolo más significativo del conjunto de protocolos SIGTRAN es el SCTP (Stream Control Transmission Protocol), descrito en la RFC 2960, que es un protocolo a nivel de transporte, una alternativa a la utilización de TCP[33] y UDP[34].

SIGTRAN es utilizado conjuntamente con MEGACO[35] para traducir la señalización telefónica en el transporte por la red IP, debido a que MEGACO no tiene señalización telefónica por canal común o SS7.

1.4.1.3 H.323

H.323 es un estándar de la UIT-T que ofrece especificaciones de componentes, protocolos y procedimientos para aplicaciones en tiempo real de voz, datos y video. Además define la señalización necesaria para las comunicaciones multimedia sobre redes IP y otras, haciéndolo más popular para las aplicaciones de VoIP. H.323 cumple con las funciones de control de llamada, uso de códecs de voz y regula las normas de otros organismos referentes a la transmisión en tiempo real de voz.

El estándar H.323 incluye también las siguientes recomendaciones:

- H.225: paquetización, sincronización y señalización.
- H.245: control del canal.
- G.711, G.722, G.723.1, G.728, G.729: codificación de audio.

La implementación de H.323 es uno de los primeros pasos para ofrecer servicios de VoIP, pero para otras aplicaciones se tienen otras alternativas como SIP o MEGACO.

1.4.1.4 MEGACO H.248

El H.248 o MEGACO es un protocolo estándar definido por la UIT-T para la gestión de sesiones y señalización. Es un complemento de los protocolos H.323 y SIP porque para

---

[33] **TCP** Transmission Control Protocol
[34] **UDP** User Datagram Protocol
[35] **MEGACO** Media Gateway Controller, nombre ITU para el H.248

controlar los Media Gateways utiliza H.323 y para la comunicación con un Softswitch o Media Gateway Controller lo hace por medio de SIP. El protocolo MEGACO permite la conmutación de llamadas de voz, fax y multimedia entre la red PSTN y las redes IP de Siguiente Generación y se originó del MGCP (Media Gateway Control Protocol), éste proporciona un control centralizado de las comunicaciones y servicios multimedia a través de redes basadas en IP.

MEGACO permite una mayor escalabilidad que el estándar H.323 y da respuesta a las necesidades técnicas y a las funciones de conferencia multimedia que se pasaron por alto en el protocolo MGCP.

El MGCP es un protocolo maestro/esclavo, donde los gateways ejecutan comandos enviados por el MGC[36] controlando de esta forma los gateways, el maestro es el MGC (Softswitch) y el esclavo es el gateway (que puede ser un gateway de VoIP, un DSLAM[37], un router MPLS o un teléfono IP).

La desventaja que presenta MGCP es que para desplegar servicios avanzados es necesario implementar otro protocolo como SIP tanto en los terminales como sobre la red de señalización, realizando las funciones de control asociadas al servicio.

1.4.1.5 SIP

SIP (Session Initial Protocol) del IETF definido en la RFC 2543 es un conjunto de protocolos que simplifican las funciones del protocolo H.323. Con el protocolo SIP se establece la iniciación, modificación y finalización de sesiones interactivas (señalización) de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos online y realidad virtual interactuando con las funciones típicas de la Red Pública Conmutada como son: llamar a un número, provocar que un teléfono suene al ser llamado, escuchar la señal de tono o de ocupado.

---

[36] **MGC** Media Gateway Controller
[37] **DSLAM** Digital Subscriber Line Access Multiplexer

Para realizar estas operaciones adopta el modelo cliente-servidor. El cliente realiza peticiones que el servidor atiende y genera una o más respuestas (dependiendo de la naturaleza de la petición). SIP además implementa muchas características del procesamiento de llamadas de SS7, siendo los dos protocolos muy diferentes. SS7 es altamente centralizado, caracterizado por una compleja arquitectura central de red y unos terminales tontos (los tradicionales teléfonos). Además es un protocolo peer to peer y como tal requiere un núcleo de red sencillo y escalable con inteligencia distribuida en los extremos de la red, incluida en los terminales (ya sea mediante hardware o software).

Para la localización del usuario la dirección usada en SIP se basa en un localizador URL[38] con un formato: nombre@192.168.132.33 o mediante un dominio: servinfo.com.ec requiriendo de un servidor de resolución de dominio DNS[39]. SIP no depende de los protocolos de las capas inferiores así que puede ser soportado sobre TCP, UDP o sobre cualquier tipo de transporte.

Para la entrega de las aplicaciones multimedia hace uso de otros protocolos como:

- RTP y RTCP que proporcionan una entrega en tiempo real (más adelante descritos)
- RTSP[40] (Protocolo de Flujo en Tiempo Real) definido en la RFC 2326, proporciona una entrega bajo demanda de datos en tiempo real.
- SDP[41] (Protocolo de Descripción de Sesión) detallado en la RFC 2327, proporciona un formato de descripción estándar para el intercambio de mecanismos para las aplicaciones como por ejemplo los códecs de voz para VoIP.

1.4.2 PROTOCOLOS DE QoS Y SOPORTE

Estos protocolos tienen la función de efectuar los mecanismos de transporte de los flujos de tráfico para el control sobre la calidad y clase de servicio en la transmisión de aplicaciones de tiempo real. A continuación se describen los más importantes.

---

[38] **URL** Uniform Resource Locator
[39] **DNS** Domain Name System
[40] **RTSP** Real Time Streaming Protocol
[41] **SDP** Session Description Protocol

1.4.2.1 RTP

RTP (Real Time Protocol), desarrollado por el IETF, define las funciones de transporte de extremo a extremo para la transmisión en tiempo real de aplicaciones de audio y video a través de Internet e incluye mecanismos de control para la sincronización de los flujos de tráfico mediante el marcado con números de secuencia de paquetes IP para la reconstrucción de la información de voz y video.

Las funcionalidades que realiza son las siguientes:

- Identificación del tipo de información transmitida.
- Control de la llegada de los paquetes a su destino.
- Funcionamiento sobre UDP o TCP.
- Los paquetes de difusión múltiple pueden usar RTP para encaminar las conversaciones a múltiples destinatarios.
- Utiliza un registro de tiempo para ajustar los intervalos de muestreo de acuerdo a la secuencia original.
- RTP es un protocolo de sesión, pero se encuentra en el nivel de aplicación, siendo el desarrollador el que lo tiene que integrar.

Para la codificación y compresión de las señales de tiempo real se requiere de CODECS de audio y video estandarizados tales como G.711, G.729, etc. (audio) y para video H.261, H.263, H.264 entre otros.

1.4.2.2 RTCP

RTCP (Real Time Control Protocol) es un protocolo de control que funciona con RTP, se basa fundamentalmente en la transmisión periódica de paquetes de control de los miembros de una sesión en aplicaciones de voz o video en tiempo real, siendo RTCP el mecanismo para enviar información de control periódicamente entre el emisor y receptor durante una conexión.

Las funciones principales son:

- Los paquetes RTCP contienen datos que ayudan a verificar las condiciones de transmisión en el extremo remoto.
- RTCP está diseñado para ser independiente de la capa de transporte (TCP o UDP) pero generalmente se lleva a cabo por encima de UDP.

1.4.2.3 RSVP

RSVP (Resource Reservation Protocol) es un protocolo que permite ofrecer Calidad de Servicio sobre aplicaciones en tiempo real en redes IP mediante la reserva de recursos en los routers intermedios para asegurar un ancho de banda en la transmisión.

Para la implementación de RSVP los routers deben utilizar los siguientes elementos:

- Admission Control: que comprueba si la red dispone de los recursos suficientes.
- Policy Control: para comprobar los permisos de los usuarios.
- Packet Classifier: clasificación de los paquetes de acuerdo al QoS al que pertenecen.
- Packet Scheduler: organiza el envío de los paquetes dentro de cada clasificación

En RSVP un flujo de datos se considera una secuencia de paquetes que tienen un mismo origen, uno o más destinos y una Calidad de Servicio, son manejados independientemente, una vez implementado RSVP los routers establecen y mantienen las rutas requeridas con el QoS necesario.

La información que proporciona RSVP es la siguiente:

- De control: para tratar correctamente al paquete, versión del protocolo, tiempo de vida, tamaño del paquete completo, identificador del mensaje, entre otros.

- Información de la reserva de recursos como: dirección IP y puerto destino, dirección IP del router con RSVP que envía el mensaje, especificación de QoS y otros.

Algunas de las características de este protocolo son:

- RSVP puede trabajar con IPv4 como en la versión 6, siendo la última mejor dotada para la reserva de recursos.
- La reserva de recursos es realizada por flujo.
- RSVP es un protocolo de Señalización.
- RSVP debe mantener los requerimientos de reserva en cada router utilizando un conjunto de mensajes de señalización.
- En RSVP los datos de usuarios son transportados una vez realizado el proceso de señalización.

1.4.2.4 LDAP

LDAP (Lightweight Directory Access Protocol) es un protocolo de Internet a nivel de aplicación que los programas de correo electrónico y otros utilizan para buscar información en un servidor de directorio, permitiendo administrar directorios al acceder a bases de información generalmente de usuarios de una red mediante protocolos TCP/IP[42].

El directorio es similar a una base de datos que contiene la información estructurada a manera de un árbol sobre el personal y hardware de una empresa ya sea a nivel local, nacional inclusive mundial. La información comúnmente almacenada es de login (usuario y contraseña), utilizada para la autenticación pero es posible almacenar otro tipo de información como datos del contacto, permisos, certificados y ubicación de los recursos de la red (si es un directorio de hardware); por ejemplo si dentro de una red se ofrece VoIP el protocolo LDAP es el que relaciona las direcciones IP con los números telefónicos.

---

[42]**TCP/IP** Conjunto de protocolos de red en los que se basa Internet

1.4.2.5 IntServ

IntServ (Integrated Services) o modelo de Servicios Integrados, utiliza RSVP para ofrecer QoS a redes IP con el objetivo de solicitar previamente los recursos de red, que son tomados en cada router de trayecto, siempre y cuando se disponga de los recursos necesarios. El modelo de Servicios Integrados incluye los servicios de mejor esfuerzo, tiempo real y compartición controlada de los enlaces mediante la reserva de los recursos en cada sesión siendo los paquetes de datos revisados para asignarles la reserva de recursos correspondiente.

Este modelo se desarrolló en base a los requerimientos emergentes de los proveedores de redes para mejorar la administración de los recursos de la red como el ancho de banda con una arquitectura del mejor esfuerzo dando la idea de que los recursos pueden ser gestionados como un punto clave que determina la Calidad de Servicio. Sin embargo las desventajas que presenta este modelo surgen en base al mantenimiento de la información de cada flujo de tráfico generada en cada router de la red provocando un overhead por paquete inaceptable por cuestiones de chequeos y administración de los recursos, afectando al núcleo de la red, además de que todos los routers deben soportar RSVP.

1.4.2.6 DiffServ

DiffServ (Differentiated Services) o modelo de Servicios Diferenciados del IETF proporciona Calidad de Servicio e intenta evitar los problemas encontrados en IntServ, únicamente se encarga del marcado del paquete mas no en la reserva de recursos como en el anterior modelo, también este modelo elimina la información sobre cada flujo de tráfico de los routers evitando la congestión en el core de la red ya que el marcado de los paquetes se realiza solo en los nodos del borde.

DiffServ se basa en la división del tráfico en diferentes clases mediante la asignación de una cabecera DSCP[43] a los paquetes para distinguirlos, clasificarlos y darles el tratamiento necesario con un código específico que indica el comportamiento de los paquetes, esta cabecera es compatible con IPv4 e IPv6. En la figura 1.5 se muestra la clasificación de los paquetes y la priorización ofrecida dependiendo de su clase.

---

[43] **DSCP** Differentiated Services Code Point

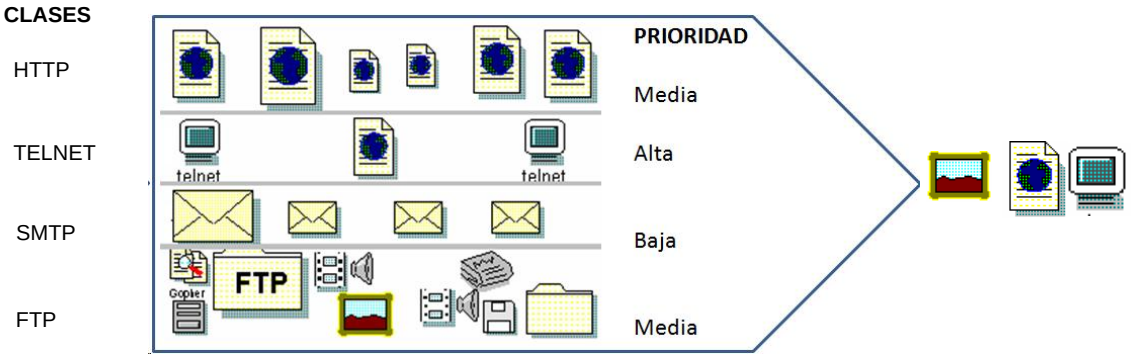


Figura 1.5 División del tráfico por clases

Con la implementación del DiffServ en una red, el usuario también puede acordar con su proveedor el nivel de servicio que requiere para las aplicaciones contratadas por medio del SLA[44], fijando en este contrato las características y parámetros que espera de su servicio.

1.5 CONSIDERACIONES GENERALES PARA LA MIGRACIÓN

Con la aparición de nuevos y novedosos servicios multimedia los operadores de redes se vieron en la obligación de mejorar sus infraestructuras con el objeto de brindar a los usuarios la posibilidad de contar con toda una gama de servicios interactivos. De esta manera comienza la búsqueda de mejores soluciones que integren diversas plataformas y servicios produciéndose una evolución tecnológica en las redes de datos.

El reto de los proveedores hoy en día es permanecer en el mercado de las Telecomunicaciones y para esto tienen que adaptar sus redes a las necesidades de los usuarios e incorporar nuevas soluciones tecnológicas. La migración a NGN (Next Generation Network) consiste en pasar de las redes tradicionales de voz o datos a una sola infraestructura de red paulatinamente, pero la preocupación de los proveedores es cómo hacerlo minimizando costos y aprovechar a lo máximo la nueva infraestructura, la estrategia depende de la red desplegada actualmente, los requerimientos de los usuarios y los planes de expansión.

---

[44]**SLA** Service Level Agreement

A continuación se describe un esquema general del procedimiento que deben seguir las empresas de Telecomunicaciones para incorporar una infraestructura NGN en sus redes.

1.5.1 IMPLEMENTACIÓN EN EL CORE

Lo primero que se realiza para la migración de las redes es la implementación y fortalecimiento del core a nivel de software y hardware incorporando dispositivos de enrutamiento y de conmutación capa 3 para el soporte de nuevas tecnologías como MPLS (Multiprotocol Label Switching) para ofrecer los servicios tradicionales con Calidad de Servicio y la posibilidad de aplicar técnicas de Ingeniería de Tráfico. Con la utilización de MPLS la infraestructura actual del proveedor a nivel de core se convierte en una troncal que a futuro permitirá la conectividad con diferentes redes de acceso y transporte.

1.5.2 INCORPORACIÓN DEL SOFTSWITCH Y ELEMENTOS DE CONTROL

Con la implementación del Softswitch como dispositivo de control de sesiones de llamada y para el suministro de aplicaciones multimedia el operador puede ya garantizar a sus usuarios la oferta de servicios de voz, datos o una combinación de servicios multimedia y enfocarse al desarrollo de nuevas y novedosas aplicaciones. Además del Softswitch se tiene que incorporar un Signalling Gateway para la señalización de servicios de voz con la finalidad de integrar la red del proveedor con la Red Telefónica Tradicional.

Es muy importante también tomar una decisión acertada en cuanto a la elección del protocolo de operación. Actualmente para el soporte de aplicaciones de voz y video en redes IP, el estándar H.323 ha ganado espacio pero hay aspectos que no hacen favorable su utilización como la ausencia de una interfaz de red a red y un mecanismo de control de gestión por lo que las mejores opciones son SIP o MEGACO, este último con mayor razón por que define las funcionalidades y características de los elementos complementarios del Softswitch (Signalling Gateway, Media Gateway, Access Gateway y otros).

A la par con la implementación en el nivel de Control y dependiendo de la infraestructura del proveedor se deben incorporar dispositivos de borde y de acceso para la interacción con los usuarios. Por ejemplo un tipo de Media Gateway para troncales TDM, en el caso de redes

HFC (Hybrid Fiber Coaxial) para el acceso de los usuarios se debe utilizar un MTA (Multimedia Terminal Adapter) y para las redes ATM el tradicional DSL o un IAD (Integrated Access Device).

1.5.3 INTEGRACIÓN DEL ACCESO WIMAX Y WIFI

Una vez que la red del proveedor garantice la provisión servicios de voz y datos, el siguiente paso es la integración del acceso fijo y móvil a través de la unificación o implementación de tecnologías de acceso inalámbrico como WIMAX[45] y WIFI[46] con la finalidad de integrar los servicios celulares con los servicios de banda ancha.

WIMAX en el contexto NGN (Next Generation Network) sobresale por su interoperabilidad mundial para el acceso por microondas y está basado en estándares que potencializan la banda ancha inalámbrica. Para la implementación de WIMAX no es necesario realizar cambios en toda la red ya que los componentes se pueden incorporar directamente a la infraestructura actual del proveedor lo que además representa menos gastos, de esta manera ofreciendo a los usuarios servicios móviles y una propuesta de banda ancha inalámbrica fija e ir migrando a banda ancha móvil a medida que crece la demanda. Con esta implementación se integra los servicios móviles y dando la opción al proveedor de ofrecer banda ancha a sectores rurales o alejados donde un sistema cableado es muy costoso.

Para esta unificación es necesario la adquisición de:

1. **BTS (Base Transceiver Station)**
   Para el acceso por radio, es una instalación fija con equipos transmisores y receptores para la comunicación bidireccional dando conectividad a los usuarios finales.

2. **ASN GATEWAY (Access Service Network - Gateway)**
   Realiza una serie de funciones críticas ya que es la interfaz con las estaciones del suscriptor y el elemento central de la red (core), permite el control de movilidad, voz, autentificación y distribución de claves de seguridad.

---

[45] **WIMAX** Worldwide Interoperability for Microwave Access
[46] **WIFI** Wireless Fidelity

3. **ELEMENTO DE ADMINISTRACIÓN DE RED**

   Para el control de los elementos WIMAX.

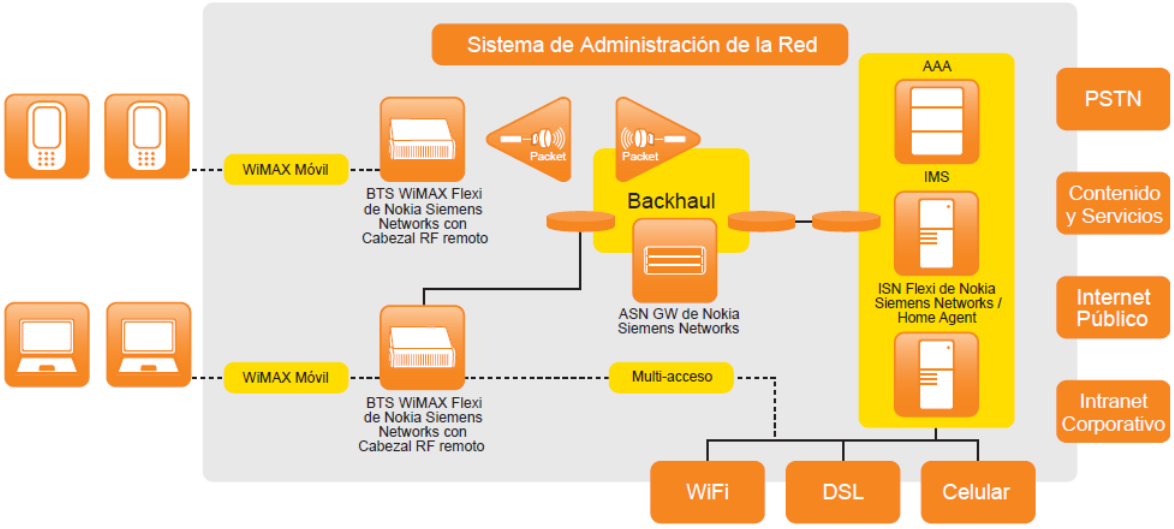
4. **SERVIDOR AAA**[47]

   Para la autenticación, autorización y facturación de los equipos del usuario.

5. **HOME AGENT**

   Elemento adicional que brinda interfaces entre la red WIMAX y otras redes y servicios IP como DSL, WIFI y celular.

En la figura 1.6 se presenta un esquema de implementación de WIMAX en un entorno en el que el proveedor integra el servicio móvil con los servicios de banda ancha.



Fuente: http://www.sec-nokiasiemensnetworks.com

Figura 1.6 WIMAX en la integración de acceso móvil y banda ancha

[47] **AAA** Authentication Authorization Accounting

1.5.4 AGREGACIÓN DE LA PLATAFORMA DE VIDEO Y CONTENIDO

Para implementar servicios de IPTV[48] es necesario agregar una plataforma de video y contenido en el nivel de Gestión y Servicio de la red para brindar a los usuarios una programación por demanda y otras opciones personalizadas e interactivas por medio de una conexión banda ancha y un dispositivo que permita enviar y recibir los requerimientos hacia el proveedor, así un usuario puede por ejemplo ver una película simultáneamente con otros usuarios separados geográficamente al mismo tiempo en que pueden intercambiar archivos y tener una sesión de chat.

Las ventajas de los servicios de IPTV frente a la televisión tradicional son las siguientes:

- **Video bajo Demanda:** el usuario elige la película o programa a la hora que desea.

- **Mayor Contenido:** además de los canales se cuenta con una gama de películas y programas que aloja el proveedor en sus servidores.

- **Comodidad:** con el servicio de video bajo demanda el usuario puede disfrutar del contenido las veces que desee y manipular las películas o programas a su manera.

- **Publicidad personalizada:** por el sentido bidireccional de la transmisión los usuarios seleccionan las áreas de su interés para recibir ofertas de publicidad.

- **Servicios de valor añadido:** mediante un televisor se tiene acceso a todo tipo de información como navegador, correo electrónico, etc.

La plataforma de video y contenido es un conjunto de elementos encargados de recibir señales en vivo provistas vía satélite o de fuentes de contenidos locales para convertirlas y encapsularlas al formato necesario para la transmisión por la red, en la figura 1.7 se muestran los elementos que se deben añadir al nivel de Gestión y Servicio para el soporte de aplicaciones de video y contenido hacia los usuarios.

---

[48] **IPTV** Internet Protocol Television

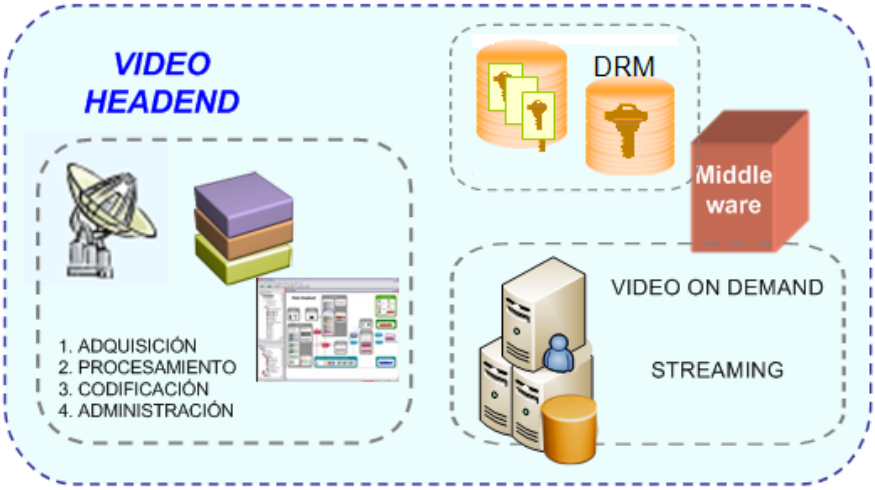


Figura 1.7 Plataforma de Video y Contenido

A continuación se describen los elementos necesarios y un esquema de implementación de los mismos en la red del proveedor:

1. **CAPTURA DE LAS SEÑALES DE VIDEO (HEADEND)**

   Se recopila el contenido para integrar la oferta de programación y se lo puede recibir de un proveedor de contenidos o de un distribuidor de señales digital o analógica. Para adecuar la señal al formato o códec de video se requiere de codificadores para transmitir el flujo de video por la red. El codificador es un dispositivo o módulo de software que permite la compresión del video sin pérdidas. En la implementación también el proveedor debe elegir acertadamente el códec porque determina el balance entre la calidad de video, cantidad de datos para representarla (tasa de bits), la complejidad de los algoritmos de codificación y decodificación, robustez ante las pérdidas de datos y los errores, retraso por transmisión entre otros que determinan la calidad.

2. **ALMACENAMIENTO Y SERVIDORES DE VIDEO**

   Los servidores tienen algunas funciones como el almacenamiento y respaldo de los contenidos, administración del video bajo demanda y streaming. También es necesario

de un servidor DRM[49] o servidor de licencias, que administra los permisos para desbloquear los contenidos, autorización y reporte de transacciones para los usuarios, teniendo los proveedores de Telecomunicaciones los derechos de distribución de canales y programación VoD[50].

3. MIDDLEWARE

Dependiendo de la elección del proveedor el Middleware puede ser un equipo, software o una combinación de los dos que interconecta a un cliente con una base de datos para la distribución de los servicios brindando al usuario una interfaz gráfica y amigable con la guía de la programación disponible por el proveedor, ofertas de servicios y administración de la interacción con el usuario además de algún sistema de protección de derechos para evitar las copias digitales. En la figura 1.8 se muestra una interfaz gráfica con la programación disponible.

Fuente: http://www.arantia.com/iptv.shtml

Figura 1.8 Interfaz gráfica de una aplicación Middleware

4. DISTRIBUCIÓN DEL CONTENIDO

Distribución de las señales a través de la red de transporte con capacidad de transmisión bidireccional del contenido y debe soportar tasas de transmisión estables con Calidad de Servicio. El proveedor puede distribuir el contenido de dos maneras ya sea unicast (un contenido a un destino) o multicast (un contenido a varios destinos).

---

[49] **DRM** Digital Rights Management
[50] **VoD** Video on Demand

5. **EQUIPO DE ACCESO Y DE USUARIO**

   Para la entrega del servicio y la visualización del usuario en el terminal (televisor) se requiere de un equipo receptor o decodificador conocido como STB (Set-Top Box), que convierte los flujos de video en señales analógicas o digitales.

1.5.5 IP MULTIMEDIA SUBSYSTEM

El IMS de 3GPP[51] fue adoptado por la UIT-T y su propósito es servir de apoyo a la red NGN en el desarrollo y distribución de servicios avanzados con un sistema inteligente de gestión proporcionando control excelente sobre las aplicaciones del usuario mediante la tasación, facturación y seguridad.

Las funcionalidades más importantes que ofrece el IMS son:

- Sistema de tarifación común y flexible para todos los servicios.
- Gestión de usuario única.
- Gestión de los servicios única.
- Gestión de identidad única.
- Sistema de identificación y autorización único.

A través de este sistema los usuarios cuentan con un servicio de ventanilla única en la que mediante una planilla se puede cancelar por todos los servicios prestados por su respectivo operador, utilizando mecanismos para la tarifación en tiempo real de los servicios que el usuario demanda a la red. Los servicios están basados en SIP, facilitando la convergencia de accesos móviles y fijos ya que es utilizado por el IMS para el control de sesiones y servicios por medio de una URL SIP hacia cada participante de una sesión.

Entonces desplegar una arquitectura IMS es una decisión estratégica que debe tomar el proveedor para posicionarse por completo en el mercado de las Telecomunicaciones abriendo camino hacia la prestación de servicios Quad-Play. En la figura 1.9 se muestra el equipamiento necesario para la implementación del IMS a la infraestructura de red NGN.

---

[51] **3GPP** 3rd Generation Partnership Project

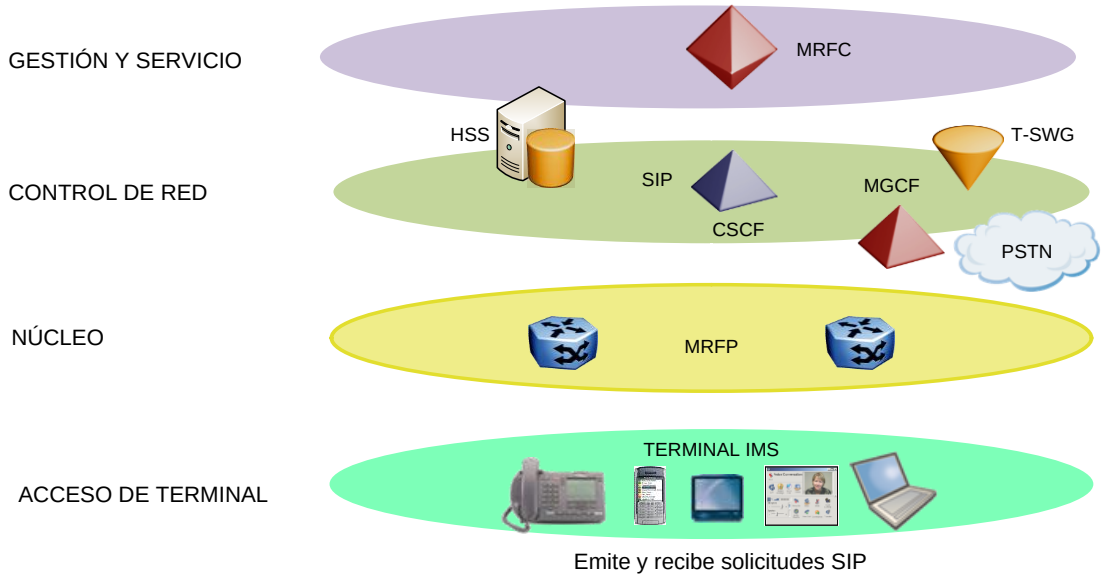


Figura 1.9 Implementación del IMS en los niveles jerárquicos de una red NGN

Como se observa en la figura 1.9 para la total convergencia de servicios fijos y móviles con el objeto de brindar diversas aplicaciones bajo un control inteligente es necesario incorporar a la red NGN el IMS, para lo cual se debe considerar la integración de equipamiento en los diferentes niveles:

a. Gestión y Servicio

Para el control de los servidores de los servicios multimedia es necesario agregar el MRFC (Multimedia Resource Function Controller) o Controlador de Funciones de los Recursos Multimedia, esta entidad gestiona y administra a los servicios inteligentes.

b. Control de red

Está formado básicamente por tres elementos: HSS[52], CSCF[53] y MGCF[54].

---

[52]**HSS** Home Subscribe Server
[53]**CSCF** Call Session Control Function
[54]**MGCF** Media Gateway Control Function

- HSS: es el servidor con la información dinámica de los usuarios y sus perfiles que permite ingresar a los servicios después de la autorización y autenticación.

- CSCF: es el elemento más importante del IMS, brinda las capacidades de control de todas las sesiones multimedia utilizando como protocolo de señalización a SIP (Session Initial Protocol). Según sus funciones puede ser: Proxy-CSCF (interfaz de acceso), Interrogating-CSCF (mediación) y Serving-CSCF (control de sesiones).

- MGCF: un Media Gateway que permite la interacción con la red tradicional PSTN. Los usuarios bajo aplicaciones SIP pueden realizar o recibir llamadas desde este tipo de red. Conjuntamente utiliza el T-SGW (para la señalización y puede ser el mismo Signalling Gateway de la red NGN del proveedor).

c. Núcleo

Las mismas características que una red NGN en los primeros inicios ratificando el protocolo MPLS como protocolo base para brindar Calidad de Servicio y DiffServ.

d. Acceso de terminal

Los terminales deben basarse en aplicaciones que corran sobre dispositivos (Pc, teléfonos IP, móviles, etc.) los cuales emiten y reciben solicitudes SIP. Estos dispositivos ya no son terminales tontos.

Al incorporar los elementos del IMS por niveles se está garantizando que la red no está sujeta a cambios agresivos solo son implementaciones que harán de la red del proveedor más inteligente por los servicios y la gestión. Como se observa en la Figura 1.9 la arquitectura del IMS es casi idéntica a la de una red NGN por lo que perfectamente encajan y se complementan para así tener una verdadera convergencia en todos los niveles.

CAPÍTULO 2. ESTUDIO DE LA TECNOLOGÍA MPLS

2.1 ANTECEDENTES DE MPLS

La demanda de los usuarios de nuevos servicios y la necesidad del aumento de ancho de banda impulsó en un inicio a los proveedores de servicios de Telecomunicaciones a desplegar en sus infraestructuras una combinación de enrutadores IP con conmutadores ATM/Frame Relay, una vez consolidada la tecnología TCP/IP, esta combinación propiciaba un equilibrio frente a las necesidades de crecimiento de la época.

Este modelo de red adoptado presentó limitaciones de interoperabilidad con otras redes, dificultad de gestionar estas conexiones y un alto crecimiento en equipamiento. Para suplir estas necesidades a mediados de la década de los 90 empezaron a aparecer soluciones de conmutación de nivel 2 diseñadas con la idea de tomar el software de control de un router con el objeto de integrar el rendimiento de reenvío con el cambio de etiqueta de un switch ATM para crear un router extremadamente rápido y eficiente.

Tras establecerse el grupo de trabajo MPLS del IETF en 1998 se definió un estándar para unificar las soluciones que presentaron algunos fabricantes conocido también como MPLS y recogido en la RFC 3031. Actualmente es una tecnología que para el operador representa la factibilidad de poder ofrecer a sus usuarios servicios multimedia desde una plataforma de red común y basada en cualquier tecnología de transporte a nivel físico y de enlace como por ejemplo: ATM, Frame Relay, SDH/SONET o la tendencia actual DWDM y otras, garantizando transparencia y Calidad de Servicio gracias al manejo de dos planos uno para enrutamiento y otro para la conmutación de etiquetas a nivel local dentro de la red.

2.2 DEFINICIÓN GENERAL DE MPLS

MPLS es una tecnología que combina las funciones de enrutamiento de capa 3 con las funciones de envío de capa 2, por esta razón se lo denomina Multiprotocolo ya que brinda la posibilidad de trabajar con cualquier tecnología de transporte ya sea a nivel de enlace o físico y con aplicaciones que están sobre el nivel de red. La Conmutación de etiquetas (Label

Switching) permite identificar una clasificación de tráfico, encaminando a esta clasificación por un determinado camino virtual brindando QoS y otras ventajas que serán descritas a lo largo del presente capítulo.

2.2.1 VENTAJAS DE MPLS FRENTE A TECNOLOGÍAS ANTERIORES

MPLS surgió como un estándar emergente para agrupar distintas soluciones de conmutación multinivel presentadas por los diferentes fabricantes, fomentando una tecnología abierta apta para el soporte de otras tecnologías de enlace conocidas hasta el momento.

Un modelo que se impuso con anterioridad fue el IP/ATM, que al inicio satisfacía los requisitos de las nuevas aplicaciones ya que utilizaba el encaminamiento inteligente de nivel 3 de los routers IP basándose en la alta velocidad de los conmutadores de nivel 2 y los circuitos permanentes virtuales de los switches ATM en la red troncal. Sin embargo esta integración presentó ciertas limitaciones debido a la dificultad de operar e integrar una red basada en dos tecnologías diferentes concebidas para finalidades distintas como son:

- Problemas en la separación de las funciones de ruteo con las funciones de conmutación.

- Complejidad en la gestión de dos redes separadas y tecnológicamente diferentes, una infraestructura de topología real de conmutadores ATM sobre una red lógica IP lo que conduce a mayores costos en la gestión de las redes.

- Por el tamaño pequeño de la celda (53 bytes) para la transmisión representa un overhead del 20%, ya que por cada celda enviada se tiene que analizar la cabecera (identificación de canal, detección de errores, etc) lo que podría ser utilizado por la carga útil, en consecuencia se reduce en este mismo porcentaje el ancho de banda disponible.

- Al contar con una solución basada en dos tecnologías que necesita crecer conforme a la demanda de los usuarios representa para los operadores de redes costos significativos en el mantenimiento.

- Problemas de interoperabilidad de los productos de diferentes fabricantes.

Esta última se dio debido a que los fabricantes decidieron buscar soluciones a estos inconvenientes por su propia cuenta para el mejoramiento de este modelo de red.

Las técnicas que se desarrollaron previas a la estandarización de MPLS fueron:

- IP Switching de Ipsilon Networks
- Tag Switching de Cisco
- Aggregate Route-Base IP Switching (ARIS) de IBM
- IP Navigator de Cascade/Ascend/Lucent
- Cell Switching Router (CSR) de Toshiba

Estas soluciones contribuyeron de manera significativa al desarrollo de MPLS como un estándar del IETF y por tanto son consideradas como un valioso aporte a esta tecnología.

2.2.2 CARACTERÍSTICAS

A continuación se describen las características más importantes de la tecnología MPLS:

- Fue diseñada para operar sobre cualquier tecnología de transporte a nivel de enlace, no solamente ATM, facilitando la migración a las Redes de Próxima Generación.

- MPLS es una tecnología que combina eficazmente las funciones de control de ruteo con la simplicidad y rapidez de la conmutación de nivel 2.

- La implementación de MPLS permite a una red ser más sencilla de operar, mayor escalabilidad e interoperabilidad debido al soporte de diversas tecnologías bajo una plataforma común que permite a los operadores ofrecer variados servicios dependiendo de los requerimientos de los usuarios con Calidad de Servicio o con el modelo de Servicios Diferenciados del IETF.

- Utiliza protocolos para el intercambio y distribución de etiquetas que permite la creación de caminos virtuales conocidos como LSP (Label Switched Path) que se crean dependiendo de la clasificación del flujo de tráfico que cursa la red.

- Al ser un estándar abierto, también para la distribución de etiquetas utiliza protocolos abiertos.

- MPLS permite aplicar técnicas de Ingeniería de Tráfico para encontrar la mejor ruta no necesariamente la más corta en algunos casos, pero que garantiza la llegada de los flujos de tráfico evitando cuellos de botella y caída de los enlaces.

2.2.3 IMPORTANCIA DE MPLS EN TRIPLE PLAY

La implementación de MPLS en el núcleo de la red para el transporte de distinto tráfico de extremo a extremo ofrece muchas ventajas en términos de simplificación de la infraestructura ya que soporta cualquier tecnología a nivel físico y enlace sin necesidad de adoptar por completo una nueva infraestructura de red para cada servicio lo que representa para los operadores abaratamiento en costos de implementación y mantenimiento.

De igual manera el acceso de los usuarios al Triple Play también se facilita ya que se utiliza un solo medio de transmisión ya sea par trenzado, fibra óptica, cobre o radiofrecuencia lo que permite además al proveedor el monitoreo y gestión del tráfico cursado hacia los clientes. En la figura 2.1 se puede apreciar la unificación de los servicios de voz, datos y video a través de un solo medio de transmisión.

Figura 2.1 Triple Play

2.3 ELEMENTOS BÁSICOS DE MPLS

Los elementos más comunes y fundamentales para la comprensión de MPLS son los siguientes:

- LER, Label Edge Router (Ruteador Etiquetador de Borde)
- LSR, Label Switching Router (Ruteador de Conmutación de Etiquetas)
- LSP, Label Switched Path (Ruta Conmutada de Etiquetas)
- FEC, Forward Equivalence Class (Clase Equivalente de Envío)
- LIB, Label Information Base (Base de Información de Etiquetas)
- LDP, Label Distribution Protocol (Protocolo de Distribución de Etiquetas)

En la figura 2.2 se presenta una red básica con MPLS en la que se indican los ruteadores de borde LER, y el ruteador de conmutación de etiquetas LSR dentro de un dominio MPLS.

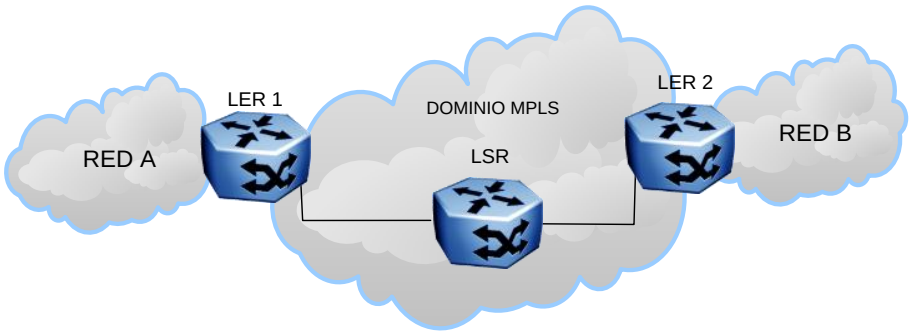


Figura 2.2 Red básica MPLS

Como se observa en la figura 2.2 una red MPLS está constituida por dispositivos capa 3 que soportan MPLS y son los LER y los LSR, básicamente con las mismas características físicas, la diferencia radica en el modo de trabajo configurado por el administrador. Además al igual que los routers IP convencionales intercambian información sobre la topología de la red mediante los protocolos de enrutamiento como: OSPF[55], BGP[56], IS-IS[57] entre otros y son capaces de manejar tablas de envío, estas últimas para la conmutación local de las etiquetas en el dominio MPLS.

2.3.1 LABEL EDGE ROUTER (LER)

Los LER se encuentran ubicados en el borde de la red MPLS y desempeñan las funciones de encaminamiento tanto para un dominio MPLS como para un dominio no MPLS (otras redes). El propósito de los LER es el análisis y clasificación del paquete IP que entra a la red de acuerdo a criterios (que se explican posteriormente), a esta clasificación por conjuntos de paquetes se le denomina FEC[58]. Una vez analizado el paquete IP se añade una cabecera MPLS y en uno de sus campos denominado Etiqueta se le asigna un valor de acuerdo a su clasificación FEC.

Al salir del dominio MPLS el LER de salida es el que direcciona el paquete a la red de destino por enrutamiento convencional eliminando la cabecera MPLS. El LER de ingreso a la red o dominio MPLS también se lo conoce como Ingress LSR y el LER de salida se lo llama Egress LSR.

2.3.2 LABEL SWITCHING ROUTER (LSR)

El LSR se encuentra ubicado en el núcleo de la red MPLS, realiza encaminamiento basándose en la conmutación de etiquetas. Una vez que le llega un paquete a una de sus interfaces éste lee la etiqueta de entrada en la cabecera MPLS y busca en la tabla de conmutación la etiqueta y la interfaz de salida para designar la nueva etiqueta que indica el siguiente salto dentro del dominio y finalmente reenvía el paquete por el camino ya designado en el LER (según el FEC).

---

[55]**OSPF** Open Shortest Path First
[56]**BGP** Border Gateway Protocol
[57]**IS-IS** Intermediate System to Intermediate System
[58]**FEC** Forward Equivalence Class

La conmutación es muy rápida ya que los LSR solo se encargan de la lectura e intercambio de etiquetas obviando la lectura de las cabeceras IP de los paquetes pero es posible que los LSR sean los que retiran la cabecera MPLS en el penúltimo salto antes de salir el paquete por un LER, este hecho puede suceder cuando en un dominio MPLS hay mucho tráfico y resulta mayor procesamiento para el LER, este mecanismo se denomina "remoción en el penúltimo salto" su siglas en inglés PHP[59].

2.3.3 FORWARD EQUIVALENCE CLASS (FEC)

El FEC es un conjunto de paquetes que son reenviados sobre un mismo camino a través de la red (LSP) y se determina una vez a la entrada a la red MPLS en un router LER. Para clasificar a los paquetes dentro de un mismo FEC se lo hace en base a criterios como:

- Dirección IP de origen, destino o direcciones IP de la red.
- Número de puerto de origen o destino
- Campo protocolo de IP (TCP, UDP, ICMP[60], etc.)
- Valor del campo DSCP de DiffServ
- Etiqueta de flujo en IPv6

Cada FEC tiene QoS debido a que se debe tratar a los paquetes que van por el mismo camino de diferente manera, dando prioridad según la necesidad de manera que se utilizan los recursos de la red óptimamente.

2.3.3.1 Agregación

La Agregación es un mecanismo que permite agrupar varios FEC mediante la asignación de una sola etiqueta para todos, de esta manera se reduce el tiempo de envío de los FEC porque se elimina asociaciones etiqueta/FEC redundantes.

Puede ser posible la Agregación cuando a un LSR le llegan desde un mismo LER varios FEC con el mismo origen y destino dentro de la red MPLS asignados al mismo camino LSP.

---

[59] **PHP** Penultimate Hop Popping
[60] **ICMP** Internet Control Message Protocol

En la figura 2.3 se puede observar que para tres FEC hay tres asociaciones etiqueta/FEC sin la utilización de la Agregación, pero al utilizarla, el FEC se convierte en un conjunto de otros FEC con características comunes teniendo así una sola asociación etiqueta/FEC.

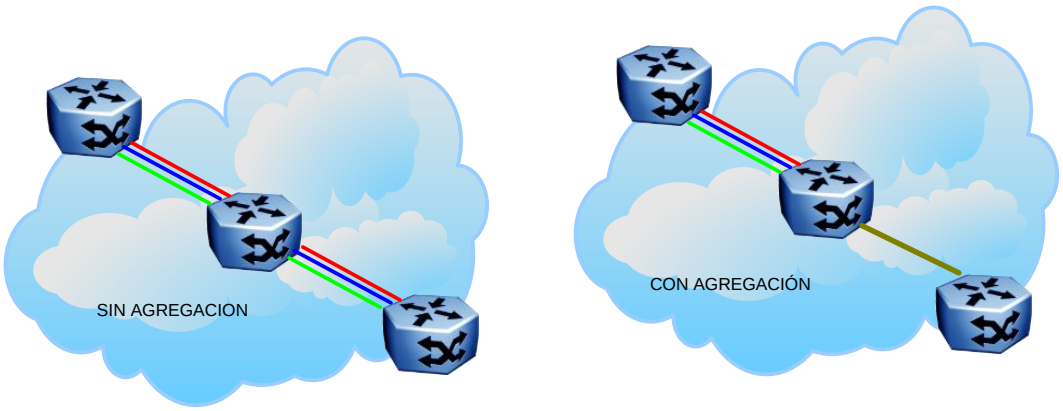


Figura 2.3 FEC sin Agregación y con Agregación

2.3.4 LABEL DISTRIBUTION PROTOCOL (LDP)

El LDP define los mecanismos para la distribución de etiquetas, permite a los LSR descubrirse e intercambiar información sobre las asociaciones FEC/Etiqueta que se han realizado y sobre todo para mantener la coherencia de las etiquetas utilizadas para los distintos tipos de tráfico que conmutan. Con este protocolo se evita que a un LSR le llegue tráfico con una etiqueta que no se encuentra en su tabla, con esto se asegura la rapidez en la conmutación de los LSR.

Para establecer la ruta LSP (Label Switched Path) los LER/LSR establecen sesiones a través de mensajes en los cuales se solicita:

- A su vecino que le informe sobre que etiqueta debe usar para el envío del tráfico por una determinada interfaz, es decir que la distribución de etiquetas se realiza contraria al camino que sigue el tráfico.

- Un LER/LSR informa de las asociaciones Etiqueta/FEC a sus vecinos que las almacenan en sus tablas sin haber solicitado la información, este mecanismo es más

eficaz ya que así todos los vecinos LER/LSR mantienen las tablas actualizadas (del mismo LSP) y haciendo el proceso de conmutación de etiquetas mucho más rápido pero incrementando el tráfico de control.

MPLS asume algunos Protocolos de Distribución de Etiquetas estandarizados como: RSVP del Modelo de Servicios Integrados de IETF, TDP (Tag Distribution Protocol) de Cisco o CR-LDP (Constrained Routing LDP), siendo el primero el más común.

2.3.5 LABEL SWITCHED PATH (LSP)

El LSP es una ruta de tráfico específica a través de la red MPLS que sigue un grupo de paquetes que pertenecen al mismo FEC. Esta ruta se crea concatenando los saltos que dan los paquetes para el intercambio de etiquetas en los LSR y para esto utiliza mensajes LDP. Los mensajes utilizados por los LSR son los siguientes:

- Descubrimiento: mediante mensajes *"hello"* de un LSR a otro LSR.
- Sesión: dos LSR establecen y mantienen la comunicación.
- Anuncio: para dar a conocer a otro LSR de las asociaciones FEC/Etiqueta.
- Notificación: información de eventos y errores

Las rutas LSP se forman desde el destino hacia el origen debido a que el LSR de origen genera las peticiones para crear un nuevo LSP mientras que el destino responde a estas solicitudes formándose de esta manera el LSP hasta el origen. Existen dos métodos para el establecimiento de los LSPs:

1. Ruta explícita:

   A partir del primer LSR de salto se construye una lista de saltos específica utilizando los protocolos de señalización o de distribución de etiquetas (RSVP, LDP, etc).

2. Salto a Salto:

   Cada LSR selecciona el próximo salto según el FEC que esté disponible.

El encaminamiento del LSP se realiza mediante protocolos de enrutamiento que utilizan algoritmos de estado de enlace para conocer la ruta trazada completa y tener rutas alternativas si algún enlace falla.

2.3.6 LABEL INFORMATION BASE (LIB)

Un LSR o LER tiene dos tablas, una dedicada a la información de enrutamiento y la segunda con la información a nivel local de las etiquetas conocida como LIB. Los datos de la taba LIB se relacionan con las etiquetas que han sido asignadas por un LER/LSR y de las asociaciones etiqueta/FEC recibidas de los vecinos del dominio MPLS mediante los protocolos de Distribución de Etiquetas.

La construcción de estas tablas se basa en las operaciones que realizan las etiquetas y son las siguientes:

- PUSH: imposición de las etiquetas en un ruteador de ingreso LER.
- SWAP: la etiqueta es cambiada por otra dentro del mismo rango que identifica un FEC en los LSRs.
- POP: operación en la que se elimina la etiqueta en un LER al salir de la red MPLS.

La información que proporciona una tabla LIB da a conocer sobre la interfaz y etiqueta de entrada seguida de la interfaz y el valor de etiqueta de salida, este proceso se realiza en cada salto de un LSR o LER y permite mantener actualizadas las rutas LSP. En la tabla 2.1 se muestra un ejemplo de la información que tiene una tabla LIB.

Interfaz de Entrada	Etiqueta de Entrada	Interfaz de Salida	Etiqueta de Salida
1	60	3	75
2	90	1	80

Tabla 2.1 Ejemplo de la información proporcionada por una tabla LIB

2.4 ENCABEZADO DE MPLS

En la figura 2.4 se presentan los campos de la cabecera genérica MPLS que se asigna una vez a la entrada en el router LER.

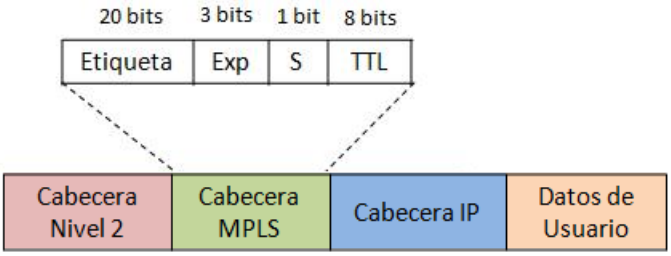


Figura 2.4 Estructura genérica de la cabecera MPLS

Como se observa en la figura 2.4 la cabecera MPLS está formada de 32 bits distribuidos en cuatro campos que son:

- **Etiqueta:** identifica a que conjunto de FEC está asignado el paquete y mediante este campo los ruteadores deciden por donde encaminar el paquete o que LSP debe seguir.

- **Exp (Experimental):** bits de uso experimental cuya proyección es la utilización para CoS aplicando Calidad de Servicio para asignar un nivel de prioridad a cada paquete.

- **S (Stack):** para apilar las etiquetas en forma jerárquica, si S vale 1 se trata de la última etiqueta en la pila (primera en ingresar a un dominio MPLS), caso contrario S vale 0. En caso de existir una sola etiqueta el valor de S es 1. El valor de S permite conocer que tras la cabecera MPLS está la cabecera de red u otra cabecera MPLS (si existen más dominios).

- **TTL (Time To Live):** cumple con una función similar a la del campo TTL de IPv4. Cuando a un paquete se le asigna la cabecera MPLS el campo TTL copia el valor TTL

del paquete IP pero reducido en una unidad en el LER y por cada salto que realice en el dominio MPLS. Este mecanismo permite reducir la posibilidad de bucles en la red y de igual manera al salir de la red MPLS en el LER el campo TTL de la cabecera MPLS se traslada al campo TTL del paquete IP.

2.4.1 APILAMIENTO

Si dentro de un dominio MPLS se encuentran más dominios, se crean cabeceras MPLS de acuerdo al número de dominios que existan, entonces las etiquetas de dichas cabeceras forman una pila. En la figura 2.5 se muestra un dominio MPLS que contiene en su interior otro dominio y en el cual el funcionamiento de una pila se puede detallar mejor.

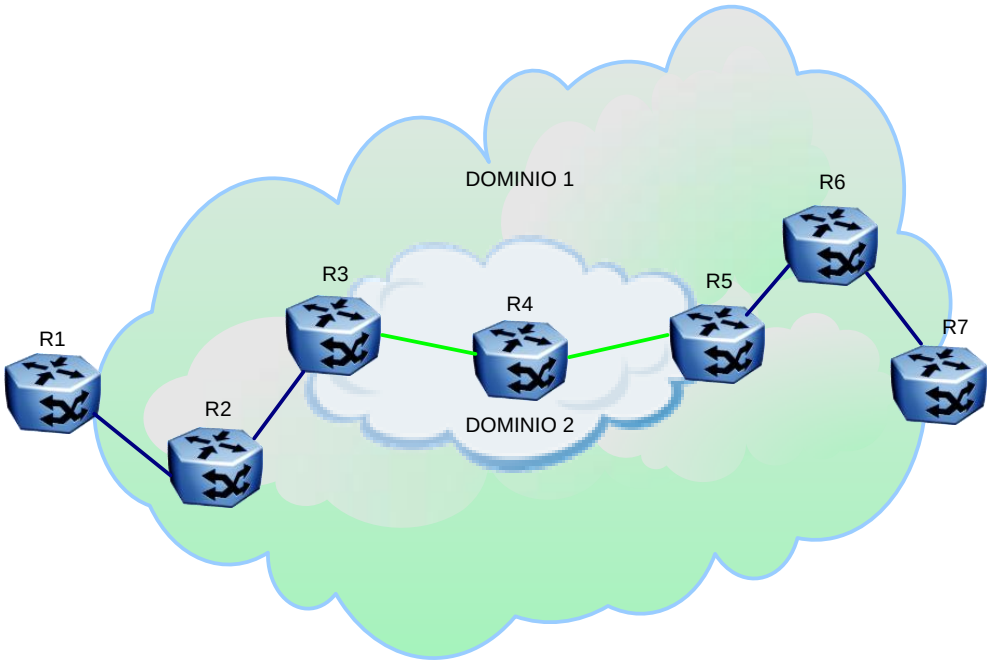


Figura 2.5 Dominio MPLS dentro de otro dominio MPLS

En la figura 2.5 se tienen dos dominios, uno dentro del otro, en este caso el campo ‘S’ (Stack) de la cabecera MPLS juega un rol muy importante ya que dependiendo del valor que indique se enviará el paquete por enrutamiento convencional o se someterá a las reglas del otro dominio MPLS.

Como se observa en la figura 2.5, tras el ingreso de un paquete a la red, el router R1 cumple la función de LER y le asigna una cabecera MPLS con el valor de S=1 porque es la primera en ingresar, pero en la pila es la última, a su paso por el R2 solo se realiza un cambio de etiqueta y un decremento en el valor del TTL. Cuando el paquete llega a R3, éste ingresa a otro dominio MPLS y se le asigna una segunda cabecera, pero como no es la primera el campo S tiene el valor de 0, y se coloca sobre la primera cabecera y el paquete se dirige a R4, en donde solo se realiza la conmutación de etiquetas y decremento del TTL de la segunda cabecera (la única que observa). Al llegar el paquete a R5 (LER de salida del Dominio 2) éste analiza el campo S y conoce que no es la única cabecera que hay así que elimina la cabecera MPLS en el orden LIFO[61], es decir la segunda. Ahora el paquete tiene una sola cabecera con un valor de TTL igual al que salió del R2 y se lo envía a R6 y finalmente a R7 que es el LER del dominio 1, en el R7 se analiza el valor de S, como es 1, conoce que es la última etiqueta en salir y lo encamina utilizando los protocolos de enrutamiento hacia la red a la que pertenece.

Para que el LER pueda interpretar el tipo de cabecera de red al salir totalmente de un dominio MPLS utiliza el campo S cuando tiene el valor de 1. En la cabecera MPLS, el campo Etiqueta tiene valores reservados para identificar la red de la que proviene el paquete, por lo que un LER de salida tras analizar S también analiza la Etiqueta para definir el tipo de cabecera de red y encaminar el paquete de acuerdo al tipo de red de la que proviene.

2.4.2 POSICIÓN DE LA CABECERA MPLS EN DIFERENTES TECNOLOGÍAS

La cabecera MPLS se inserta generalmente entre los niveles 2 y 3, si el protocolo de transporte de datos a nivel de enlace ya contiene un campo para etiquetas como el VPI/VCI[62] de ATM o DLCI[63] de Frame Relay se pueden utilizar estos campos para asignar la primera etiqueta y el resto de etiquetas entre la cabecera de enlace y la cabecera IP como se indica en la figura 2.6.

---

[61] **LIFO** Last In, Fist Out
[62] **VPI/VCI** Virtual Path Identifier/Virtual Circuit Identifier
[63] **DLCI** Data Link Connection Identifier

Figura 2.6 Posicionamiento de la cabecera MPLS en ATM y Frame Relay

En este tipo de redes hay un inconveniente con el decremento del TTL de la cabecera MPLS porque se coloca como se menciona anteriormente en el campo VPI/VCI o DLCI al no contar con el hardware para este proceso, pero se soluciona calculando al inicio el número de routers que va a atravesar el paquete y se decrementa su TTL al inicio además se necesita un mecanismo extra para evitar fallos por bucles que debe ser configurado por el administrador de la red; este método es válido solo para el dominio MPLS.

Para el caso de otras tecnologías como PPP[64] y LAN[65] que no cuentan con un campo que pueda ser utilizado para las etiquetas se emplea una nueva cabecera genérica MPLS de 4 octetos, esta cabecera se inserta entre la cabecera del nivel 2 y la del nivel 3 como se muestra en la figura 2.7.

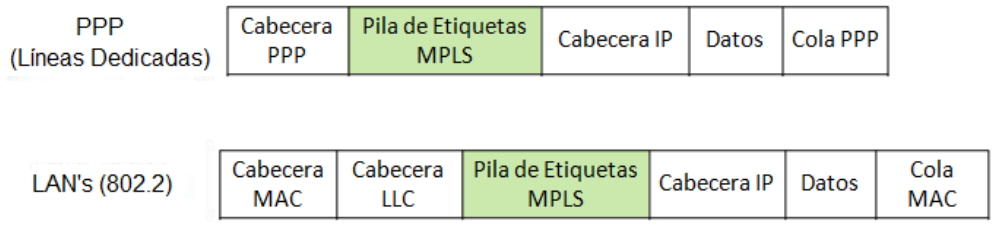


Figura 2.7 Posicionamiento de la cabecera MPLS en PPP y LAN

[64]**PPP** Point to Point Protocol
[65]**LAN** Local Area Network

CAPÍTULO 2

2.5 DESCRIPCIÓN FUNCIONAL DE MPLS

La conmutación multinivel que realiza MPLS se basa fundamentalmente en la separación de dos funciones que a su vez están efectivamente coordinadas, estas funciones se las conoce como:

- Plano de Control
- Plano de Envío

Los routers o switches que soportan MPLS trabajan en estos dos planos, específicamente los LER al ser el borde del dominio MPLS cumplen con estas dos funciones de encaminamiento y de envío inicial de los paquetes asignando una cabecera MPLS mientras que los LSR solo se encargan de la conmutación de las etiquetas ignorando que es lo que hay tras de la cabecera MPLS, es decir la cabecera de red.

2.5.1 FUNCIONAMIENTO DEL PLANO DE CONTROL

El Plano de Control utiliza los protocolos de enrutamiento ya sean de vector distancia o estado de enlace, para el intercambio de información dentro de la red MPLS, permitiendo la construcción y mantenimiento de las tablas de enrutamiento que proporcionan las características de la topología, patrón de tráfico o detalles de los enlaces. De esta manera se mantiene coherencia entre los LER y LSR evitando que a un determinado LSR le llegue un paquete con una etiqueta para el cual no tiene entrada en su tabla.

La difusión de las tablas de enrutamiento a los vecinos es muy importante porque establece los caminos virtuales LSP que los LER indican al inicio para la generación de las tablas de envío utilizando también la señalización que proveen los Protocolos de Distribución de Etiquetas (RSVP, LDP o TDP) y posteriormente el intercambio de etiquetas (Plano de Envío). Al tener la tabla de encaminamiento actualizada se escoge la dirección del próximo salto permitiendo el cálculo de las mejores rutas dentro de la red MPLS y caminos emergentes en caso de fallos.

2.5.2 FUNCIONAMIENTO DEL PLANO DE ENVÍO

El Plano de Envío MPLS utiliza la información de las etiquetas para la conmutación local de las mismas y para el envío de los paquetes a sus vecinos dentro del dominio, es decir se encarga de las asignaciones y modificaciones de etiquetas rigiéndose a la información proporcionada por el Plano de Control.

El paquete conforme avanza dentro de la red MPLS adquiere una nueva etiqueta, el valor de esta etiqueta define el FEC (Forward Equivalence Class) asignado. En la figura 2.8 se puede apreciar el intercambio de etiquetas de un paquete.

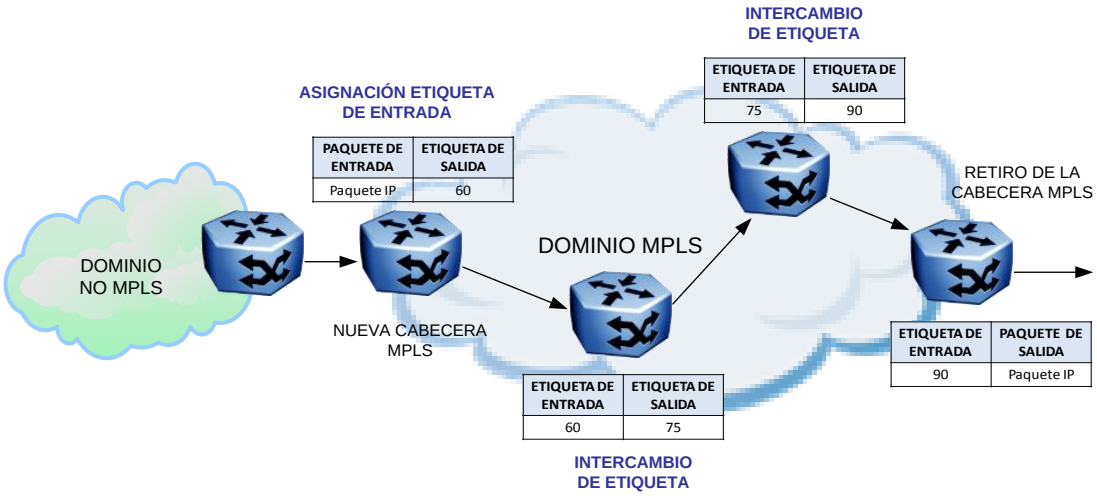


Figura 2.8 Intercambio de Etiquetas de un dominio MPLS

Como se observa en la figura 2.8 un paquete de cualquier otra red (dominio no MPLS) ingresa a la red MPLS, el router de borde LER es el encargado de analizar el paquete y clasificarlo a un determinado FEC, luego al añadirle una cabecera MPLS el campo etiqueta tiene un valor de acuerdo a su FEC consultando con la tabla de enrutamiento y envío para este caso la etiqueta de salida es 60.

Posteriormente tras la asignación de la cabecera MPLS el paquete realiza su siguiente salto a otro LSR y éste consulta en su tabla de envío y observa que la etiqueta de entrada es 60 y le asigna una nueva con el valor de 75, el siguiente LSR realiza la misma acción y tiene como

etiqueta de entrada 75 y de salida 90. Al llegar al LER de salida para éste la etiqueta de entrada es 90 pero su función es la de retirar la cabecera MPLS y enviar al paquete utilizando enrutamiento convencional (tabla de enrutamiento).

En resumen los LSR solo analizan el campo *"etiqueta"* para buscar y localizar si en su tabla se encuentra la etiqueta de entrada, una vez localizada esta etiqueta es modificada por una nueva a su salida por una determinada interfaz. El camino que siguen los paquetes (LSP) se forma a través de cada salto en un solo sentido, para un tráfico dúplex se requiere la creación de dos LSPs, uno en cada sentido.

2.6 GENERALIDADES DEL FUNCIONAMIENTO DE MPLS

MPLS encaja perfectamente en las redes troncales ya que una de sus funcionalidades es manejar un plano de control (enrutamiento) y un plano local para el intercambio de etiquetas con lo cual adapta redes de distintas tecnologías al insertar una nueva cabecera que le permite al paquete pasar por un dominio MPLS de acuerdo a ciertos parámetros de Calidad de Servicio dependiendo del valor asignado en el campo etiqueta.

El significado de los valores asignados a las etiquetas es definido en rangos de acuerdo a la clasificación FEC y basados en los criterios de los administradores de red. En la tabla 2.2 se muestra un ejemplo de rangos de etiquetas que identifican al tráfico de algunos tipos de redes.

TRÁFICO	RANGO DE ETIQUETAS	
IPv4	16	50
Fast Ethernet	51	150
Token Ring	151	155

Tabla 2.2 Ejemplo de la asignación de etiquetas para algunas tecnologías

Las etiquetas tienen 2^{20} -16 posibilidades para asignar los valores, las 16 etiquetas exceptuadas son de carácter reservado. Con esto durante el paso del paquete por el dominio MPLS cada

LSR intercambia las etiquetas; pero por otra dentro del mismo rango, así en todo el dominio se guarda la consistencia. Una vez conocida como es la asignación de las etiquetas, en la figura 2.9 se presenta un esquema general del funcionamiento de MPLS.

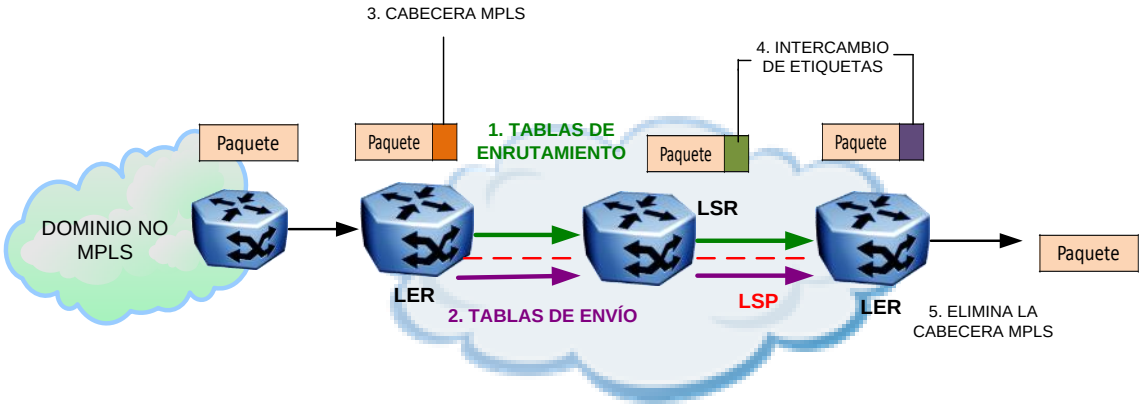


Figura 2.9 Funcionamiento general de MPLS

Como se observa en la figura 2.9 se puede describir el funcionamiento de MPLS en 5 pasos básicos que son los siguientes:

1. En primera instancia se construyen las tablas de encaminamiento que son proporcionadas como información de los protocolos de enrutamiento interno, tras la difusión de estas tablas de enrutamiento se crean los caminos virtuales LSP que los LER indican.

2. Con la utilización de los Protocolos de Distribución de Etiquetas se proporciona la información de las tablas de envío para el intercambio de etiquetas de los LSR.

3. Una vez informados los LER/LSR de las tablas de enrutamiento y envío, tras la llegada de un paquete a un LER de entrada, éste le asigna una cabecera MPLS con una etiqueta de acuerdo a su FEC y lo envía dentro del dominio MPLS.

4. Una vez dentro del dominio MPLS los LSRs se encargan del intercambio de etiquetas haciendo uso de las tablas de envío, relacionando la etiqueta de entrada y la etiqueta de salida.

5. Finalmente al llegar el paquete al LER de salida se elimina la cabecera MPLS del paquete; si su campo S es igual a 1, analiza la etiqueta para saber de qué tipo de red procede y se lo envía por enrutamiento fuera del dominio a su destino final.

2.7 APLICACIONES DE MPLS

MPLS es una tecnología abierta y proporciona muchas aplicaciones a nivel de redes troncales, a continuación se describen las más comunes.

2.7.1 INGENIERÍA DE TRÁFICO

Es una facilidad que ofrece MPLS para adaptar los flujos de tráfico a los recursos físicos de la red, equilibrando de forma óptima la utilización de los mismos, de manera que no haya recursos utilizados excesivamente y otros no, con lo que se provocaría cuellos de botella y colapso de los enlaces.

La utilización masiva de algunas rutas de enlaces se puede dar por la elección de algún protocolo de enrutamiento que se base en el cálculo del camino más corto lo que provoca la utilización de uno solo y se sature, pese a la existencia de otros alternativos pero no tan cortos.

Con la Ingeniería de Tráfico es factible desviar parte del tráfico cursante por otro camino alternativo menos congestionado aunque no sea la ruta más corta, teniendo el administrador de la red la posibilidad de:

1. Establecer rutas explícitas especificando el camino LSP exacto (cobre, fibra óptica, etc.)

2. Rutas restringidas para el caso de servicios especiales.

3. Calcular la ruta más eficiente en base a los requerimientos y restricciones.

4. Obtener informes estadísticos sobre el tráfico que cursa constituyendo una herramienta eficaz para el análisis de la distribución de los recursos de la red y para una planificación futura.

2.7.2 CALIDAD DE SERVICIO

La Calidad de Servicio o QoS se define por la UIT como *"el efecto global de la calidad del funcionamiento de un servicio que determina el grado de satisfacción de un usuario de dicho servicio"*. [14]

La Calidad de Servicio permite controlar algunas de las características que influyen en la transmisión de paquetes como el ancho de banda, latencia, jitter, las pérdidas de los paquetes en la red, retardos, entre otras, garantizando la disponibilidad del servicio.

La aplicación de QoS en una infraestructura de red permite al proveedor:

- Priorizar las aplicaciones que requieren de un alto nivel de servicio como la voz.
- Maximizar el uso de la infraestructura de red, utilizando los recursos eficazmente.
- Mejorar las prestaciones para los servicios en tiempo real.
- Actuar de forma rápida y eficiente en caso de incidencias.
- Dimensionar óptimamente los recursos de la red en función del número de usuarios y del nivel de disponibilidad.

En MPLS, la Calidad de Servicio está dada por la priorización que se da a los flujos de tráfico conocidos como FEC y también por la posibilidad de aplicar técnicas de Ingeniería de Tráfico

para descongestionar la red despachando el tráfico por rutas seguras (LSP) y sin mayores demoras de la siguiente manera:

1. Tras la asignación de una cabecera a un paquete al ingresar a un dominio MPLS, el campo etiqueta es asignado en base a la clasificación FEC, después de esto no es necesario que los LSRs tengan que volver a clasificar los paquetes en cada salto, simplificando los recursos de la red y disminuyendo los retardos en los saltos porque solo se conmutan las etiquetas sin analizar las cabeceras de red.

2. Un LSP además de ser la ruta para cierto conjunto de paquetes también puede encaminarlos por distintos medios de transmisión como fibra óptica o cobre según las necesidades que presenten los usuarios.

2.7.3 DIFERENCIACIÓN DE SERVICIOS MEDIANTE CLASES

La cabecera MPLS tiene el campo EXP, que se ha mencionado anteriormente, estos tres bits de uso experimental se están utilizando en la actualidad para la diferenciación de las Clases de Servicios (CoS) por lo que sería posible implementar el modelo de Servicios Diferenciados propuesto por el IETF en la RFC 2474 y RFC 2475.

El modelo de Servicios Diferenciados define una variedad de mecanismos para poder clasificar el tráfico en un número finito de Clases de Servicio, de tal forma que cada clase de tráfico tenga diferente prioridad como por ejemplo diferenciar entre aplicaciones de correo electrónico y transferencia de archivos (para los que el retardo no es crítico) de otros como la voz y el video interactivo (que dependen del retardo y de su variación).

En MPLS, con la utilización del campo EXP para la implementación del modelo de Servicios Diferenciados la cabecera MPLS añadida al inicio lleva un identificador con $2^3=8$ posibilidades para que los LSRs traten a los paquetes con prioridad. De esta manera un LSR que soporte Servicios Diferenciados dentro del dominio MPLS además de conmutar en base a los 20 bits del campo etiqueta, examina también en base a los 3 bits del campo EXP para proporcionarle al paquete una Calidad de Servicio.

Es posible que los paquetes clasificados dentro de un determinado FEC que sigue un mismo LSP puedan tener más prioridad que otros utilizando las Clases de Servicios y también de forma independiente los LSP puedan tener más prioridad que otros siendo LSP de máxima prioridad, de media prioridad o LSP que transportan tráfico Best Effort.

Actualmente no existen restricciones en la utilización del campo EXP y puede ser usado a conveniencia por cada proveedor, ofreciendo a sus clientes servicios de distinta calidad y precio.

2.7.4 REDES PRIVADAS VIRTUALES

A continuación se describe de manera muy general las ventajas que se tiene con la implementación de VPNs[66] utilizando MPLS.

Una Red Privada Virtual es una red de información privada que utiliza una infraestructura de Telecomunicaciones pública y conecta a usuarios de forma remota hacia una red principal, siendo una solución ideal para las empresas, y su objetivo es brindar aplicaciones Intranet y Extranet integrando soluciones multimedia.

Entre las características más importantes de una VPN se destaca la seguridad ya que se crea un canal privado de comunicación entre dos puntos utilizando la infraestructura de Internet, la privacidad se mantiene a través de Protocolos de Túnel o de aislamiento, que aplican encapsulación o cifrado de datos.

Las VPNs tradicionales ya sean basadas en PVC[67] (Circuitos Virtuales Permanentes) o túneles IP han sido de gran beneficio pero tienen ciertos inconvenientes que pueden ser resueltos con la utilización de MPLS.

Las VPNs basadas en PVC utilizan la infraestructura de las redes ATM o Frame Relay y los PVCs se establecen entre los nodos de extremo a extremo con la configuración manual de cada uno, lo que implica complejidad en la gestión de la red del proveedor ya que se trata de

---

[66] **VPN** Virtual Private Network
[67] **PVC** Path Virtual Circuit

una topología lógica mallada sobrepuesta a la red física y al agregar un nuevo miembro a la VPN es necesario reestablecer todos los PVCs, la seguridad que ofrecen se basa en la separación de tráfico por PVC.

Las IP VPN están basadas en Protocolos de Túnel como por ejemplo IPSec[68], la información se cifra y se encapsula en una nueva cabecera IP. La desventaja en este tipo de implementaciones se da porque se ocultan las cabeceras de los paquetes originales y las opciones de QoS son bastante limitadas ya que no se puede distinguir los flujos por aplicación dificultando la asignación de los diferentes niveles de servicio.

En general los inconvenientes más comunes que tienen las VPN tradicionales son las siguientes:

- Se basan en conexiones punto a punto (PVC o túneles).
- La configuración de cada nodo de la VPN es manual y cada vez que se integra uno supone la reconfiguración de todos los anteriores.
- La Calidad de Servicio se ofrece hasta cierta parte, más no durante el transporte.
- El modelo topológico sobrepuesto a la red existente implica poca flexibilidad en la provisión y gestión del servicio.

Utilizando MPLS para implementar VPNs se eliminan los inconvenientes de las tecnologías anteriores. En primera instancia el modelo topológico que se crea no se sobrepone sino se acopla a la red del proveedor, esto elimina las conexiones extremo a extremo (túneles IP convencionales o circuitos virtuales) y los túneles se van creando con el intercambio de las etiquetas formándose así los LSP que vendrían a ser los “túneles MPLS”.

---

[68] **IPSec** Internet Protocol Security

Dentro de la red del proveedor las VPNs se forman mediante las rutas virtuales LSPs, similares a los túneles de las VPNs tradicionales pero con la diferencia de que la información se transporta por el mecanismo de intercambio de etiquetas obviando la información de enrutamiento lo que facilita aplicar técnicas de QoS que son propagadas hasta el destino, reservando ancho de banda, estableciendo Clases de Servicios y aplicando Ingeniería de Tráfico de esta manera optimizando los recursos de la red y cumpliendo los máximos requerimientos de disponibilidad y seguridad.

Las ventajas que se tiene con MPLS son:

- Se elimina la complejidad de los túneles y los PVCs.

- Para la implementación no es necesario realizar cambios en todos los puntos involucrados como ocurre con las VPNs tradicionales por lo contrario solo se configura a nivel del proveedor evitando tareas complejas y riesgosas.

- Las garantías de Calidad de Servicio se mantienen de extremo a extremo separando los flujos de tráfico por clases.

- Para aumentar la seguridad se pueden utilizar los protocolos de encriptación manejados también por las VPNs tradicionales como IPSec.

- Con la Ingeniería de Tráfico que ofrece MPLS se garantiza que en el servicio VPN no influyan parámetros que afecten la calidad de extremo a extremo.

2.7.4.1 Generalidades de la Arquitectura de las VPN/MPLS

Una VPN/MPLS básica está formada de tres elementos físicos que son: P (Provider) o router interno del proveedor, PE (Provider Edge) o router frontera del proveedor y CE (Customer Edge) denominado así al router frontera del cliente; estos elementos constituyen la arquitectura externa de una VPN. Además existen dos aspectos internos de la arquitectura de

las VPN soportadas en MPLS que es necesario mencionar para una mejor compresión de su funcionamiento y son: el Route Distinguisher y el Route Target, mecanismos que permiten distinguir los requerimientos del cliente suscrito a una VPN.

2.7.4.1.1 Route Distinguisher

Los routers PE (Provider Edge) se conectan a los routers CE (Customer Edge) y distribuyen la información que contienen sobre las VPNs a otros routers PE a través del protocolo MP-BGP o Multiprotocolo BGP, en este intercambio de información el router PE agrega como prefijo a la dirección IPv4 una cantidad de 64 bits conocidos como Route Distinguisher lo que permite a la dirección IPv4 hacerla globalmente única (ruta privada) y resultando finalmente una dirección de 96 bits denominada VPNv4.

2.7.4.1.2 Route Target

El Route Target o ruta objetivo es un atributo adicional colocado a las rutas VPNv4 vía BGP que permite identificar la membresía de un cliente a una VPN cuando algunos sitios de cliente participan en más de una VPN. El Route Target se introdujo en la arquitectura de las VPN/MPLS para soportar topologías más complejas.

Cada enrutador PE define un valor numérico llamado Route Target que pueden ser:

- **Export:** es un valor numérico que identifica una membresía de VPN y es adjuntada a la ruta del cliente cuando se convierte en una ruta VPNv4.

- **Import:** cuando el valor numérico de una VPNv4 de la red de origen (Route Target Export) coincide con los valores del Route Target Import del route PE de destino, esta ruta es insertada en la tabla de ruteo virtual del router PE correspondiente al sitio del cliente de destino.

Para que una nueva ruta sea aceptada el valor de su ruta objetivo de salida (exportación) debe de coincidir con el valor de entrada (importación) del dispositivo de entrada.

CAPÍTULO 3. INFRAESTRUCTURA ACTUAL DE ECUANET-MEGADATOS S.A

3.1 INTRODUCCIÓN

En este capítulo se describe la infraestructura actual de la empresa MEGADATOS considerando la tecnología desplegada en el backbone de Quito y los nodos de Guayaquil y Cuenca, además de un breve análisis de las características de los equipos para conocer la posibilidad de su utilización a futuro para el soporte de nuevas aplicaciones y finalmente se realiza el análisis FODA de la empresa.

3.2 DESCRIPCIÓN DE LA INFRAESTRUCTURA

ECUANET - MEGADATOS S.A es una empresa de Telecomunicaciones que ofrece soluciones tecnológicas para usuarios residenciales y corporativos con cobertura a nivel nacional. Como parte de su infraestructura cuenta con enlaces nacionales e internacionales por medio de fibra óptica y para la entrega de los servicios finales lo hace por medio de enlaces de última milla por microondas, enlaces satelitales y cobre ya sean dedicados o compartidos. En la figura 3.1 se presenta un diagrama de bloques de la infraestructura general de MEGADATOS que será detallado a lo largo de este capítulo.

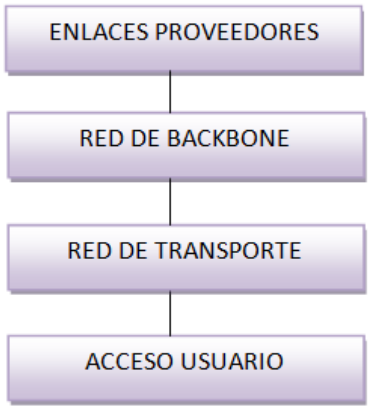


Figura 3.1 Diagrama de bloques de la Infraestructura de MEGADATOS

3.2.1 ENLACES CON PROVEEDORES

Actualmente la empresa cuenta con un backbone principal en la ciudad de Quito, el cual recibe enlaces internacionales de Transnexa y Telefónica además de enlaces nacionales con Telconet y CNT[69]. Estos enlaces son administrados en este backbone para la región Sierra y Oriente y para la cobertura de la región Costa desde Quito se envía al nodo de Guayaquil parte del enlace de Transnexa conjuntamente con otro enlace de Telefónica. Estos enlaces alcanzan capacidades de STM-1[70] que son distribuidos en E1[71] o E1 fraccionados para la cobertura en los nodos secundarios de las diferentes ciudades en donde los canales de datos pueden alcanzar velocidades más pequeñas.

Como se muestra en la figura 3.2 los enlaces que llegan al backbone de Quito son gestionados por un router de borde Cisco de la serie 7600 y para el enlace con Guayaquil la empresa utiliza la red de transporte de Transnexa. Cabe señalar que todos los enlaces de los proveedores de Internet son por medio de fibra óptica.

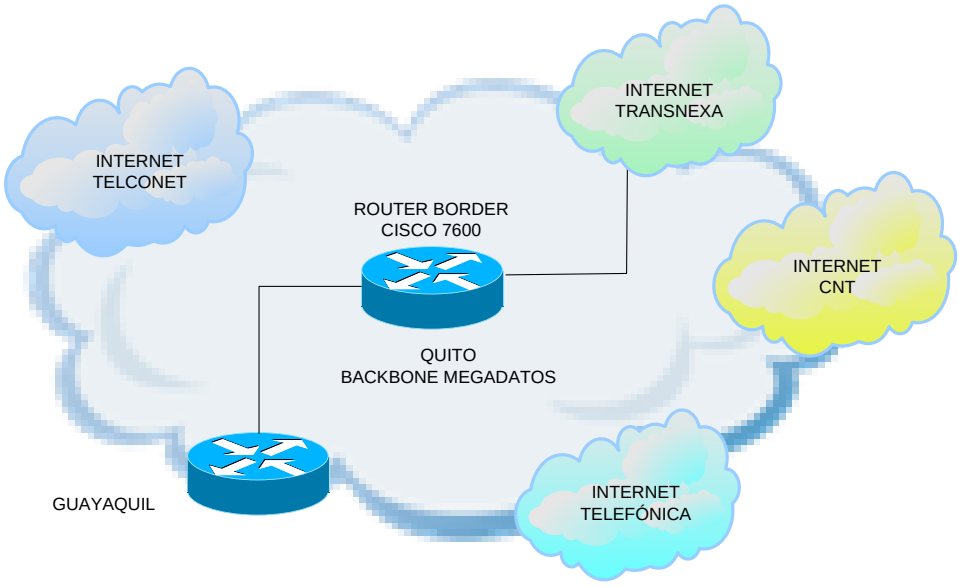


Figura 3.2 Enlaces con Proveedores

---

[69] **CNT** Corporación Nacional de Telecomunicaciones
[70] **STM-1** Synchronous Transport Module level-1
[71] **E1** 2Mbps

3.2.2 RED DE BACKBONE ACTUAL

Los tres nodos más importantes de la empresa MEGADATOS se encuentran en: Quito, Guayaquil y Cuenca, sin embargo el NOC-R1[72] de la ciudad de Quito es el de mayor importancia considerando la infraestructura y número de usuarios; el mismo esquema de arquitectura funcional es adoptado por el NOC-R2[73] de Guayaquil y el nodo de Cuenca. A continuación en la figura 3.3 se presenta un esquema de la red de backbone del NOC-R1 conjuntamente con la distribución de los equipos principales que constituyen la parte activa del Telepuerto UIO de la empresa.

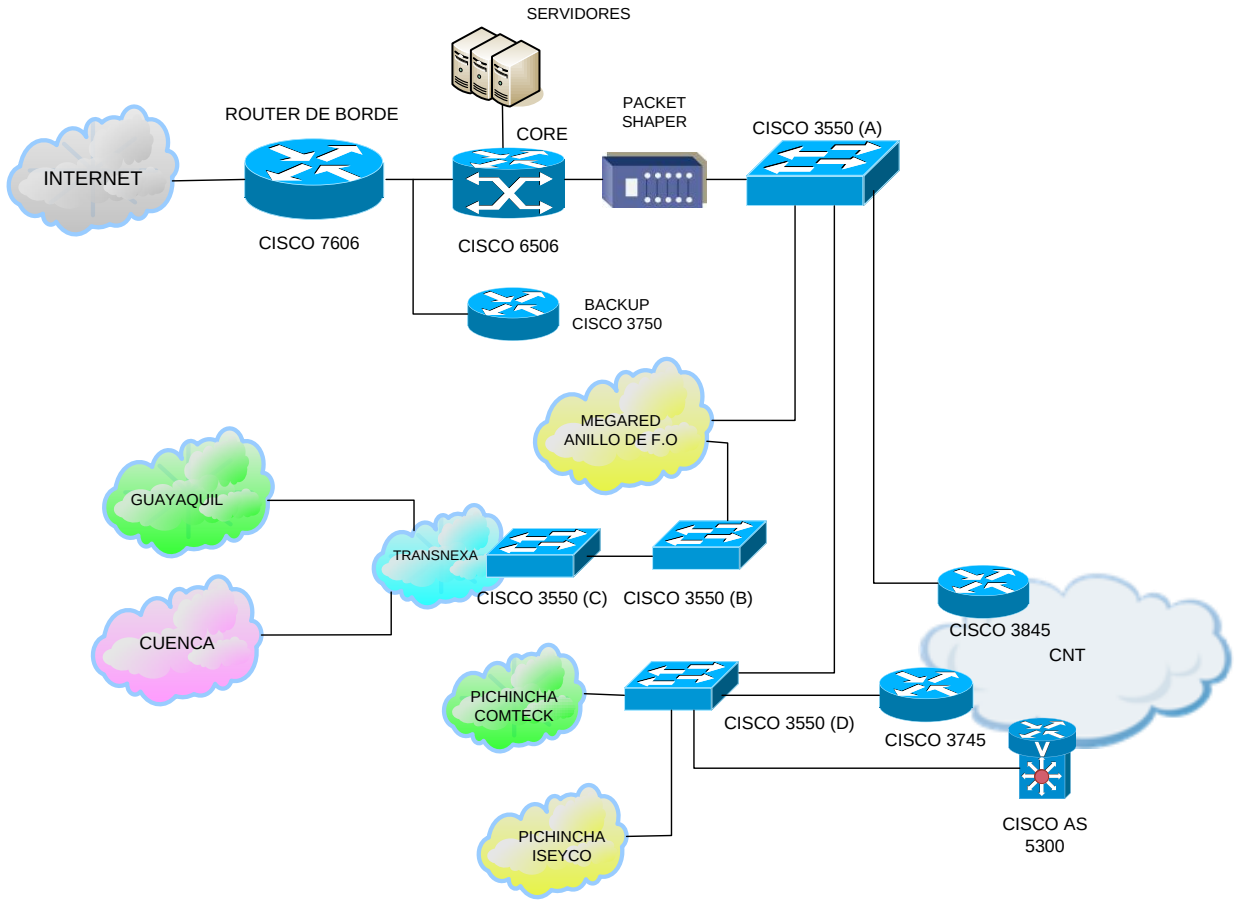


Figura 3.3 Esquema del Backbone Gigabit Ethernet de MEGADATOS

[72]**NOC-R1** Network Operation Center-Region 1
[73]**NOC-R2** Network Operation Center-Region 2

Como se observa en la figura 3.3 el router de borde Cisco 7606 es el concentrador de los enlaces de Internet, junto a éste mediante interfaz Gigabit Ethernet se encuentra el switch Cisco 6506 core de la red, de la misma manera utilizando interfaz Gigabit Ethernet se conecta con el switch 3550 (A) pasando antes por un equipo segmentador de ancho de banda, desde éste primer switch se distribuyen los enlaces hacia la Megared, otro switch 3550 (C) para Guayaquil y Cuenca utilizando la red transporte de Transnexa y finalmente otro switch 3550 (D) para la conectividad con los routers Cisco 3745, Cisco AS 5300 y los nodos Pichincha Comteck y Pichincha Iseyco éste último por medio de un Cisco 2950 con interfaz Fast Ethernet.

Los dos últimos nodos Pichincha Comteck y Pichincha Iseyco permiten la cobertura de sectores no céntricos del Distrito Metropolitano mediante enlaces de radio además de los sectores de Tabacundo y Cayambe con última milla de cobre e inalámbrica. También en el switch Cisco 6506 se hallan configurados en una VLAN[74] los servidores con interfaces Fast Ethernet; cabe mencionar que el switch core 6506 tiene un backup que es el router Cisco 3750.

En los routers Cisco 3845 y 3745 se hallan configurados la mayoría de los clientes ADSL[75] home utilizando arquitectura ATM ya sea para canales compartidos o dedicados dentro de la región de cobertura del NOC-R1.

Como se menciona anteriormente uno de los enlaces hacia los clientes utilizando fibra óptica o cobre desde el Telepuerto UIO es la Megared que está formada mediante dos anillos: anillo A y anillo B en los cuales se enlazan los nodos mediante rutas activas así como también rutas de backups.

En la figura 3.4 se indican las rutas activas de los anillos A y B que corresponden a los nodos principales del Telepuerto UIO (Megared) que constituyen los enlaces principales en la ciudad de Quito.

---

[74] **VLAN** Virtual Local Area Network
[75] **ADSL** Asymmetric Digital Subscriber Line

CAPÍTULO 3

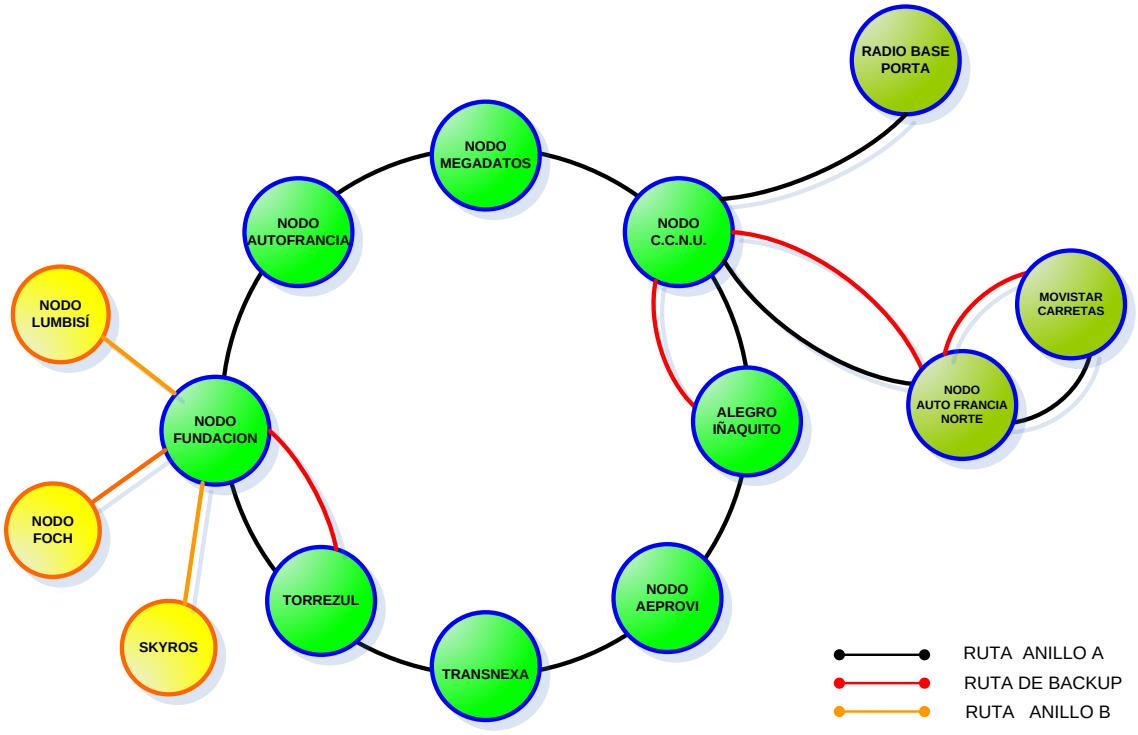


Figura 3.4 Rutas activas de la Megared

Los nodos que conforman la ruta A son los que se enlazan directamente con el Telepuerto UIO por medio de fibra óptica, mientras que los nodos de la ruta B nacen en los nodos de la ruta A con el objeto de cubrir más sectores de la ciudad de Quito inclusive a otras ciudades como es el caso del nodo SKYROS que da cobertura al Coca. En la tabla 3.1 se indica los enlaces de los nodos de la ruta A hacia B en los que se utiliza fibra óptica.

NODO ORIGEN	NODO DESTINO
FUNDACIÓN	LUMBISÍ
FUNDACIÓN	SKYROS
FUNDACIÓN	TORREZUL
CCNU	AUTOFRANCIA NORTE
AUTOFRANCIA NORTE	CARRETAS

Tabla 3.1 Nodos que se enlazan por fibra óptica

CAPÍTULO 3

En la figura 3.5 se presentan los nodos que conforman la Megared, específicamente se muestran los equipos e interfaces que se utilizan para la interconexión.

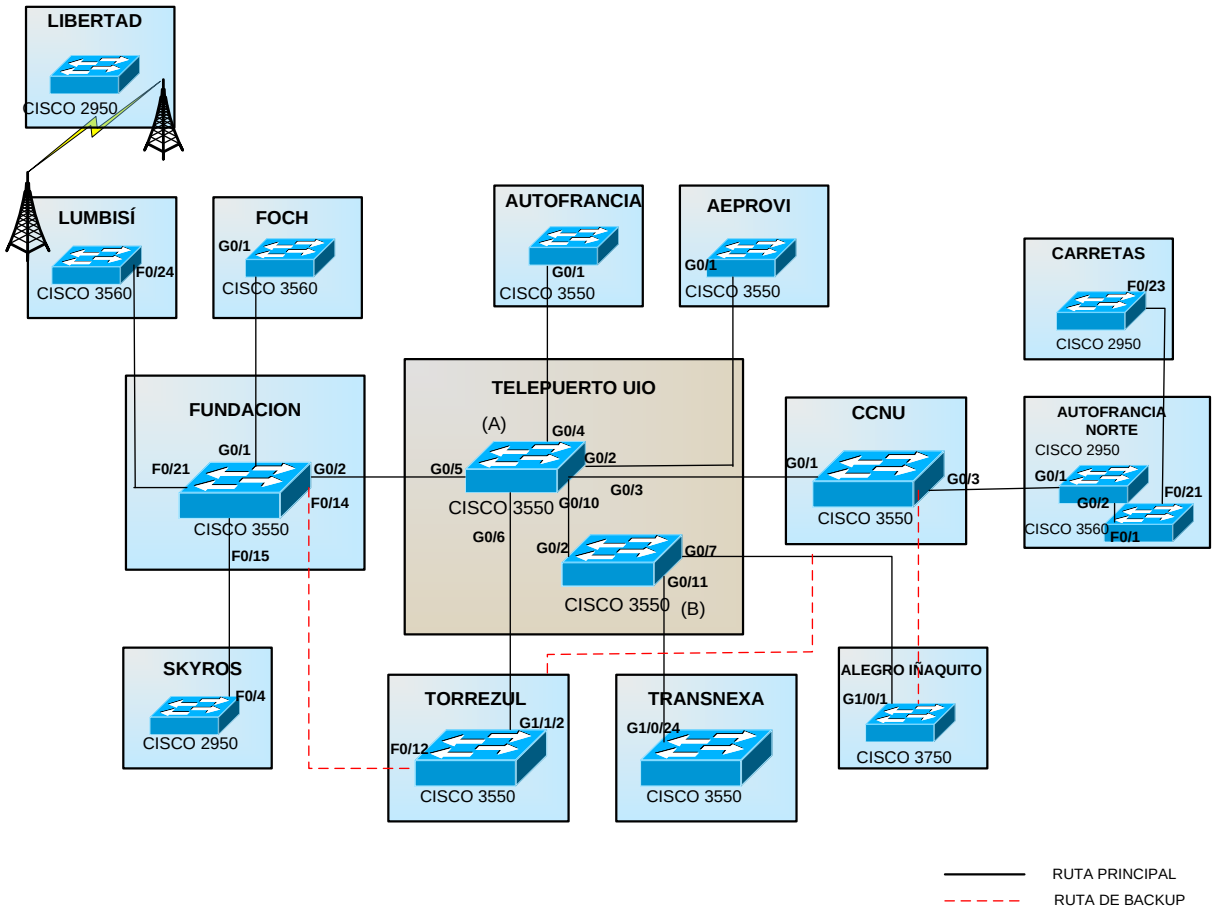


Figura 3.5 Nodos que conforman la Megared

Como se observa en la figura 3.5 desde el Telepuerto UIO se distribuyen los enlaces por medio de los dos switch 3550 hacia la Megared, específicamente desde el switch que forma parte del core el Cisco 3550 (A) parten los enlaces de los nodos: Fundación, CCNU, Torrezul, Autofrancia y AEPROVI[76] con interfaces Gigabit Ethernet a los equipos Cisco 3550.

Desde el otro switch 3550 (B) del Telepuerto que está enlazado al core se distribuye el enlace hacia los nodos de Transnexa y de Alegro Iñaquito con interfaces Gigabit Ethernet.

[76]**AEPROVI** Asociación Ecuatoriana de Proveedores de Internet

CAPÍTULO 3

En el nodo de Alegro Iñaquito se encuentran configurados en VLANs los clientes home correspondientes a la tecnología ADSL que utilizan la última milla de cobre de CNT.

En la tabla 3.2 se resumen los equipos de red operativos de cada uno de los nodos del NOC-R1 de Quito.

NODO	CANTIDAD/EQUIPO	MARCA	SERIE
AUTOFRANCIA	1 SWITCH 2 SWITCH LRE	CISCO CISCO	3550 2950ST
FUNDACIÓN	1 SWITCH 1 SWITCH 2 SWITCH LRE	CISCO CISCO CISCO	3550 2950 2950ST
FOCH	1 SWITCH 2 SWITCH LRE	CISCO CISCO	3560 2950ST
SKYROS	1 SWITCH 2 SWITCH LRE	CISCO CISCO	2950 2950ST
LUMBISI	1 SWITCH	CISCO	3560
LIBERTAD	1 SWITCH	CISCO	2950
TORREZUL	1 SWITCH 2 SWITCH LRE 1 SWITCH	CISCO CISCO CISCO	3750 2950ST 2960
AEPROVÍ	1 SWITCH	CISCO	3550
CCNU	1 SWITCH 1 SWITCH 3 SWITCH LRE	CISCO CISCO CISCO	3550 2950 2950ST
AUTOFRANCIA NORTE	1 SWITCH 1 SWITCH LRE 1 SWITCH	CISCO CISCO CISCO	3560 2950ST 2950
CARRETAS	1 SWITCH	CISCO	2950
TRANSNEXA	1 SWITCH	CISCO	3550
ALEGRO IÑAQUITO	1 SWITCH	CISCO	3750

Tabla 3.2 Equipos de los nodos de la Megared

3.2.2.1 Nodo de Guayaquil

Para la interconexión con el Nodo de Guayaquil, como se mencionó anteriormente, se utiliza la red de transporte de Transnexa que parte desde el nodo Transnexa de la Megared de Quito, este enlace proporciona Internet y comunicación directa con los equipos que se encuentran en Guayaquil. Cabe mencionar que el router core de esta ciudad también recibe un enlace de Internet de Telefónica para suplir con la demanda de los clientes que se enlazan a los diferentes nodos secundarios.

En la figura 3.6 se muestra un esquema básico del nodo de Guayaquil y su interconexión con los nodos secundarios más importantes.

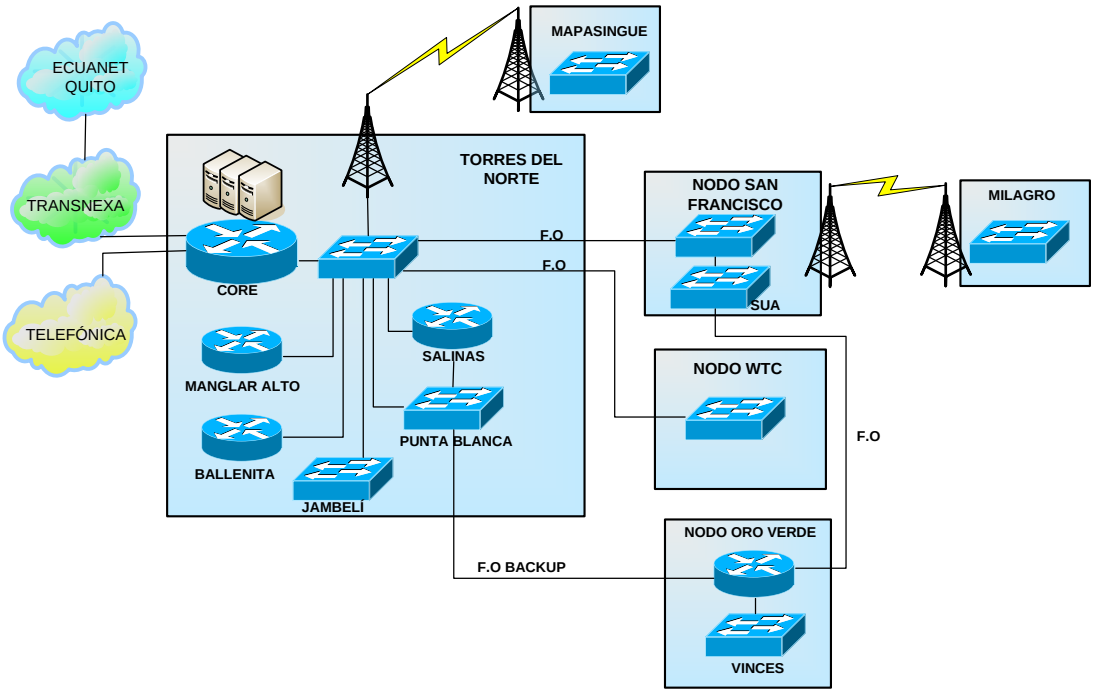


Figura 3.6 Interconexión del Nodo de Guayaquil

Como se observa en la figura 3.6 al router de core llegan los enlaces de Internet y en éste se gestionan y administran para la conectividad con los nodos secundarios WTC, San Francisco, Oro Verde, Milagro y Mapasingue por medio de routers o switchs utilizando cobre, fibra óptica y enlaces inalámbricos.

3.2.2.2 Nodo de Cuenca

Para la interconexión con el nodo de Cuenca se utiliza también la red de transporte de Transnexa que parte desde el nodo Transnexa de la Megared de la ciudad de Quito y llega a un router de borde Cisco 2851. A continuación en la figura 3.7 se indica un esquema general del nodo de Cuenca.

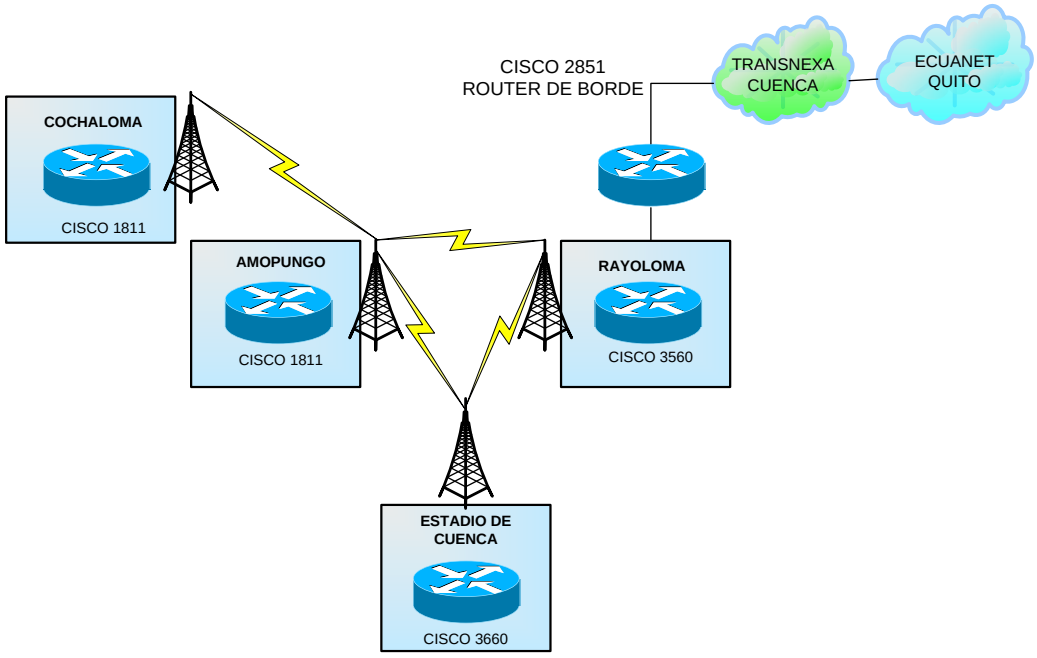


Figura 3.7 Esquema general del Nodo de Cuenca

Como se indica en la figura 3.7 el router de borde se enlaza directamente por medio de interfaz Fast Ethernet al router Cisco 3560 de Rayoloma, la función principal de este es la generación de VLANs. Entre el router de borde y Rayoloma hay un segmentador de ancho de Banda Packet Shaper. Para la conectividad de Rayoloma con el router Cisco 1811 de Amopungo se utiliza un enlace de radio de 5.8 Ghz y desde éste último por enlace de radio de 5.7 Ghz se conecta al router Cisco 1811 de Cochaloma.

El nodo Estadio de Cuenca tiene dos enlaces de radio el primero parte desde Amopungo con una capacidad de 12 Mbps y el segundo desde Rayoloma con una capacidad de 33 Mbps los dos llegan al router Cisco 3660.

En el nodo Estadio de Cuenca se encuentran los servidores de correo, RADIUS[77] y monitoreo para estos sectores.

3.2.3 RED DE TRANSPORTE

Para dar servicio a las diferentes ciudades en el país MEGADATOS utiliza infraestructura de otras empresas de Telecomunicaciones para el transporte de Internet y datos a los nodos, para que a su vez éstos den servicio a los clientes finales con enlaces inalámbricos o de cobre. A continuación en la figura 3.8 se indican las redes de transporte que utiliza la empresa para cubrir las diferentes ciudades del país.

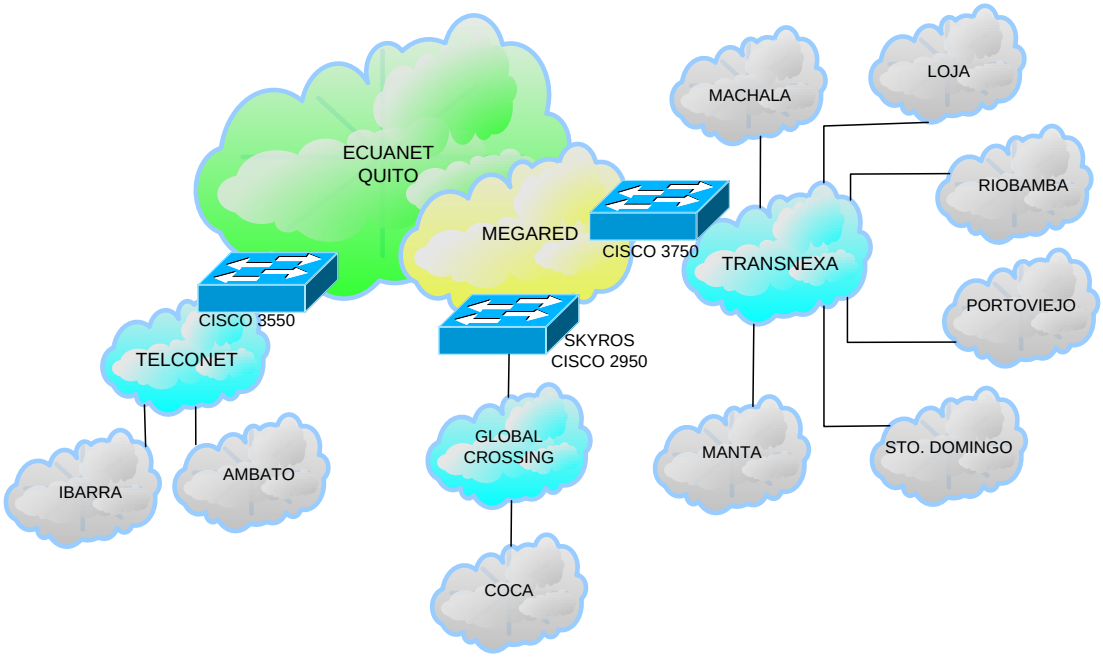


Figura 3.8 Esquema de las redes de Transporte que utiliza MEGADATOS

Como se observa en la figura 3.8 para los nodos de Ibarra y Ambato se utiliza la red de Transporte de TELCONET con capacidades de 5 y 4 E1 respectivamente, estos enlaces son distribuidos desde un switch Cisco 3550 que se encuentra en el backbone de la ciudad de Quito.

---

[77] **RADIUS** Remote Authentication Dial In User Service

Para la ciudad del Coca se utiliza la red de transporte de GLOBAL CROSSING que se enlaza desde el nodo de Skyros con un switch Cisco 2950 que pertenece a la Megared de Ecuanet-Quito. En el caso de las ciudades de Manta, Sto. Domingo, Portoviejo, Riobamba, Loja y Machala se utiliza infraestructura de TRANSNEXA desde el nodo del mismo nombre de la Megared.

En la figura 3.9 se indican los enlaces de Puyo y Macas que utilizan la red de trasporte de PORTA y se encuentran configurados en un router Cisco 3745 del backbone de Quito; cabe mencionar que el nodo de Macas cuenta con un enlace de backup desde el nodo Rayoloma de Cuenca utilizando un enlace de radio de EERCS[78], empresa que tiene infraestructura propia de datos e Internet en el sur del país.

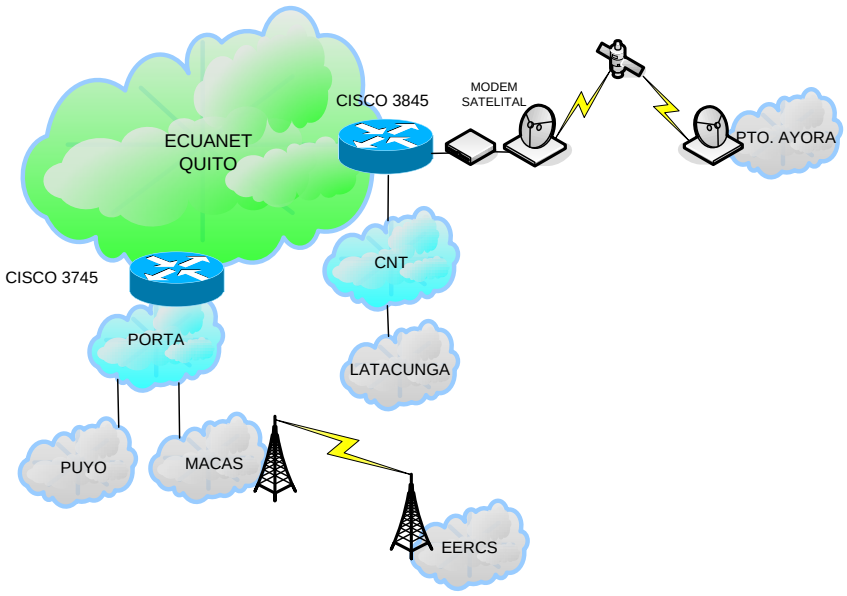


Figura 3.9 Esquema de la red de Transporte para otras ciudades

Por otra parte también se utiliza la infraestructura de CNT para la ciudad de Latacunga y por medio de enlace satelital para cubrir a Pto. Ayora en Galápagos, estos dos enlaces parten de un Router Cisco 3845 en el backbone de Quito.

---

[78] **EERCS** Empresa Eléctrica Regional Centro Sur

3.2.4 ACCESO DE LOS USUARIOS

El acceso del usuario para los servicios de Telecomunicaciones pueden ser por diferentes medios ya sea por fibra óptica, cobre, satelital e inalámbrico previa a la factibilidad del enlace. Generalmente en las ciudades de Quito y Guayaquil se utiliza fibra óptica para los clientes corporativos o clientes que lo requieran. En Quito estos enlaces se los distribuye desde los nodos de la Megared y en la ciudad de Guayaquil se los distribuye desde los nodos: Torres del Norte, San Francisco y nodo WTC.

Los enlaces por cobre pueden ser de dos maneras: si se trata de un cliente corporativo ECUANET proporciona la última milla hacia el cliente, utilizando switches Cisco LRE[79] desde uno de los equipos de conmutación en los nodos; otra de las maneras para llegar al cliente si es un usuario home o pequeña empresa se lo realiza utilizando la tecnología ADSL que como ya se conoce utiliza la línea telefónica para la transmisión de voz e Internet, para este caso se utiliza la última milla de CNT a nivel nacional. Como se indica en la figura 3.10 los clientes ADSL con tecnología ATM o VLAN se hallan configurados en el backbone de Quito, si utilizan ATM éstos se encuentran configurados en los routers Cisco 3745 y 3845 mientras que si son VLAN se encuentran configurados en el nodo Alegro Iñaquito, perteneciente a la Megared.

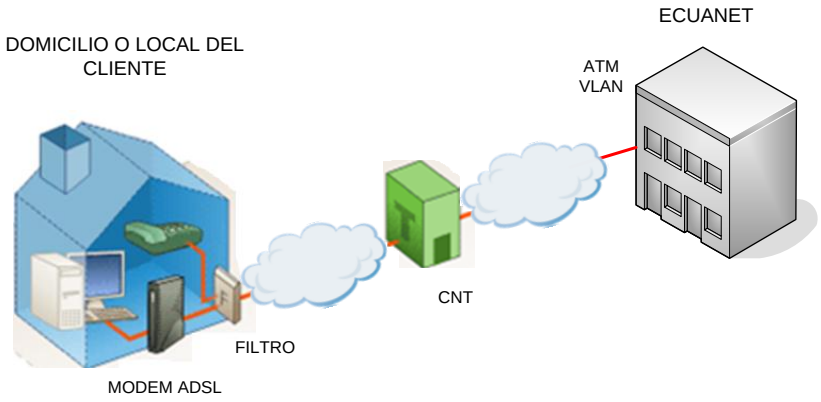


Figura 3.10 Acceso del usuario por tecnología ADSL

[79] **LRE** Long Reach Ethernet

Otro medio utilizado por la empresa para dar servicio a los clientes es a través de enlaces inalámbricos desde los nodos secundarios utilizando enlaces punto a punto y punto a multipunto con tecnología WIMAX, Microondas y Spread Spectrum. Para la ciudad de Quito los nodos Lumbisí, Carretas, Libertad, Cananvalle y Pichincha Comteck dan cobertura a los sectores alejados de la ciudad.

Para los clientes que utilizan enlaces satelitales a nivel nacional se requiere de la gestión de Internexa de Colombia para la comunicación con el Telepuerto de PanAmSat en Atlanta-USA permitiendo el acceso de los usuarios a Internet.

Finalmente dentro de la infraestructura de la empresa algunos nodos a nivel nacional y principalmente de Quito, Guayaquil y Cuenca cuentan con respaldos de enlaces satelitales para la contingencia y recuperación ante los desastres.

3.3 DESCRIPCIÓN GENERAL DE LOS EQUIPOS DE BACKBONE

A continuación se describen las características más importantes de los principales equipos que conforman la red actual de la empresa ECUANET-MEGADATOS, mencionando las series de switches y routers más utilizados.

3.3.1 SERIE CISCO CATALYST 2950

Los switches de la serie Cisco 2950 proveen acceso Ethernet sobre redes de fibra óptica, es un modelo apilable y proporciona puertos para Fast Ethernet y Gigabit Ethernet. Esta serie permite ofrecer servicios inteligentes con mayor seguridad, disponibilidad y QoS, características ideales para su ubicación al borde de la red. El software IOS ofrece funcionalidad para la transmisión de datos, video y servicios de voz mediante la configuración automática de la Calidad de Servicio mediante políticas de clasificación y discriminación de los distintos flujos de tráfico propio del software, es decir soportan DiffServ. En la figura 3.11 se muestra una gráfica de los switches de la serie 2950.

Fuente: http://www.cisco.com

Figura 3.11 Serie Cisco Catalyst 2950

En la tabla 3.3 se identifican los modelos que utiliza MEGADATOS con sus características más relevantes.

PRODUCTO	PUERTOS	CARACTERÍSTICAS
WS-C2950ST-24-LRE	2 puertos 10/100/1000BASE-T (uplink), 24 LRE y 2 SPF.	Proveen acceso a los servicios de banda ancha sobre el cableado telefónico.
WS-C2950ST-8-LRE	2 puertos 10/100/1000BASE-T (uplink), 8 LRE y 2 SPF.	
WS-C2950-24	24 puertos 10/100 y 2 puertos 100BASE-FX (uplink).	16 MB de memoria DRAM y 8 MB de memoria Flash.

Tabla 3.3 Productos de la serie 2950 utilizados por MEGADATOS

3.3.2 SERIE CISCO CATALYST 2960

El switch WS-C2960-24TT, se encuentra ubicado en el nodo Terrazul de la Megared, perteneciente a la serie 2960, ofrece conectividad Fast Ethernet y Gigabit Ethernet incluyendo características de seguridad mediante ACL[80] y control de admisión a la red además de QoS y soporte de servicios inteligentes mediante multidifusión, características adecuadas para su utilización al borde de la red.

[80] **ACL** Access Control List

La seguridad de la red se garantiza con el manejo de una amplia gama de métodos de autenticación, tecnologías de encriptación de datos, puertos y direcciones MAC, en la figura 3.12 se puede apreciar al switch Cisco WS-C2960-24TT.

Fuente: http://www.cisco.com

Figura 3.12 Switch Cisco WS-C2960-24TT

Las características más relevantes del switch WS-C2960-24TT son las siguientes:

- Este switch posee 24 puertos Ethernet de 10/100BASE-T y dos enlaces ascendentes de 10/100/1000TX.
- Proporciona mejoras para Spanning Tree.
- Configuración de hasta 255 VLANs por puerto.
- La tasa de envío basada en paquetes de 64bytes es de 6.5Mpps.
- 64 MB de memoria DRAM y 32 MB de memoria Flash.
- Soporte para MPLS e IPv6.

3.3.3 SERIE CISCO CATALYST 3750

Entre las características más importantes de la serie 3750 están la facilidad para el despliegue de aplicaciones convergentes, proporcionan flexibilidad de configuración adaptándose al cambiante entorno tecnológico mediante el software de imagen que permite un enrutamiento IP unicast y multicast, configuraciones avanzadas para datos y video y principalmente soporte de IPv6. Para la configuración utiliza Cisco Network Assitant Software, una herramienta basada en web para una configuración rápida utilizando plantillas preestablecidas.

Esta serie adicionalmente incorpora la tecnología Cisco StackWise, una arquitectura de apilamiento optimizada para Gigabit Ethernet hasta de nueve conmutadores de la serie Cisco

Catalyst 3750. Una pila de la serie 3750 se gestiona como un objeto único teniendo una dirección IP única lo que permite la administración única en cuanto a la seguridad, creación de VLANs y control con Calidad de Servicio.

Para el control de la seguridad tanto en la conectividad como en el control de acceso incluye ACL, autenticación y seguridad a nivel de puerto lo que ayuda a prevenir de ataques externos, principal preocupación de las empresas actualmente. Esta serie permite la configuración de hasta 1005 VLANs por pila y de hasta 12000 direcciones MAC, en la figura 3.13 se puede apreciar la serie Cisco 3750.

Fuente: http://www.cisco.com

Figura 3.13 Serie Cisco 3750

Otras características de importancia se mencionan a continuación:

- La serie Cisco 3750 tiene funcionalidades capa 2 y capa 3.
- 128 MB de DRAM y 16 MB de memoria FLASH.
- Enrutamiento IP unicast estático RIP[81].
- Enrutamiento OSPF, IGRP[82], BGPv4 y IS-ISv4.
- Enrutamiento IPv6 (OSPF y EIGRP[83]).
- Soporta MPLS y Servicios Diferenciados (DiffServ).

En la tabla 3.4 se resaltan las particularidades de los modelos utilizados por MEGADATOS.

---

[81] **RIP** Routing Information Protocol
[82] **IGRP** Interior Gateway Routing Protocol
[83] **EIGRP** Enhanced Interior Gateway Routing Protocol

PRODUCTO	PUERTOS	CARACTERÍSTICAS
WS-C3750G-24T	24 puertos Ethernet 10/100/1000	Controla LANs inalámbricas ofreciendo claras políticas de seguridad con un sistema inalámbrico de prevención de intrusiones.
WS-C3750-24TS	24 puertos Ethernet 10/100 y dos enlaces ascendentes (uplinks) SFP[84].	Configuración de hasta 11000 rutas unicast. Configuración de hasta 1000 grupos IGMP[85] y rutas de multidifusión. Una unidad de rack.
WS-C3750-24TS-1U	24 puertos Ethernet 10/100/1000, 4 uplinks SPF.	

Tabla 3.4 Productos de la serie 3750

3.3.4 SERIE CISCO CATALYST 3550

Es una serie apilable, proporciona alta disponibilidad, seguridad y Calidad de Servicio. Posee velocidades de puerto Fast Ethernet y Gigabit Ethernet, su funcionalidad permite utilizarlo para la capa de acceso, para armarios de cableado o como un conmutador de red troncal para redes pequeñas, en la figura 3.14 se presenta un gráfico de la serie Cisco 3550.

Fuente: http://www.cisco.com

Figura 3.14 Serie Cisco 3550

[84]**SPF** Small Form-Factor Pluggable
[85]**IGMP** Internet Group Management Protocol

Entre los servicios inteligentes que brinda están: QoS avanzada (configuración automática), ACL, gestión multicast y alto rendimiento de enrutamiento IP, manteniendo la sencillez de las redes LAN. Entre las características de rendimiento de enrutamiento están:

- Switch con funcionalidades de capa 2 y capa 3.
- Cisco Express Forwarding (CEF), tecnología de conmutación avanzada.
- 64 MB de memoria DRAM y 16 MB de memoria Flash.
- Soporte unicast y multicast.
- Enrutamiento IP unicast (RIP v1 y RIP v2)
- Enrutamiento IP avanzado unicast (OSPF, IGRP, EIGRP, BGPv4)
- Servicios Diferenciados y MPLS.

En la tabla 3.5 se incluyen las características particulares de cada uno de los modelos.

PRODUCTO	PUERTOS	CARACTERÍSTICAS
WS-C3550-12G	10 puertos Gigabit Interface Converter (GBIC) 1000BASE-X y dos puertos 10/100/1000BASE-T.	Ancho de banda máximo de envío de 12Gbps. Tasa de reenvío de paquetes de 64 bytes de 17Mpps. Configuración de hasta 12000 direcciones MAC, 24000 rutas unicast y 8000 rutas multicast.
WS-C3550-24	24 puertos 10/100BASE-T y dos puertos (GBIC).	Ancho de banda máximo de envío de 4.4 Gbps. Tasa de reenvío de paquetes de 64 bytes de 6.6 Mpps. Configuración de hasta 8000 direcciones MAC, 16000 rutas unicast y 2000 rutas multicast.

Tabla 3.5 Productos de la serie 3550

3.3.5 SERIE CISCO CATALYST 3560

El modelo de switch utilizado por MEGADATOS de esta serie es el WS-C3560-24TS el cual permite desplegar aplicaciones tales como: telefonía IP, wireless, video vigilancia y servicios

inteligentes para la gestión como QoS avanzada (automática), Listas de Control de Acceso y un alto rendimiento de enrutamiento IP, en la figura 3.15 se puede apreciar el switch WS-C3560-24TS.

Fuente: http://www.cisco.com

Figura 3.15 Switch WS-C3560-24TS

En la serie 3560 la agregación de ancho de banda puede ser de hasta 8 Gbps a través de la tecnología Gigabit EtherChannel y hasta 8 Mbps con la tecnología Cisco Fast EtherChannel.

Otras características más relevantes de este modelo son:

- Switch multicapa con 24 puertos Ethernet de 10/100 Mbps y 2 puertos SPF (Small Form-Factor Pluggable).
- Enrutamiento IPv6 unicast y multicast.
- Soporte de protocolos de enrutamiento como OSPFv3, EIGRPv6, IS-ISv4 y BGPv4.
- Configuración de hasta 1024 VLANs.
- 128 MB de memoria DRAM y 32 MB de memoria Flash.
- Soporta DiffServ y MPLS.

3.3.6 SERIE CISCO CATALYST 6506

El switch Cisco Catalyst 6506 provee funcionalidades de Triple Play, servicios y características para una red convergente brindando interfaces WAN, ATM y SONET, ideal para servicios a través de una red Metro Ethernet. Este switch es un sistema modular que puede crecer conforme a los requerimientos del proveedor y la evolución de la tecnología para añadir nuevas funciones y un rendimiento mejorado con la adición de nuevos módulos en el mismo chasis como por ejemplo: módulos de interfaz Ethernet, de interfaz WAN, etc.

El switch de MEGADATOS además utiliza un módulo de funcionalidad conocido como Super Engine 720, permitiendo a este switch ser más escalable ya que ofrece más aplicaciones tanto para capa 2 y capa 3 con un rendimiento de hasta 720 Gbps.

A continuación se detallan las características del Catalyst 6506 que es utilizado para la interconectividad del núcleo y Data Center de la empresa.

- Tiene 6 ranuras de chasis y provee servicios inteligentes como: protección Firewall Gigabit, Sistema de Detección de Intrusos.
- Proporciona MPLS para los servicios de VPN, Ingeniería de Tráfico y despliegue de Metro Ethernet.
- QoS para la capa 2 y capa 3 a través de la limitación de la velocidad y tráfico.
- Permite la integración de módulos Ethernet: 10/100 Mbps, 10/100/1000 Mbps, 100BASE-FX, Gigabit Ethernet (GBIC) y 10 Gigabit Ethernet.
- Conectividad a través de interfaces PSTN: T1/E1 y FXS (Foreing exchange-Station).
- Puede servir de apoyo para ofrecer servicios de pasarela de voz a teléfonos tradicionales, fax, PBX[86] y PSTN.
- Soporte de los protocolos BGPv4, PPP sobre SONET, RIPv1, RIPv2, OSPF, RSVP, LDP (Label Distribution Protocol).

En la figura 3.16 se muestra una gráfica del switch Cisco Catalyst de la serie 6506.

Fuente: http://www.cisco.com

Figura 3.16 Switch Cisco 6506

[86]**PBX** Private Branch Exchange

3.3.7 ROUTER CISCO DE LA SERIE 7600

El Cisco 7606-S es un router de alto rendimiento que permite a los proveedores de servicios de Telecomunicaciones desplegar una infraestructura de red avanzada con el soporte de servicios Triple-Play tanto a nivel residencial como corporativo, cumpliendo con requisitos de redundancia, alta disponibilidad y densidad de rack. Este router se encuentra ubicado en el Telepuerto UIO de Quito realizando las funciones de borde con los enlaces de los carriers y de enrutamiento hacia los nodos. Las características más importantes de este router son las siguientes:

- Tiene 6 ranuras de chasis, puertos Ethernet de 10/100Mbps, Gigabit Ethernet y 10 Gigabit Ethernet.
- Operatividad LAN/WAN, ATM y acceso Metro Ethernet.
- Servicios de seguridad como: IPSec, Firewall, denegación de servicio distribuido y Sistemas de Detección de Intrusos, ACLs, QoS (con la configuración de políticas propias del proveedor).
- Plataforma de enrutamiento con visión IP NGN, servicios de IP/MPLS.
- Tasa de reenvío distribuido de 240 Mpps y rendimiento total de 480 Gbps.
- IPv6 unicast y multicast.
- VLAN, Protocolo Spanning Tree y VPNs de capa 2 y capa 3.

En la figura 3.17 se muestra un gráfico del router Cisco 7606.

Fuente: http://www.cisco.com

Figura 3.17 Router Cisco 7606

3.3.8 ROUTER CISCO 3845

El Cisco 3845 es un router que brinda servicios integrados de datos, voz, video, seguridad y servicios inalámbricos. Esta plataforma es adecuada para la implementación de telefonía IP con una capacidad de procesamiento desde 240 teléfonos que puede ser más alta con la implementación de módulos o tarjetas con interfaces para voz. Al ser capaz de ofrecer servicios inalámbricos es posible desplegar toda una infraestructura de red inalámbrica con la incorporación de WICs (WAN Interface Card) o tarjetas de interfaz WAN. En la figura 3.18 se presenta un gráfico del router Cisco 3845.

Fuente: http://www.cisco.com

Figura 3.18 Router Cisco 3845

A continuación se mencionan las características más relevantes del router Cisco 3845:

- Proporciona un alto rendimiento de hasta T3/E3[87].
- Integra IP, QoS, wireless y conectividad entre redes (PSTN, WAN e Internet).
- Tiene dos puertos LAN Gigabit Ethernet, un slot SFP, cuatro NMEs (Network Modules), cuatro HWICs (High-Speed WIC), dos slots AIM (Advanced Integration Module), 4 slots PVDM (Packet Voice DSP Module) y un EVM-HDS (Extension Voice Module).
- Proporciona servicios avanzados de seguridad para VPN con IPSec, AES[88], DES[89] y MPLS y soporta hasta 2500 túneles VPN.
- Con los módulos PVDM soporta voz analógica, voz digital, conferencia, voz sobre Frame Relay, voz sobre ATM (incluyendo AAL5 y AAL2).

---

[87] **T3/E3** 45Mbps/43Mbps
[88] **AES** Advanced Encryption Standard
[89] **DES** Data Encryption Standard

- Utiliza protocolos para el control de los paquetes de voz como H.323, MGCP (Media Gateway Control Protocol) y SIP (Session Initial Protocol).

3.3.9 ROUTER CISCO 3745

Es un router de acceso multiservicio, son modulares para la flexibilidad y escalabilidad de las redes. Ofrecen una solución integrada de seguridad, telefonía IP, correo de voz, video, datos y servicios inteligentes como: QoS, IP multicast, VPN, Firewall, Prevención de Intrusiones y control de admisión de llamadas, todas estas cualidades sin sacrificar su rendimiento en la red.

Otras características adicionales del router Cisco 3745 se nombran a continuación:

- Hasta 256 MB de memoria SDRAM y hasta 128 MB de memoria Flash.
- Tiene dos puertos de 10/100 Mbps, dos slots para módulos AIM (Advanced Integration Module), tres tarjetas de interfaz WAN y dos HDSM (High Density Service Module).
- Soporte para las principales tecnologías WAN: Frame Relay, ATM y XDSL.
- Con un módulo AIM de compresión de datos gestiona el ancho de banda con una relación de 4:1, cada AIM soporta 4T1/E1 que puede llegar hasta 8T1/E1.
- También posee un AIM para el cifrado de datos, para el caso del 3745 es el AIM-VPN/HP que admite 1800 túneles con velocidades de hasta 90 Mbps.

En la figura 3.19 se muestra gráficamente al router Cisco 3745.

Fuente: http://www.cisco.com

Figura 3.19 Router Cisco 3745

3.3.10 CISCO AS 5300

El Cisco AS 5300 es un servidor de acceso remoto telefónico y un gateway de voz sobre IP, con la implementación de tarjetas de función de voz y la activación del software de voz. El software IOS ofrece mecanismos altos de Calidad de Servicio, tamaño de tramas variables y control basado en el estándar H.323 admitiendo un conjunto de códecs estandarizados (G.711, G.729, G.729a y G.723.1). Su implementación en una red ofrece la posibilidad de incorporar servicios de larga distancia mediante la adición de puertos e interfaces Primary Rate Interface (PRI), T1 o E1 con la red PSTN y un gatekeeper para servir a varios gateways además el AS 5300 puede funcionar con gatekeepers de otros proveedores.

Para la gestión se utiliza una aplicación basada en web CVM (Cisco Voice Manager) para la configuración, monitorización de los gateways de voz sobre IP y creación de informes como historial de llamadas, informe de volumen de llamadas e informes de excepción de calidad de voz, esta aplicación de java se ejecuta en Windows NT o Solaris. Esta aplicación facilita que los administradores de red puedan implementar planes de acceso telefónico, controlar los parámetros y calidad de las llamadas en tiempo real. En la figura 3.20 se muestra gráficamente al gateway de voz Cisco AS 5300.

Fuente: http://www.cisco.com

Figura 3.20 Cisco AS 5300

Otras características adicionales del Cisco AS 5300 son las siguientes:

- Además de los servicios de VoIP admite servicios de fax sobre IP.

- Aplicación IVR (Interactive Voice Response) que incluye indicativos de voz y un conjunto de dígitos para autenticar al usuario e identificar el destino de las llamadas además de la interconectividad con los RADIUS.
- El gateway Cisco AS 5300 de voz puede aceptar más tarjetas de función de voz/fax, por lo que puede ampliarse las conexiones de voz/fax en un solo chasis.
- Incluye los protocolos RSVP (Resource Reservation Protocol) y QoS.
- Interoperabilidad con el Cisco 3600 y 2600 (funcionalidad gatekeeper).
- Compatible con los teléfonos, faxes, centralitas y sistemas centrales existentes proporcionando una interfaz estándar sin la necesidad de realizar una adaptación para los usuarios.
- Puede utilizar RSVP para solicitar el ancho de banda necesario para una llamada.

En la tabla 3.6 se muestran algunas especificaciones técnicas del Cisco AS 5300.

	CARACTERÍSTICAS
Tipo de procesador	R4700 a 150 MHz
Memoria	64 MB DRAM
Memoria flash	16 MB de memoria Flash de sistema, en uno o dos bancos, hasta 16 MB de memoria Flash de inicio
Ranuras del chasis	Tres
Ethernet (RJ-45)	Dos (una de 10 Mbps y otra de 10/100 Mbps)
Puertos de voz, fax	Hasta 96 (T1) ó 120 (E1)
Módems de 56k	Un máximo de 48 (T1) ó 60 (E1) modems cuando se instalan 48 (T1) ó 60 (E1) puertos de voz
ISDN PRI, T1 o E1	Admite PRI Q.931 y señalización asociada a canales

Tabla 3.6 Especificaciones técnicas del Cisco AS 5300

3.4 CAPACIDAD ACTUAL DE LA RED

Para conocer la capacidad actual de la red se toma la información proporcionada por la empresa, esta información muestra la capacidad de cada uno de los nodos primarios en cada una de las ciudades, en donde se concentra el tráfico. Estos datos son obtenidos utilizando una aplicación basada en Java denominada NetEnforcer que permite monitorear el ancho de banda creando informes históricos que dan la facilidad de planificar la capacidad y gestión de los recursos.

Los nodos primarios que conforman la ciudad de Quito son: Fundación, Torrezul, CCNU, Autofrancia y Foch, los que concentran el tráfico de las diferentes localidades de la urbe. En la tabla 3.7 se muestra el ancho de banda de la red de Quito generado por los usuarios, esta información corresponde a la estadística que lleva la empresa.

NODO	CAPACIDAD (Mbps)
FUNDACIÓN	38,59
TORREZUL	11,52
AUTOFRANCIA	19,20
CCNU	23,68
FOCH	21,76
TOTAL	114,75

Tabla 3.7 Tráfico generado en la red de Quito

Como se puede apreciar en la tabla 3.7 en la red de Quito se tiene un consumo de 114,75 Mbps, de los cuales 80,6 Mbps son utilizados actualmente para transmisiones de datos y 34,15 Mbps para las aplicaciones de Internet, según la información proporcionada por la empresa.

De la misma manera la capacidad actual de los nodos primarios de la ciudad de Guayaquil se muestra en la tabla 3.8.

NODO	CAPACIDAD (Mbps)
TORRES DEL NORTE	36,21
SAN FRANCISCO	31,36
ORO VERDE	14,72
WTC	21,02
TOTAL	103,31

Tabla 3.8 Tráfico generado en la red de Guayaquil

La capacidad actual de la ciudad de Guayaquil es de 103,31 Mbps como se presenta en la tabla 3.8 de los cuales el 68,47 % del tráfico corresponde a la transmisión de datos es decir 70,74 Mbps y el 31,53 % a las aplicaciones de Internet equivalente a 32,57 Mbps.

El nodo de concentración de la red de Cuenca es Rayoloma. En la tabla 3.9 se puede observar la capacidad actual de este nodo conforme a los datos llevados por la empresa.

NODO	CAPACIDAD (Mbps)
RAYOLOMA	40,56
TOTAL	40,56

Tabla 3.9 Tráfico generado por la red de Cuenca

De acuerdo a la información, el 33 % de esta capacidad es para la transmisión de datos es decir 13,38 Mbps y el 67 % corresponde a las aplicaciones de Internet, es decir 27,18 Mbps.

De lo revisado anteriormente la capacidad actual del backbone es la siguiente:

Capacidad Total= Capacidad Quito+ Capacidad Guayaquil+ Capacidad Cuenca

Capacidad Total= 114,75+ 103,31+ 40,56 [Mbps]

Capacidad Total= 258,62 [Mbps]

CAPÍTULO 3

3.5 ANÁLISIS FODA DE LA EMPRESA ECUANET-MEGADATOS

Este análisis se obtuvo de la convivencia con el personal técnico de la empresa y del sondeo a los clientes asistidos técnicamente, el resultado refleja la situación global de Ecuanet-MEGADATOS en la actualidad y permitirá desarrollar la propuesta de diseño de la red de backbone con MPLS en el siguiente capítulo tomando en cuenta los aspectos positivos que la empresa tiene a su favor.

3.5.1 FORTALEZAS

- Presencia comercial y técnica en la mayor parte del país.
- Diferentes soluciones tecnológicas tanto para usuarios residenciales como para corporativos.
- Los servicios de Telecomunicaciones son competitivos en costo y calidad en el mercado ecuatoriano.
- Alto nivel profesional y técnico.
- Experiencia de 16 años en el mercado de las Telecomunicaciones
- La empresa cuenta con la certificación ISO 9001:2000 a la gestión de calidad, lo que la posiciona como líder en satisfacción al cliente dentro del país.
- La infraestructura y servicios están amparados dentro del marco legal que exige la Superintendencia de Telecomunicaciones como Portadores e Internet.

3.5.2 OPORTUNIDADES

- La implementación de nuevas tecnologías posibilita mayores prestaciones y nuevos productos para los clientes.
- Las alianzas estratégicas con diferentes Portadores permite llegar con los servicios hacia donde los clientes lo requieran.
- Son muy pocas las empresas de Telecomunicaciones y en especial las de datos que tengan implementado en sus redes troncales MPLS con la visión de ofrecer paquetes de servicios de voz, video y datos.

- Al contar con una red de backbone con MPLS se puede administrar y gestionar la red con la incorporación de técnicas de Ingeniería de Tráfico, ofrecer servicios de VPN y flexibilidad para el soporte de tecnologías subyacentes al transporte de datos, permitiendo además migrar la red actual a una red NGN (Next Generation Network).
- Al incorporar tecnologías con estándares internacionales posibilita ofrecer a los usuarios aplicaciones con Calidad de Servicio.

3.5.3 DEBILIDADES

- La dependencia de infraestructura con otras empresas de Telecomunicaciones refleja las falencias de las mismas como propias de MEGADATOS hacia los clientes.
- Manejo inadecuado del marketing y publicidad para atraer a nuevos clientes.
- El cuerpo profesional de la empresa y en especial el talento humano del NOC no se enfocan al desarrollo constante de proyectos para su ejecución.
- La situación económica del país no ofrece la seguridad necesaria para que las empresas de Telecomunicaciones inviertan en la implementación de tecnologías ya que las aplicaciones y servicios pueden no ser aceptados por los usuarios debido a los costos que pueden representar.
- La resistencia al cambio tecnológico no solamente de los clientes sino también de una parte del personal dentro de la empresa.

3.5.4 AMENAZAS

- Existen empresas a nivel nacional que han planificado su migración a nuevas tecnologías para la prestación de servicios Triple-Play por lo que la competitividad está presente.
- El desarrollo de la tecnología móvil abarca aplicaciones que pueden ser preferidas por los usuarios.
- La competencia está constantemente desarrollando estrategias para la reducción de los costos de los servicios e incremento de valores agregados.

- Dentro del marco legal de las Telecomunicaciones en el país no existen lineamientos específicos en cuanto a la provisión de servicios Triple-Play.
- Otras empresas al contar con infraestructura de transporte propia sumada la implementación de nuevas tecnologías se encuentran en la posición de liderar el mercado ecuatoriano.

3.6 REQUERIMIENTOS DE LA RED DE BACKBONE

Con lo detallado en el análisis FODA, es evidente que se deben aprovechar las fortalezas y oportunidades que tiene la empresa en el mercado ecuatoriano y uno de sus aspectos positivos es la presencia a nivel nacional con un número aproximado de 17.000 usuarios entre residenciales y corporativos los cuales podrían ser clientes asegurados en cuanto a la provisión de servicios Triple Play sin mencionar los nuevos usuarios que se puede atraer en el futuro. En la tabla 3.10 se muestra una estadística del incremento de clientes que presenta MEGADATOS desde el año 2005 hasta el presente.

AÑOS	SERVICIOS PORTADORES	SERVICIOS DE VALOR AGREGADO
2005	491	2157
2006	471	6441
2007	498	7809
2008	571	12422
2009	916	15320
2010	923	16186

Fuente: http://www.supertel.gov.ec

Tabla 3.10 Crecimiento del número de usuarios desde el 2005 a 2010

En la figura 3.21 se puede apreciar gráficamente el crecimiento de los abonados por año tanto para servicios portadores como para los servicios de valor agregado.

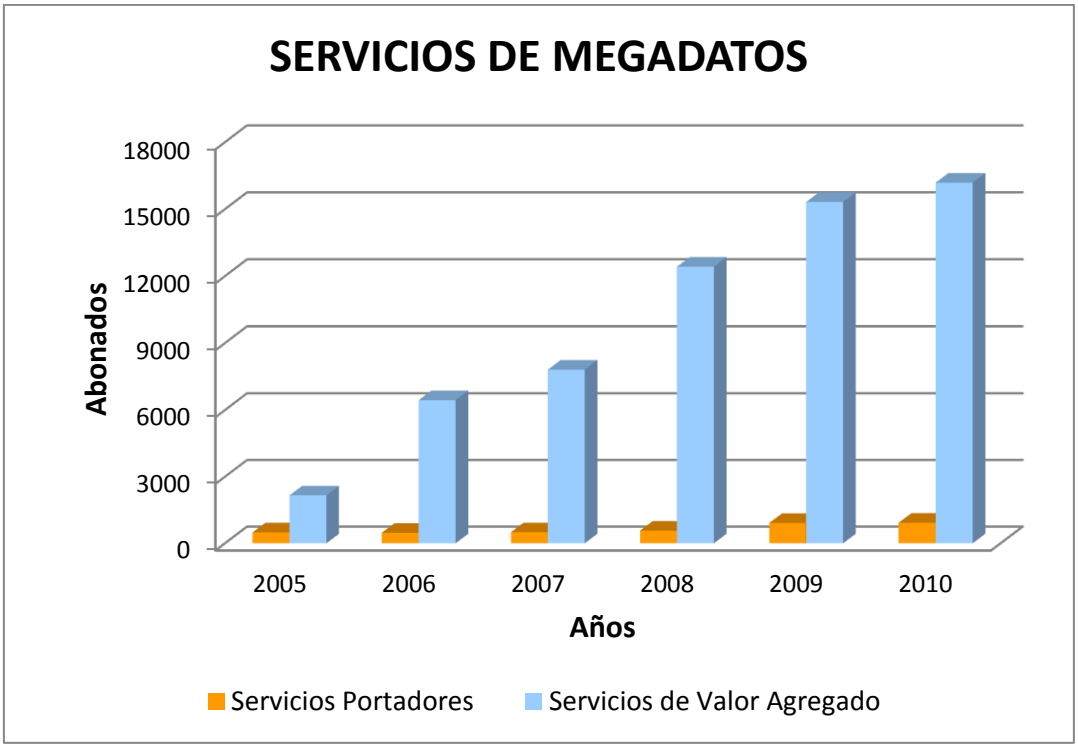
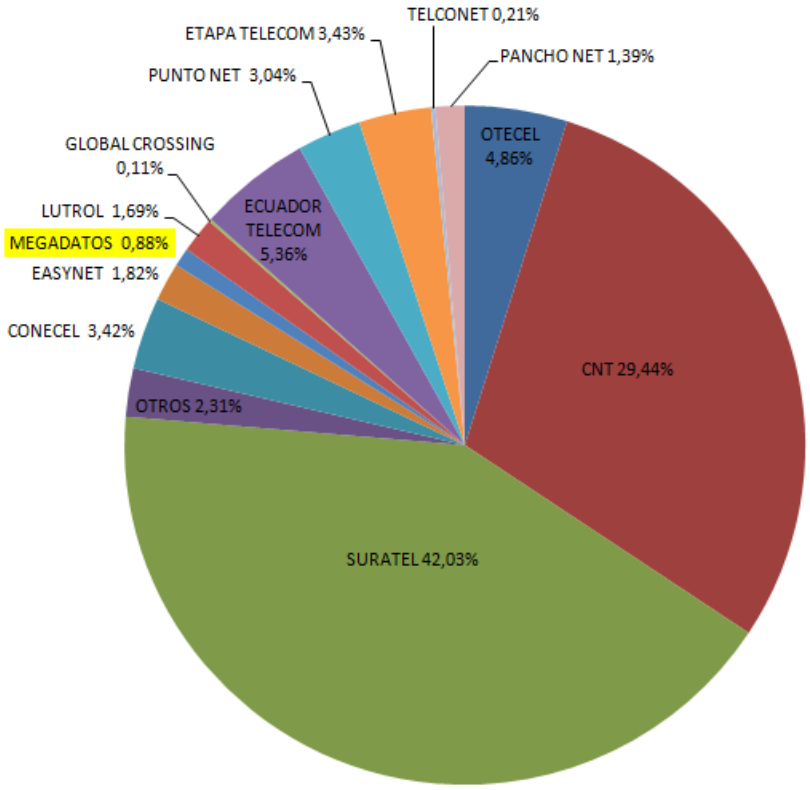


Figura 3.21 Estadísticas de crecimiento de MEGADATOS

Dadas las exigencias y la tendencia de los usuarios a la contratación de servicios innovadores, de bajo costo y alta calidad, la empresa tiene que redefinir en el futuro inmediato la infraestructura del backbone actual conservando en lo posible las tecnologías desplegadas hasta el momento para que el costo inicial no sea excesivo y así mantenerse y crecer competitivamente en el país con servicios nuevos que estén al alcance de los usuarios.

A continuación en la figura 3.22 se muestra en porcentaje el número de usuarios que tiene MEGADATOS con relación a otros permisionarios del país.



Fuente: http://www.supertel.gov.ec

Figura 3.22 Cuentas de Internet por Permisionario en porcentaje

Como se observa en la figura 3.22 MEGADATOS abarca el 0,88% de los usuarios del 1.840.678 que tienen cuentas de Internet y servicios de valor agregado a nivel nacional y para permanecer competitivo en el mercado de las Telecomunicaciones la empresa debe crecer por medio de la oferta de servicios innovadores con nuevas tecnologías. El diseño de red de backbone que se propone además de soportar las exigencias actuales debe permitir a futuro extender su capacidad y su cobertura para satisfacer la demanda de los usuarios, esta red debe brindar soporte de Calidad de Servicio o el modelo de Servicios Diferenciados que son posibles con la implementación de MPLS, lo que además permite priorizar el tráfico de las aplicaciones de tiempo real de acuerdo a las políticas acordadas por la empresa y los clientes.

Para cubrir la capacidad requerida la empresa debe ampliar sus enlaces con los diferentes proveedores e implementar más equipos que soporten la tecnología MPLS con grandes

capacidades de rendimiento a nivel de core puesto que el Triple Play requiere de un importante ancho de banda que puede llegar hasta los 20 Mbps según el número de aplicaciones que requiera el usuario, este ancho de banda debe ser optimizado por la empresa para no saturar los canales y abastecer tanto a clientes actuales como a futuros clientes.

Con el backbone soportado en MPLS hay aplicaciones que se pueden realizar para mejorar los servicios e implementar otros como por ejemplo la Ingeniería de Tráfico y VPN/MPLS. Con la Ingeniería de Tráfico los administradores de la red de la empresa pueden realizar el balanceo de cargas en el interior del core al no centrar en un único punto todo el tráfico de las aplicaciones y con las VPN basadas en MPLS se eliminan los inconvenientes de los PVC (Path Virtual Circuit) y túneles IP dando paso a la conectividad mediante rutas virtuales mucho más seguras y a precios razonables.

CAPÍTULO 4. DISEÑO DE LA RED DE BACKBONE CON MPLS

4.1 INTRODUCCIÓN

En el entorno competitivo en el que se desarrollan las empresas de Telecomunicaciones domina la importancia de las tecnologías de redes implementadas y desplegadas a lo largo de su cobertura para ofrecer a sus usuarios los servicios requeridos de la manera más óptima, por una parte para incrementar los ingresos y por otra para permanecer activos en este mercado con la visión de estar latentes a esa gran evolución tecnológica que es la integración de los servicios sobre una sola infraestructura de red que como base del núcleo está la implementación de MPLS.

El propósito de este capítulo es el diseño de la red de backbone entre los nodos principales de MEGADATOS en Quito, Guayaquil y Cuenca con la tecnología MPLS considerando la red desplegada en la actualidad. Este diseño incluye la topología, selección de equipos tomando en cuenta los requerimientos técnicos y económicos, protocolos de enrutamiento, ventajas de la empresa con la nueva red y finalmente la simulación del backbone MPLS en software.

4.2 CONSIDERACIONES INICIALES PARA EL DISEÑO DE LA RED

El buen funcionamiento y éxito de una red depende de la disposición en capas, basadas en modelos jerárquicos, para aprovechar las ventajas de modularidad a medida en que la red crece. Para el caso de una red de backbone es necesario asignar tareas específicas a los dispositivos de conmutación y enrutamiento para tener la diferenciación entre el acceso, borde y núcleo para operar y mantener a la red multiservicio.

La asignación de las tareas a los equipos de conmutación y enrutamiento se basa específicamente en la división de las funciones de concentración y de backbone.

A continuación se indican las tareas que deben cumplir los equipos del núcleo:

1. **Equipos de concentración:** Los switches o routers de concentración proporcionan el acceso de los clientes a la red ya sea con enlaces compartidos o dedicados. Estos equipos tienden a soportar números elevados de puertos y deben ofrecer prestaciones adicionales como ACLs y QoS además son utilizados también en el borde de la red.

   Las características de estos equipos son:

   - Escalabilidad y alto ancho de banda para el soporte de nuevas aplicaciones.
   - Alta densidad de puertos para satisfacer el crecimiento del número de clientes.
   - Procesador optimizado para gestionar agregaciones de tráfico de gran volumen y nuevas funcionalidades de software.
   - Prestaciones adicionales al enrutamiento de paquetes de alta velocidad: Redes Privadas Virtuales, seguridad con Listas de Acceso extendidas, Firewalls, Calidad de Servicio y soporte multicast.

2. **Equipos de backbone:**
   Deben proporcionar el transporte eficaz entre los nodos de la red mediante el envío de paquetes a gran velocidad de un dominio a otro con el objeto de alcanzar las mayores tasas de transmisión sobre las interfaces más rápidas y disponibles, conmutando los paquetes tan rápido como sea posible, estos equipos deben ser de alta velocidad y gran rendimiento.

   Los equipos de backbone no necesitan conocer las redes individuales del nivel de acceso, ésta función la realizan los routers o switches de concentración que luego de conocer los destinos y sumarizar las rutas las anuncian a los routers de backbone.

Al distribuir a los equipos en funciones de concentración o de backbone la configuración de los routers de core puede permanecer estable y no verse afectada cuando se añaden o eliminan

clientes individuales de los routers de concentración, o cuando clientes individuales contratan servicios de valor agregado.

Otras de las consideraciones iniciales es la topología de la red a diseñar, la ideal sería aquella que brinde alta conectividad entre todos los dispositivos de red, una red mallada, que si en verdad tiene muchas ventajas los costos de administración y mantenimiento hacen desistir a las empresas de Telecomunicaciones. En la práctica la topología más flexible es la de estrella en la que cada nodo se enlaza con los proveedores de tránsito con la facilidad de ir mallando la red en función de la utilización de los enlaces y las necesidades cambiantes de los clientes.

Además se deben tener habilitados enlaces redundantes y sobredimensionados para proteger a la red frente a la caída o saturación de los enlaces principales y hacer frente al crecimiento del tráfico para soportar los requerimientos más exigentes.

4.3 PLANTEAMIENTO DEL DISEÑO DE RED

Se propone un diseño de red de backbone lo suficientemente escalable y flexible con una alta capacidad de transporte utilizando en la medida de lo posible la infraestructura actual de MEGADATOS con la finalidad de ofrecer mayores prestaciones como:

- Redundancia de los enlaces principales para aumentar la disponibilidad de la red y tolerancia a fallas.
- Alta capacidad de transporte para el soporte de servicios de voz, datos y video.
- Posibilidad de ofrecer servicios de VPN sobre MPLS para la transmisión de servicios Triple Play.
- Garantizar el crecimiento futuro, el diseño de red utiliza equipos que soportan IPv6 para facilitar la expansión de la red.
- La red brindará Calidad de Servicio y Servicios Diferenciados para mantener niveles de servicio según la aplicación requerida.
- Supervisión de red única la que permite disminuir costos de operación y mantenimiento.

Estas son las características que cumplirá la red de backbone con MPLS en base al tipo de tecnología desplegada actualmente que es una red Gigabit Ethernet, en cuanto a la provisión de servicios Triple Play se realiza el estudio de implementación para IPTV y VoIP en conjunto con las propuestas de equipos a utilizar.

4.4 DESARROLLO DEL DISEÑO

Se pretende realizar un diseño de backbone sobre la red Gigabit Ethernet del nodo principal de MEGADATOS con la tecnología MPLS que lo integra con Guayaquil y Cuenca realizando una proyección futura de la red y de los clientes. La red Gigabit Ethernet de la empresa trabaja con el protocolo IP y fue diseñada para ofrecer ciertos Acuerdos de Nivel de Servicio contratados según los requerimientos de los clientes basándose en la transmisión de paquetes con el mejor esfuerzo sin ofrecer QoS, lo que se puede mejorar con la implementación de MPLS.

Actualmente las capacidades de transmisión contratadas al carrier para los nodos de Quito y Guayaquil es de 155 Mbps y para la ciudad de Cuenca es de 50 Mbps, debido al tráfico actual generado por los usuarios, con lo que el nuevo backbone debe superar estas capacidades e inclusive debe estar diseñado para soportar capacidades futuras para satisfacer el crecimiento de la demanda.

4.4.1 REQUERIMIENTOS DE ANCHO DE BANDA PARA TRIPLE PLAY

Para ofrecer servicios Triple Play el ancho de banda necesario se detalla a continuación:

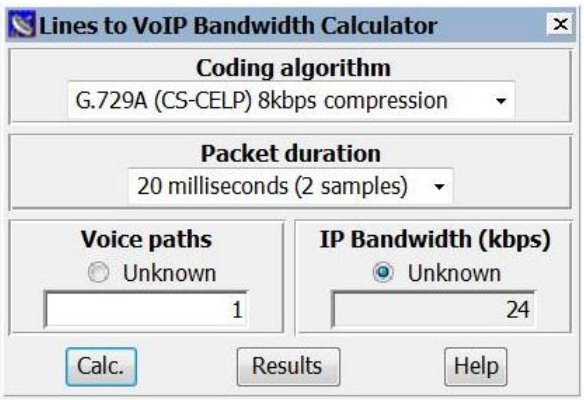
- **Video:** IPTV se basa en el estándar DVB IPI (Digital Video Broadcast IP Infraestructure) que determina a MPEG-4[90] como el formato de compresión de las señales de video, éste define una tasa de bits no inferior a 1Mbps (cantidad de datos para representar óptimamente una señal de video) que puede variar dependiendo de la calidad de video y puede ser mayor. El ancho de banda requerido para un canal SDTV[91] está entre 1 y 2 Mbps, en base al formato MPEG-4 y la calidad de video

[90] **MPEG-4** Moving Picture Experts Group 4
[91] **SDTV** Standard Definition Television

mientras que un canal HDTV[92] ocupa un ancho de banda entre 7 y 8 Mbps, utilizando también MPEG-4 pero su calidad de video es superior. [13]

- **Internet:** Como se mencionó anteriormente la capacidad necesaria únicamente para la transmisión de video debe ser mayor a 1 Mbps, a esta capacidad hay que añadirle el ancho de banda para la conexión a Internet que como mínimo se requiere de 1Mbps para el soporte de otras aplicaciones de nueva generación que requieren tasas de acceso altas. Además este ancho de banda debe ser mayor a las bases requeridas ya que la conexión de acceso debe soportar múltiples canales de video simultáneo ya que se parte de la idea de que en cada hogar hay un promedio de 2 receptores, por esta razón se toma dos flujos de video para un plan básico.

- **Voz:** Se propone utilizar el estándar G.729, en el que se basa la VoIP, que define una velocidad de transmisión de 8kbps con la menor tasa de bits y permite ahorro de ancho de banda del canal. Para un circuito de voz se utiliza la calculadora web que resuelve los ancho de banda IP en función del número de enlaces, este caso para un circuito de voz es necesario 24kbps y se muestra en la figura 4.1.



Fuente: http://www.erlang.com/calculator/lipb

Figura 4.1 Calculadora Erlang

[92]**HDTV** High Definition Television

A continuación en la tabla 4.1 se indican los requerimientos para un plan básico de Triple Play que consta de dos canales SDTV cada uno ocupando una capacidad de 2 Mbps o la segunda opción que consta de un canal SDTV (2 Mbps) y un canal HDTV (8Mbps).

SERVICIO	IPTV	INTERNET	VoIP	TOTAL
2 canales SDTV	4 Mbps	1 Mbps	0,024 Mbps	5,024 Mbps
1 canal SDTV+1 canal HDTV	2 Mbps+8Mbps	1 Mbps	0,024 Mbps	11,024 Mbps

Tabla 4.1 Plan básico de Triple Play

Como se muestra en la tabla 4.1 el ancho de banda requerido para un plan básico que ofrece dos canales SDTV es de 5, 024 Mbps pero si el usuario desea un paquete en el que incluye 1 canal SDTV y 1 HDTV el ancho de banda mínimo es de 11, 024 Mbps, de lo cual el valor promedio de ancho de banda para un usuario residencial es de 8,024 Mbps.

Para clientes corporativos con requerimientos más exigentes la proyección se muestra en la tabla 4.2, este plan ofrece un canal HDTV (8 Mbps) y 3 canales SDTV que pueden ser de 1 o 2 Mbps cada uno, según la elección del usuario.

SERVICIO	ANCHO DE BANDA	CAPACIDAD REQUERIDA
1 HDTV	8 Mbps	8 Mbps (1 Señal)
1 SDTV	1 – 2 Mbps	3 – 6 Mbps (3 Señales simultáneas)
Internet Alta Velocidad	2 Mbps	2 Mbps
VoIP	24 kbps	1.5 Mbps (varias líneas simultáneas)
	TOTAL	14.5 – 17.5 Mbps

Fuente: http://www.acta.es/articulos_mf/43039.pdf

Tabla 4.2 Ancho de banda para requerimientos más exigentes

Como se muestra en la tabla 4.2 si el cliente solicita dentro de su plan 3 canales SDTV de 1 Mbps cada uno, el ancho de banda requerido es de 14,5 Mbps caso contrario si solicita 3 canales SDTV de 2 Mbps el ancho de banda sería de 17,5 Mbps. Para dimensionar la capacidad del backbone se tomará como referente el valor promedio que resulta 16 Mbps para un usuario corporativo.

4.4.2 COBERTURA DE LA RED

La empresa desde un inicio ha decidido implementar nuevas tecnologías en las ciudades más importantes y productivas del país como son: Quito, Guayaquil y Cuenca, en una primera fase.

Es por ello que los nodos principales de MEGADATOS se encuentran ubicados en estas ciudades y dan cobertura a toda la provincia inclusive a otras aledañas, además estas provincias registran la mayor cantidad de habitantes que acceden a Internet y a servicios de valor agregado como se muestra en la tabla 4.3.

PROVINCIAS	Porcentaje de habitantes que acceden a Internet
Pichincha	32.46 %
Guayas	16.48 %
Azuay	12.03 %

Fuente: http://www.supertel.gov.ec

Tabla 4.3 Provincias con el mayor número de usuarios que acceden a Internet

4.4.3 TOPOLOGÍA Y ELEMENTOS

La red de backbone propuesta se conforma de tres zonas, cada una con un nodo principal en Quito, Guayaquil y Cuenca, con el objetivo de distribuir el ancho de banda, cuenta con rutas alternas en el caso de la saturación del enlace; por ejemplo si se desea transmitir información desde el nodo Quito al nodo Cuenca, la primera ruta es Quito – Cuenca y la ruta alterna sería Quito – Guayaquil – Cuenca. En la figura 4.2 se observa la topología y elementos de red utilizados para la implementación de MPLS a nivel de core.

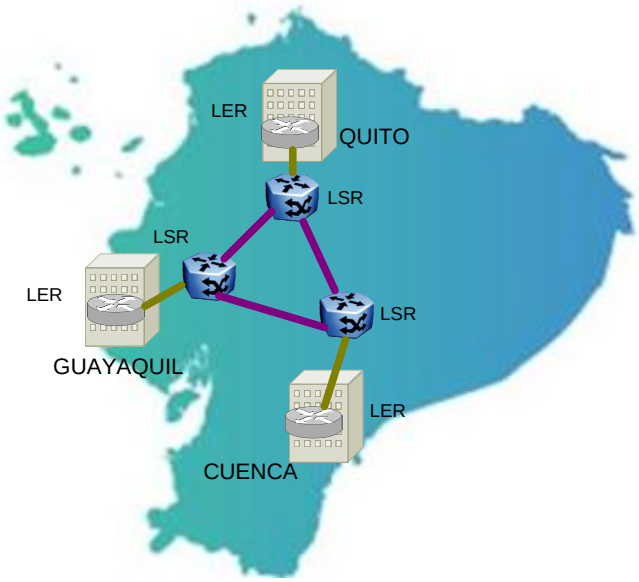


Figura 4.2 Esquema Topológico del Backbone MPLS

Se escoge esta topología conformada de tres routers LER de borde, cada uno en una ciudad (Quito, Guayaquil y Cuenca), porque la proyección inicial de la empresa es cubrir 50 demandas en el 50% de los nodos de distribución. Este criterio en el que se basó la empresa MEGADATOS se debe a que la red actual está limitada a la capacidad de la red de transporte del Carrier y dadas las condiciones tecnológicas del país hasta el momento son escasos los carriers que ofrezcan más capacidad de transporte y beneficios que TELCONET. Habría que esperar que en el corto o mediano plazo con la baja de los precios de Internet y que el avance tecnológico en el país mejore para generalizar los servicios Triple Play a toda la infraestructura actual de MEGADATOS.

Con la proyección inicial se cubren 5 nodos en Quito, 2 en Guayaquil y uno en Cuenca con lo que la demanda inicial bordea las 500. Los nodos de distribución que se escogieron son los puntos estratégicos más concurridos en estas ciudades y se muestran en la tabla 4.4.

CIUDAD	NODO
QUITO	FUNDACIÓN
	TORREZUL
	CCNU
	AUTOFRANCIA
	FOCH
GUAYAQUIL	TORRES DEL NORTE
	SAN FRANCISCO
CUENCA	RAYOLOMA

Tabla 4.4 Nodos de Distribución

4.4.3.1 Interconectividad del Backbone MPLS

La red propuesta mostrada en la figura 4.2 forma un dominio MPLS en el que los LER representan la salida del dominio y están situados al borde de los nodos de las ciudades de

Quito, Guayaquil y Cuenca además el centro de conmutación está formado por tres LSRs que se ubican en las ciudades respectivamente.

El transporte del tráfico entre estas ciudades como se mencionó en el capítulo tres, la empresa utiliza infraestructura de Transnexa, para este diseño y por las alianzas estratégicas desarrolladas en los últimos meses con la empresa TELCONET se propone utilizar su infraestructura para los enlaces con Guayaquil y Cuenca ya que implementar el backbone por completo resulta una inversión muy alta.

La capacidad para el enlace de Guayaquil y Cuenca debe ser a 1Gbps y para la ciudad de Quito a 10 Gbps (por tener mayor número de nodos de distribución), capacidad necesaria para cubrir con la demanda inicial planificada por la empresa. El carrier ofrece transporte a estas tres ciudades con nodos intermedios y con sus respectivos backups, utilizando fibra óptica monomodo de 12 hilos en tendido aéreo de los cuales dos hilos son necesarios para el transporte del tráfico de MEGADATOS. En la figura 4.3 se detalla el backbone MPLS y los elementos que intervienen como los LSP (Label Switched Paths) que utilizarán la red de transporte del carrier para conmutar el tráfico a cada uno de los destinos.

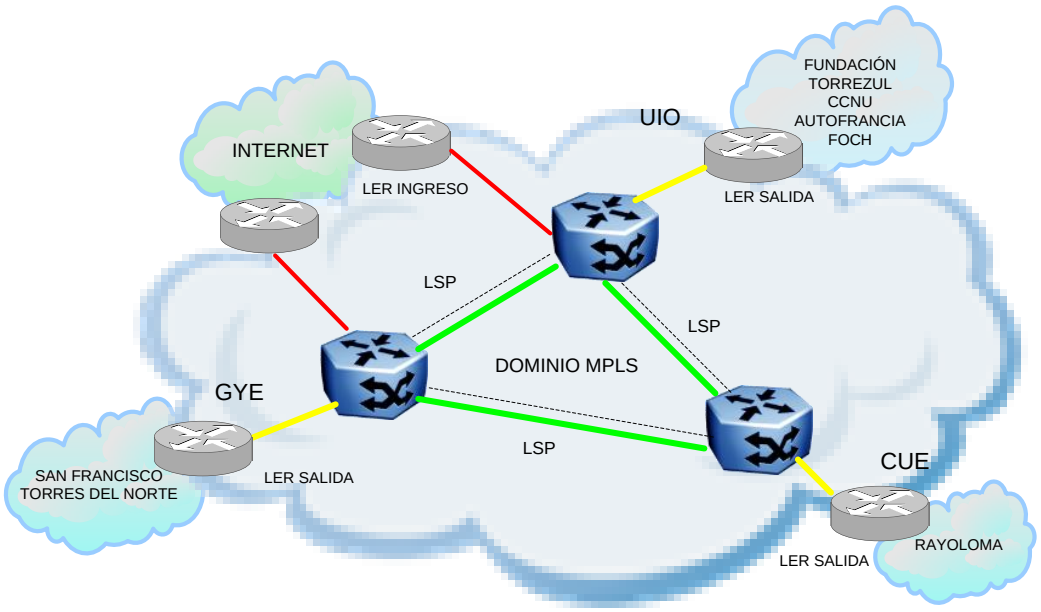


Figura 4.3 Diagrama detallado del Backbone MPLS

Adicional a la implementación puramente en el core, los routers de borde LER se interconectarán a los nodos de distribución de la tabla 4.4 y finalmente a los de acceso que son los encargados de repartir el servicio a los usuarios. Los nodos de distribución de las tres ciudades deben equiparse con switches adecuados para la transmisión de video en formato IP y VoIP, se propone en este diseño los Cisco Catalyst 3750, que se interconectarán al backbone.

4.4.4 DIMENSIONAMIENTO DEL BACKBONE MPLS

Para el soporte de servicios Triple Play y sobre todo por el requerimiento de ancho de banda de las aplicaciones de video la propuesta de la capacidad del backbone MPLS requiere de un incremento inicial en el Core de 10 Gbps y 1 Gbps en los nodos de distribución en base a los requerimientos analizados en la tabla 4.2 tomando un valor promedio de ancho de banda de los servicios Triple Play de 16 Mbps para usuarios corporativos, capacidad que será directamente distribuida desde los nodos de MEGADATOS.

De esta manera para la ciudad de Quito se tiene:

Capacidad de un nodo de distribución= 50 usuarios x 16 Mbps= 800 Mbps

Capacidad del nodo de Quito= 5 nodos x 800Mbps= 4 Gbps

En la ciudad de Guayaquil se dará cobertura a 2 nodos de distribución: Torres del Norte y San Francisco y la capacidad del nodo de esta ciudad será:

Capacidad de un nodo de distribución= 50 usuarios x 16 Mbps= 800 Mbps

Capacidad del nodo de Guayaquil= 2 nodos x 800 Mbps= 1,6 Gbps

Para la ciudad de Cuenca al tener un solo nodo de distribución la capacidad será de:

Capacidad de un nodo de distribución= 50 usuarios x 16 Mbps= 800Mbps

Capacidad del nodo de Cuenca= 1 nodos x 800Mbps= 800 Mbps

CAPÍTULO 4

La capacidad total del backbone MPLS es la siguiente:

Ci= Capacidad Quito+ Capacidad Guayaquil+ Capacidad Cuenca
Ci= 4,0+ 1,6 + 0,8 [Gbps]
Ci= 6,4 Gbps

Como se observa la capacidad inicial del backbone MPLS será de 6,4 Gbps considerando las condiciones presentadas y para conocer el tiempo en el que la capacidad del backbone sobrepasaría los 10 Gbps se utiliza la siguiente ecuación de crecimiento geométrico:

$$Cf = Ci\ (1 + x)^n \qquad (4.1)$$

Donde:

Cf = Capacidad estimada en *n* años
Ci = Capacidad inicial
x = Índice de crecimiento anual del servicio de Telecomunicaciones
n = Tiempo de proyección en años

El índice de crecimiento anual de MEGADATOS es del 21% según las estadísticas presentadas a nivel nacional. [31]

Reemplazando los valores conocidos en la ecuación 4.1 se obtiene:

$$10\ Gbps = 6{,}4\ Gbps(1 + 0{,}21)^n$$

$$\frac{10Gbps}{6{,}4\ Gbps} = (1 + 0{,}21)^n$$

$$log\frac{10}{6{,}4} = log(1 + 0{,}21)^n$$

$$nlog(1 + 0{,}21) = \log(10) - \log(6{,}4)$$

$$n = \frac{1 - \log(6{,}4)}{\log(1{,}21)} = 2{,}3 \text{ años}$$

En la tabla 4.5 se presentan los valores del ancho de banda requeridos acorde al crecimiento anual de la empresa para satisfacer la demanda de Triple Play dentro de los primeros cinco años.

TIEMPO (años)	CAPACIDAD MÍNIMA REQUERIDA (Gbps)	INDICE DE CRECIMIENTO (%)
1	7.74	21
2	9,37	21
3	11,33	21
4	13,71	21
5	16.60	21

Tabla 4.5 Proyección de la capacidad del Backbone en los primeros cinco años

Como se observa en la tabla 4.5 se estima aproximadamente que después de 2 años la capacidad del backbone MPLS sobrepasaría los 10 Gbps si se mantiene constante el índice de crecimiento anual de la empresa con lo que a partir del tercer año se debe incrementar la capacidad a unos 20 Gbps en el core.

En el caso de los usuarios ADSL para Triple Play se propone también destinar una capacidad de 1Gbps para la distribución de estos servicios, al ser usuarios residenciales el requerimiento de ancho de banda promedio es de 8 Mbps con lo que se cubriría una demanda aproximada de 200 usuarios inicialmente y la capacidad total del backbone en el primer año sería de 7,74 Gbps como lo indica la tabla 4.5.

4.4.5 SELECCIÓN DE EQUIPOS DE CORE

Para realizar el diseño del backbone MPLS que soporte servicios Triple Play se ha considerado en lo posible mantener los equipos de red actuales e implementar solamente los equipos necesarios para que trabajen como LSR y LER.

A partir del diseño propuesto en la sección 4.4.3 se mencionan las características más importantes que deben cumplir los equipos de backbone para un mejor rendimiento de la red y se presentan tres alternativas para establecer una comparación y seleccionar la mejor.

4.4.5.1 Requerimientos de los equipos LSR

Entre los requerimientos más importantes que deben cumplir los equipos con funcionalidad de LSR son las que se indican a continuación:

- Soporte de MPLS y funcionalidad de VPN.
- Interfaces Gigabit Ethernet y fibra óptica.
- Modulares para la escalabilidad de la red.
- Soporte de protocolos de capa 2 como VLAN Trunk Protocol (VTP), IEEE 802.1q.
- Soporte de protocolos de enrutamiento como OSPF, IS-IS, BGPv4 y soporte de IPv6.
- Al ser una tecnología abierta estos equipos deben soportar cualquier protocolo de señalización como RSVP o LDP.

En la tabla 4.6 se presentan tres propuestas de fabricantes con los requerimientos más importantes.

CARACTERÍSTICAS	Cisco Catalyst 6506	Alcatel 7710 SR- c12	3COM MSR 30-40 Mult-Service Router
			
Soporte MPLS	Si	Si	Si
Protocolos de Señalización MPLS	RSVP, LDP, RSVP-TE.	RSVP-TE, LDP.	RSTP, DLDP.
MPLS/VPN	Si	Si	Si
Velocidad de reenvío	400 Mpps en IPv4 Hasta 200 Mpps en IPv6	350 Mpps en IPv4 y hasta 150 Mpps en IPv6	240 Mpps en IPv6
QoS en el core MPLS	Si	Si	Si
Protocolos de enrutamiento	OSPF, IS-IS, EIGRP, RIP, BGP.	OSPF, BGP, IS-IS, RIP.	RIP, OSPF, BGP,IS-IS
Velocidad de Backplane	720 Gbps	320 Gbps	80 Gbps
Numero de VRF	1024	1024	No soporta VRF
Bases de Información Gestionada MIB	MPLS MIB LDP, LSR MIB, MIB MPLS-TE, MPLS VPN MIB.	MPLS LSR MIB, MPLS-TE MIB, MPLS LDP MIB.	MPLS MIB, LDP, MIB, LSR MIB.
Apilamiento MPLS	Si	Si	No
Rutas	256.000	64.000	64.000
COSTO	**4.067 USD**	**6.330 USD**	**2.119 USD**

Tabla 4.6 Comparación de equipos con funcionalidad LSR de diferentes fabricantes

Las características de los equipos de la tabla 4.6 con respecto a la tecnología MPLS son similares y para el diseño del backbone se selecciona al switch Cisco Catalyst 6506 debido a que soporta mayor número de protocolos de señalización, mayor velocidad de backplane, apilamiento de etiquetas y mayor velocidad de reenvío a diferencia de los otros dos fabricantes, además ofrece flexibilidad y escalabilidad para la creciente demanda de usuarios y servicios, otra ventaja de su utilización se debe a que la empresa cuenta con uno de estos equipos en el nodo de Quito por lo que solo conviene adquirir dos switches: uno para Guayaquil y otro para Cuenca.

4.4.5.2 Requerimientos de los equipos LER

Los equipos que desempeñan la funcionalidad de LER deben cumplir con los siguientes requisitos:

- Interfaces Gigabit Ethernet y fibra óptica.
- Soportar MPLS, VRF (VPN Routing and Forwarding) y Qos.
- Protocolos de enrutamiento principalmente OSPF, IS-IS, BGP, IGMP y multidifusión.
- Soportar MPLS/VPNs.
- Flexibilidad en módulos para cubrir las futuras demandas.

En la tabla 4.7 se presentan tres propuestas de fabricantes.

CARACTERÍSTICAS	**Router Cisco 7206 VXR/NPE-G2**	**3COM Router 6080**	**Juniper J-4350-JB-DC-N**
Descripción General			
	Posee 1GB de memoria SDRAM y 256 MB de memoria FLASH. Entre sus características más importantes están:	Funcionalidades de núcleo y borde proporcionando conectividad WAN. Tiene una unidad de	Diseño modular, soporte DHCP, limitación de tráfico, 1 GB (instalados) / 2 GB (máx.), 256 MB (instalados) / 1 GB (máx.),

	control de flujo, soporte de DHCP, compresión, cifrado y gestión de tráfico (QoS).	montaje en rack equipada con ocho ranuras para tarjetas de interfaz.	prevención contra ataque de DoS (denegación de servicio), filtrado de contenido.
Puertos	Interfaces flexibles y modulares para la agregación de tráfico: OC-3, Gigabit Ethernet, DS3, Fast Ethernet y Ethernet.	10/100/1000 puertos Ethernet modular con SPF, un puerto serial auxiliar.	Ethernet, Fast Ethernet, Gigabit Ethernet, X.21, V.35.
Protocolos	H.323, SIP, IPv6, EIGRP, IGRP, IS-IS, OSPF, BGP, PIM e IPv6.	OSPF, RIP v1/v2, IS-IS, BGP-4, IPv6 y PIM.	OSPF, IS-IS, RIP-2, BGP, PIM, IGMP, OSPF e IPV6.
MPLS	MPLS VPN, QoS MPLS, MPLS TE.	IP/MPLS, MPLS QoS y MPLS-TE.	VPN MPLS, MPLS QoS y MPLS TE.
VRF	Hasta 2000 VRF	No soporta VRF	No soporta VRF
COSTO	**17.800 USD**	**9.400 USD**	**7.200 USD**

Tabla 4.7 Comparación de equipos con funcionalidad LER de distintos fabricantes

De la tabla 4.7 y en base a los requerimientos principales que deben cumplir los equipos para trabajar como LER se elige al router Cisco 7206 VXR por soportar mayor número de protocolos de enrutamiento, más características para MPLS, mayor rendimiento, protocolos para redes NGN y escalabilidad por ser un router modular. Además viene equipado con el NPE-G2 (Network Processing Engine) que permite funcionalidades superiores a las de los otros equipos ya que soporta las aplicaciones de voz, video y datos permitiendo la configuración de DiffServ y aplicar al tráfico para brindar la Calidad de Servicio con velocidades de envío muy altas.

4.4.6 IMPLEMENTACIÓN A NIVEL DE OTRAS CAPAS

Para ofrecer los servicios Triple Play además de incorporar la tecnología MPLS e incrementar la capacidad del backbone es necesario realizar otras implementaciones tanto a nivel de capas superiores como capas inferiores para ofrecer los servicios de voz y video.

4.4.6.1 Servicios de VoIP e Interconexión con la red PSTN

En este diseño de red se propone el mismo mecanismo de ruteo e interconexión con CNT a través del Gateway de voz AS 5300 como actualmente se realiza para ofrecer los servicios de VoIP a los usuarios corporativos. El nodo de Quito actualmente cuenta con un AS 5300 por lo que es necesario incrementar tarjetas modulares de voz/fax para la cobertura inicial, mientras que para las ciudades de Guayaquil y Cuenca se deben adquirir dos gateways más, se considera este gateway por que es apilable y crece modularmente conforme crece la demanda mediante la adición de las tarjetas modulares.

En la figura 4.4 se puede apreciar la escalabilidad y flexibilidad que presenta una solución Cisco AS 5300 de clase portadora denominándose AccessPath VS3 que podría tener hasta 2.520 Interfaces T1/E1 digitales.

Fuente: http://www.cisco.com

Figura 4.4 Solución apilable del AS 5300

En cuanto a la interoperabilidad, Cisco también ha introducido el soporte para el protocolo Open Settlements Protocol, un estándar que se está desarrollando para facilitar el intercambio de tráfico de VoIP entre operadores de redes.

Para cubrir la demanda de los servicios de voz inicialmente no es viable la adquisición del Softswitch, ya que una solución económica entre servidor y software están alrededor de unos 40.000 USD y durante los dos primeros años esta implementación no sería aprovechada al 100% de su capacidad. En la figura 4.5 se presenta un esquema general de la interconexión para los servicios de voz.

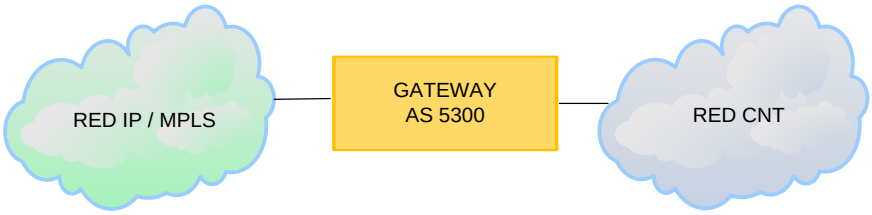


Figura 4.5 Interconexión de la red IP/MPLS con CNT

En cuanto a la provisión de servicios de voz para los usuarios ADSL el tráfico generado se dirige a un MSAG o gateway multiservicio (posibilita el enrutamiento Triple Play) el cual enruta al softswitch en caso de una llamada convencional o la dirige al ruteador de borde de MEGADATOS si se trata de clientes corporativos con VoIP.

4.4.6.1.1 Establecimiento de una llamada

Si el cliente realiza una llamada, se ejecutan los siguientes pasos:

1. El cliente descuelga el teléfono y marca el número de teléfono del destinatario. Esta llamada le llega al Media Gateway (AS 5300 o MSAG).

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

3. El Softswicth busca en su base de datos el número de teléfono del destinatario para saber su dirección IP y 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 sesión RTP (Real Time Protocol) cuando el usuario descuelga y se inicia la conversación.

4.4.6.1.2 Cisco Voice Manager

Es una aplicación para la gestión de la redes de VoIP basada en web que permite la configuración y monitoreo de los gateways de voz de Cisco. Con esta herramienta los administradores pueden implementar planes de acceso telefónico, control de los parámetros y calidad de las llamadas en tiempo real.

El AS 5300 ofrece un completo conjunto de variables SNMP (Simple Network Management Protocol), MIB (Management Information Base) generales y específicas de voz. El Cisco Voice Manager detecta automáticamente los productos con soporte para voz y es ideal para gestionar un máximo de 50 gateways en redes grandes, medianas o pequeñas.

4.4.6.2 Plataforma de video y contenido

Para la implementación de una plataforma de video y contenido se va a adoptar el modelo "Operador de servicios de video", consiste en que el operador de la red despliega la infraestructura necesaria para proveer el servicio más no la generación del contenido.

Dentro de la plataforma de video se encuentran equipos para adquirir, procesar, codificar y administrar el contenido de video que luego será distribuido por el backbone MPLS y posteriormente encaminado hacia el usuario final.

En el capítulo 1 se describe más detalladamente el procedimiento para la implementación de la plataforma IPTV por lo que en esta sección se dará a conocer los equipos necesarios a partir del esquema que se muestra en la figura 4.6.

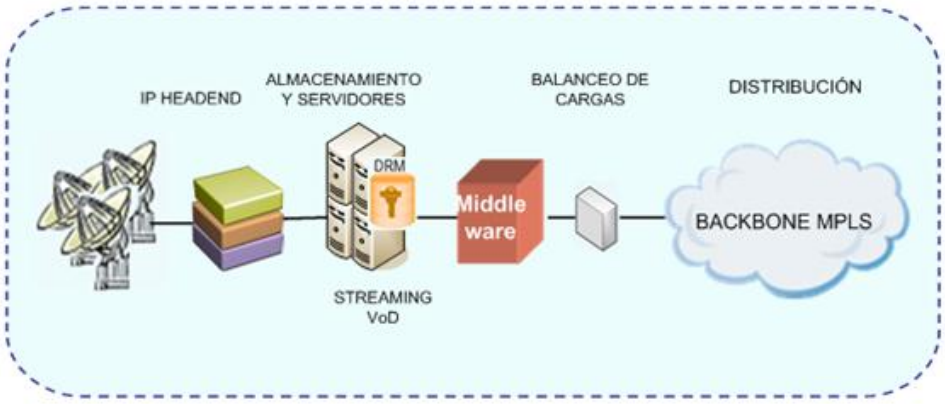


Figura 4.6 Esquema general de la Plataforma de Video y Contenido

En la implementación del IP HEADEND se utilizará la solución de Cisco mientras que los servidores de streaming y de VoD son de la casa comercial MatrixStream. Las dos casas comerciales ofrecen una solución integrada en cuanto al IP HEADEND y servidores por ésta razón resulta más conveniente implementar estos equipos para no tener dificultad de operatividad con las redes existentes.

1. **ADQUISICIÓN DE VIDEO** (Recepción y Decodificación)

   Para el diseño se ha seleccionado el modelo D9854, una unidad versátil para la recepción de señales satelitales de distribución y tiene las siguientes características:

   - Decodificación de alta calidad para todos los estándares de emisión de video.
   - Ideal para la distribución primaria, el seguimiento de video o de re-codificación de aplicaciones.
   - Demodulación DVB-S[93], QPSK[94] y DVB-S2 QPSK/8PSK[95].
   - Permite la migración de las redes de DVB-S a DVB-S2 y SD a HD.
   - Soporta MPEG 2 o MPEG 4 AVC HD.
   - Salidas digitales para distribución y salidas analógicas HD o SD.

---

[93] **DVB-S** Digital Video Broadcasting by Satellite
[94] **QPSK** Quadrature Phase-Shift Keying
[95] **8PSK** 8 Phase Shift Keying

- Utiliza SNMP para la configuración, control y vigilancia mediante el panel LCD frontal.
- Perfil ultra delgado de 1U para el montaje en el rack.
- Resolución de 720x480, 30 fps en NTSC[96] y 720x576, 25 fps, en PAL[97].

La figura 4.7 muestra el gráfico de un receptor-decodificador Cisco D9854.

Fuente: http://www.cisco.com

Figura 4.7 Modelo D9854 de Cisco

2. PROCESADOR DE VIDEO

El DCM (Digital Content Manager), modelo D9900 MPEG es una plataforma compacta con capacidad de procesamiento masivo y puede trabajar con miles de secuencias de video simultáneamente incluyendo la inserción de programas digitales.

Este dispositivo proporciona la funcionalidad tanto en definición estándar (SD) y alta definición (HD) y capacidades avanzadas como la admisión de aplicaciones de video de próxima generación incluyendo la carta de servicios digitales, el programa local, inserción de publicidad, herramientas para el proceso de video más eficaces y ahorro del ancho de banda.

A continuación se presentan características adicionales del DCM:

- Plataforma capaz de procesar un número elevado de flujos de video MPEG.
- Perfil 2U para montaje en rack y fuentes de alimentación redundantes.
- Configuración de hasta cuatro tarjetas I/O, cada tarjeta con más de diez puertos ASI[98] o cuatro puertos Gigabit Ethernet.

---

[96]**NTSC** National Television System Committee
[97]**PAL** Phase Alternating Line
[98]**ASI** Asynchronous Serial Interface

- Unicast y soporte Multicast además de los protocolos: Ethernet, VLAN, RTP, UDP, IP, modelo DiffServ, etc.
- Puede equiparse con tarjetas VSB-8[99] para recibir simultáneamente hasta 8 canales RF.
- La administración se la realiza por medio de SNMP, gestión ROSA, control mediante navegador web, los dos últimos por interfaz Ethernet con el sistema de gestión.

La figura 4.8 muestra el gráfico del Procesador de Video DCM D9900 MPEG.

Fuente: http://www.cisco.com

Figura 4.8 DCM D9900 MPEG

3. CODIFICADOR DE VIDEO

Para este diseño se ha seleccionado el Video Encoder de Cisco D9036 que ofrece servicios de video IP con alta calidad, importante ahorro de ancho de banda, soporte de audio integrado, enrutamiento de video y audio ya que posee un conjunto de codificadores y multiplexores en una sola unidad. Acepta las señales SD (Standard Definition) y HD (High Definition) y las codifica en tiempo real a MPEG-2 o MPEG-4 simultáneamente.

---

[99] **VSB-8** Vestigial Sideband Level 8

A continuación se presentan las características más importantes:

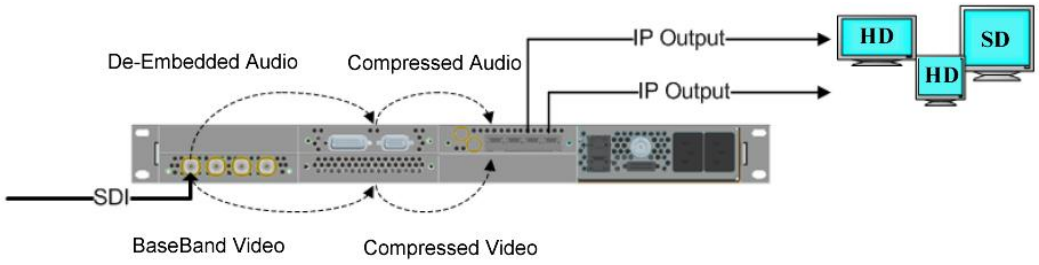
- Perfil delgado de 1U para montaje en rack.
- Hasta 6 módulos: para entradas, codificación de audio y salidas de video.
- Codifica hasta 8 canales SD o 4 canales HD, pudiéndose extender hasta 16 SD o 8HD.
- El módulo de video soporta SD/MPEG-2, SD/MPEG-4, HD/MPEG-2 o HD/MPEG-4 /AVC (H.264).
- La configuración se la realiza a través de una GUI basada en web o a través del software de gestión de Cisco (ROSA).
- Posee cuatro puertos Ethernet de 100/1000BaseT.

La figura 4.9 muestra un gráfico del codificador D9036.

Fuente: http://www.cisco.com

Figura 4.9 Video Encoder D9036

Además la tecnología de codificación es altamente programable, lo que permite mayores avances en la calidad de video permitiendo una conversión de HD a SD, según las solicitudes del usuario. La figura 4.10 muestra las interfaces disponibles para la conversión de HD a SD.



Fuente: http://www.cisco.com

Figura 4.10 Conversión de HD a SD

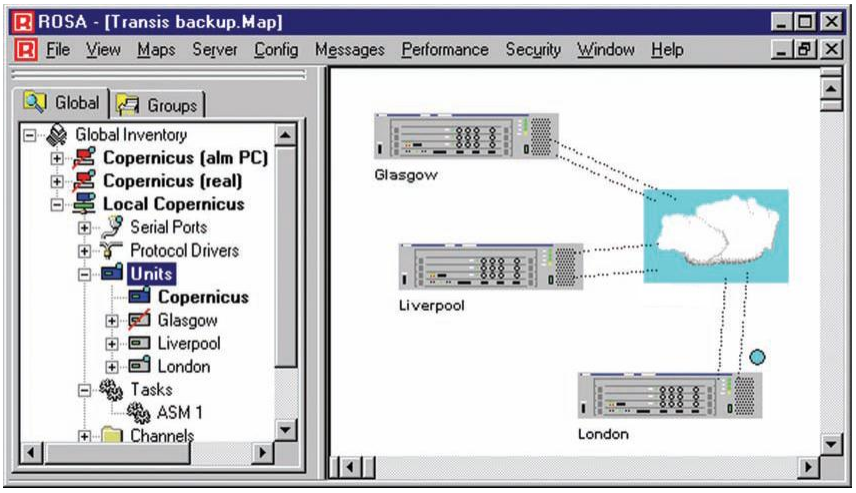
4. VIDEO MANAGEMENT

Es una herramienta que permite monitorear remotamente todos los elementos de la red, incluyendo la plataforma de distribución de video, Middleware y STBs, integrando también la gestión remota para resolución de incidencias y actualización de versiones.

Se propone la adquisición del Sistema de Administración de Cabeceras de CISCO conocido como ROSA y sus características principales son las siguientes:

- Actúa como un Proxy SNMP.
- Envía notificaciones mediante alarmas cuando se produce algún problema.
- Activa automáticamente dispositivos de backup.
- Informes de ejecución, tendencias de la disponibilidad y rendimiento de red.
- Escalabilidad para crecer junto con la oferta de IPTV, incluyendo soporte para más de 725 dispositivos a través de SNMP y protocolos propietarios.
- Gestión de seguridad mediante diferentes niveles de acceso.
- Arquitectura abierta de software que abarca prácticamente todos los aspectos de la red y gestión de elementos.

La figura 4.11 muestra la interfaz gráfica del Sistema de Administración de red ROSA.



Fuente: http://www.cisco.com

Figura 4.11 Sistema de Administración de red ROSA

5. SERVIDOR DE STREAMING

Un servidor de streaming es un dispositivo que maneja flujos de datos para reproducir contenidos multimedia sin necesidad que el usuario descargue todo el archivo para visualizarlo en tiempo real.

Para el diseño se propone el Servidor Streaming IMX i2410 Live TV MatrixCast y tiene las siguientes características:

- Diseñado para aplicaciones de TV en vivo.
- Puede soportar simultáneamente hasta 1000 flujos SD por servidor.
- Compatible con tarjetas SD y HD con resoluciones 720p, 1080i y 1080p.
- Ofrece calidad de servicio para HD a 2Mbps y para SD a solo 750 Kbps.
- Puede trabajar con cualquier codificador de video MPEG-4/AVC (H.264).

La figura 4.12 muestra un gráfico del Servidor Streaming IMX i2410.

Fuente: http://www.matrixstream.com

Figura 4.12 Servidor Streaming IMX i2410

6. SERVIDOR VoD y MIDDLEWARE

En la tabla 4.8 se presentan las características del servidor VoD IMX v2420 y del Middleware IMX M500 del fabricante MatrixStream.

PRODUCTO	CARACTERÍSTICAS
SERVIDOR VoD  **IMX v2420 MatrixCast**	• Servidor de alta capacidad con tecnología robusta y escalable. • Soporta unicast y multicast hasta 1000 flujos de video. • Formato de almacenamiento (MPEG-2 o MPEG-4) • Compatible con tarjetas SD y HD con una resolución de 720p, 1080i y 1080p.
SERVIDOR MIDDLEWARE  **IMX M500**	• Equipamiento para la distribución de servicios e interfaces al usuario final permitiendo ofrecer diferentes opciones con servicios básicos y avanzados. • Permite hasta 600 IPTV espectadores en esta modalidad. • Soporta transmisión de video a la carta con el Servidor IMX v2420 VoD. • Gestión de usuarios y contenidos. • Brinda seguimiento estadístico del usuario.

Tabla 4.8 Características del Servidor VoD y Middleware de MatrixStream

4.4.6.3 Acceso del terminal

La empresa tiene dos segmentos de mercado como se ha mencionado anteriormente, un sector corporativo (empresas e instituciones) y residenciales (hogares y pequeños negocios) los cuales acceden a la red por diferentes tecnologías y en este diseño se propone su utilización ya que cumplen con los requerimientos.

4.4.6.3.1 Acceso de Banda Ancha ADSL

El acceso de los usuarios residenciales para los servicios Triple Play mantendrán la tecnología ADSL ya que cumple con los requisitos necesarios para la transmisión, una conexión ADSL2+ puede llegar a ser mayor a 20Mbps pero para ofrecer planes básicos diseñados para este segmento de mercado el ancho de banda requerido no sobrepasa los 12 Mbps en caso de solicitar señales HDTV caso contrario es necesario 5 o 6 Mbps, con lo que si se cubriría la demanda.

La empresa entrega módems ADSL TP-LINK TD-8811, TD-8817 y módems HUAWEI MT882 entre los más comunes, éstos si cumplen con los requerimientos para servicios Triple Play en especial para los planes básicos.

Además del módem ADSL2+ se utilizará un STB para la recepción y decodificación de las señales de Televisión Digital permitiendo que el flujo de video sea transportado por IP y se enlace al módem ADSL2+ por medio de un puerto Ethernet como se muestra en la figura 4.13.

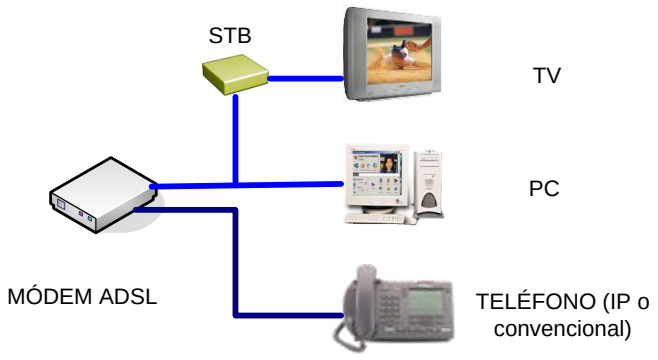


Figura 4.13 Acceso de usuarios residenciales

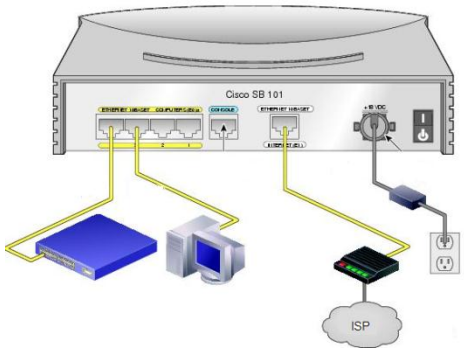
4.4.6.3.2 Interconexión al Nodo de Distribución por Fibra Óptica

Para ofrecer los servicios Triple Play a los usuarios corporativos en las ciudades que cubre el backbone MPLS, éstos se conectarán a través de una acometida de fibra óptica que interconecta a los nodos de acceso y distribución (en su mayoría son Switch Catalyst Cisco 3550) y posteriormente el tráfico generado es enrutado a los LER.

Utilizando un transceiver de fibra óptica a UTP se conecta al respectivo equipo final del cliente el cual provee el servicio de Internet y puede ser conectado a un Set top Box para el servicio de Televisión. Para el diseño se propone la utilización del router Cisco SB 101 para el acceso del usuario y presenta las siguientes características:

- Está diseñado para la transmisión de voz, video y datos operando con seguridad y flexibilidad.
- Soporta VLANs y VPNs.
- Posee 4 interfaces Ethernet de 10/100 Mbps, puerto de consola RJ-45.
- Tiene 64 MB de memoria DRAM y 12MB de memoria Flash.
- Soporta DHCP, Listas de Control de Acceso (ACL) y protocolos de enrutamiento.

En la figura 4.14 se muestran las características físicas del router Cisco SB 101.



Fuente: http://www.cisco.com

Figura 4.14 Router Cisco SB 101

CAPÍTULO 4

Para la visualización de los servicios de video los usuarios deben utilizar un STB (Set-Top Box) para la traducción de la información de las señales televisivas a IP, en este diseño se propone la adquisición del MediaPro IP3000SD/HD de la casa comercial Eagle Broadband y tiene las siguientes especificaciones:

- El MediaPro IP3000SD/HD es un IP Set-Top Box diseñado para satisfacer las necesidades residenciales y empresariales.
- Tiene menús fáciles y legibles de manejar para los usuarios y flexibilidad para soportar una variedad de sistemas Middleware.
- Utiliza formatos MPEG-2 y MPEG-4 AVC (H.264).
- Soporta WMV9[100] sobre MPEG-2, streaming y VoD.
- En cuanto a la seguridad de la recepción del contenido lo hace por medio de CA (Conditional Access) y DRM (Digital Rights Management).
- Posee puertos Ethernet de 10/100Mbps, USB, HDMI[101] y otros.
- Tiene capacidades para SD de hasta 8Mbps y para HD de hasta 30 Mbps.

La figura 4.15 muestra un gráfico del STB a utilizar en el diseño de la red.

Fuente: http://www.eaglebroadband.com

Figura 4.15 Set Top Box MediaPro IP3000SD/HD

[100]**WMV9** Windows Media Video 9
[101]**HDMI** High-Definition Multimedia Interface

Finalmente en la figura 4.16 se muestra la red de backbone MPLS para la distribución de servicios Triple Play a usuarios corporativos y residenciales con el equipamiento necesario.

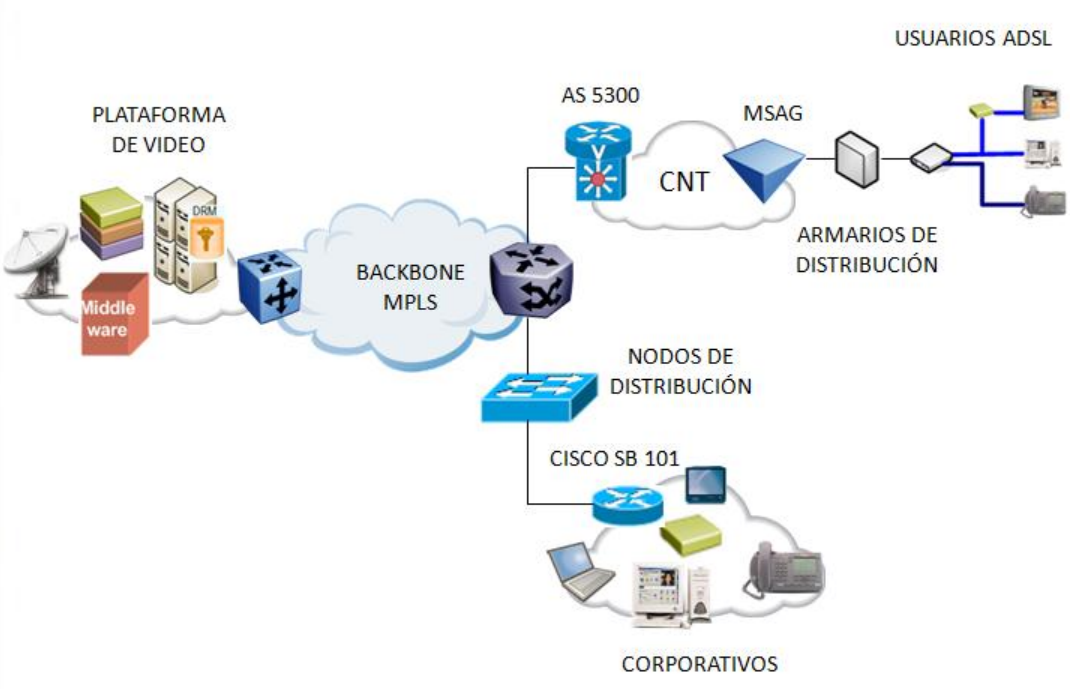


Figura 4.16 Backbone MPLS y servicios Triple Play

4.4.7 PRESUPUESTO REFERENCIAL DEL DISEÑO

En el ANEXO III se muestra una proyección de la demanda para los Servicios Triple Play, de este análisis se obtiene que en cinco años se tendrán aproximadamente 845 clientes corporativos y 430 clientes residenciales. Utilizando esta proyección se proponen los equipos a adquirir para la implementación de Triple Play en la tabla 4.9, en la que se detalla el número de equipos necesarios para el core, plataforma de video y equipos complementarios para VoIP conjuntamente con su costo individual y costo total, cabe recalcar que dichos valores pueden variar dependiendo de la casa comercial.

RED	EQUIPO	PRECIO U (USD)	CANTIDAD	TOTAL (USD)
PLATAFORMA IPTV	Receptor/Decodificador CISCO D9854	2371	1	2371
	Procesador de Video CISCO DCM D9900 MPEG	1400	1	1400
	Codificador de Video D9036	6950	1	6950
	Servidor Streaming IMX i2410	7500	1	7500
	Servidor VoD IMX M2200	6500	1	6500
	Middleware	7000	1	7000
	ROSA	20000	1	20000
VOZ	Gateway Cisco AS 5300	25000	2	50000
	Tarjetas modulares de voz/fax AS 53-CC-60VOXD	750	8	6000
	Cisco Work Voice Manager	19000	1	19000
CORE	Switch Cisco Catalyst 6506 (LSR)	4067	2	8134
	Routers Cisco 7206 VXR/NPE-G2 (LER salida)	17800	3	53400
DISTRIBUCIÓN	Switch Cisco Catalyst 3750 WS-C3750-24TS	5000	3	15000
	Switch Cisco Catalyst 3550 WS-C3550-48	3800	18	68400
	Transceivers	350	845	295750
ACCESO	Cisco SB 101	400	845	338000
	Modem ADSL2+ TD 8817	41	430	17630
USUARIO	STB (IPTV Services para el usuario)	80	1275	102000
	SISTEMA DE FACTURACIÓN	1	20000	20000
	TOTAL			1045035

Tabla 4.9 Costo de equipos

Como se observa en la tabla 4.9 para el funcionamiento de VoIP se debe adquirir 2 Gateways AS 5300 (uno para Guayaquil y uno Cuenca), además de 7 tarjetas voz/fax cada una con capacidad para 120 canales de voz con esto se cubre las 845 demandas corporativas.

En cuanto a los equipos de core se deben adquirir 3 routers 7206 VXR/NPE-G2 que serán el borde de la red MPLS en las 3 ciudades y dos switches capa 3 con función LSR CISCO 6506 para Guayaquil y Cuenca, el nodo de Quito actualmente cuenta con uno de estos y se lo utilizará para este diseño.

Para la Distribución de la misma manera se utilizarán 3 switches Catalyst 3750-24TS de 24 puertos. El switch 3750 para Quito cubre inicialmente 5 nodos, el de Guayaquil 2 nodos y el switch 3750 para Cuenca 1 nodo, se está garantizando la redundancia gracias a que estos

equipos son apilables. Para la distribución a los nodos secundarios (acceso de usuarios) son necesarios 18 switches Catalyst 3550 para cubrir las 845 demandas dentro de los cinco años.

Para el acceso de los usuarios corporativos se requieren 845 routers CISCO SB 100 y 845 tranceivers, mientras que para los usuarios residenciales se necesitan 430 módems ADSL y 1275 STB IP3000SD/HD para visualización de los servicios de video de todos los usuarios.

Además se debe considerar el tendido de fibra óptica a nivel de acceso para los usuarios corporativos, en la tabla 4.10 se indica los costos de tendido tomando como referencia que el promedio aproximado del tendido de fibra óptica es de 500 m por usuario y su precio es de 5$ por metro. Se considera 8 nodos porque son: 5 nodos de Quito, 2 de Guayaquil y un nodo en Cuenca.

Cobertura de 50 clientes por nodo= 50 clientes x 500m= 25000 m. de fibra óptica

Metros de fibra óptica para 8 nodos= 25000m x 8 nodos= 200.000 m.

DESCRIPCIÓN	METROS (m)	COSTO POR METRO (USD)	TOTAL (USD)
Fibra óptica	200000	5	1000000

Tabla 4.10 Costo de tendido de fibra óptica a nivel de acceso

No se considera el costo de instalación de la fibra óptica debido a que se lo hará paulatinamente en el momento que solicite el cliente y con los técnicos que tiene la empresa actualmente.

En la tabla 4.11 se presenta el costo total de la Ingeniería e Instalación, estos costos corresponden a los honorarios que la empresa debe cancelar a las personas que realizan el diseño y la instalación de los equipos, en este último se incluye la configuración de los mismos. La Plataforma IPTV al ser una solución integrada de CISCO la casa comercial

también proporciona la implementación y configuración de los equipos correspondientes a esta plataforma.

	DESCRIPCIÓN	CANTIDAD	COSTO (USD)
INGENIERÍA	Diseño de Red	1	6700
	Documentación de equipos	1	300
	SUBTOTAL		**7000**
INSTALACIÓN	Switch Cisco 6506 (LSR)	2	300
	Routers Cisco 7206 VXR (LER)	3	450
	Switch 3750-24TS	3	300
	Switch 3550-48	18	500
	Gateway AS 5300	2	400
	Tarjetas de voz/fax	7	560
	SUBTOTAL		**2510**
		TOTAL	**9510**

Tabla 4.11 Costo de Ingeniería e Instalación

Se debe también tomar en cuenta los costos de Operación y Mantenimiento, la empresa para la ejecución de proyectos anteriores ha estimado el 10% de los costos de los equipos como costo de Operación y Mantenimiento y para el desarrollo del presente proyecto también se estima este porcentaje tanto para el tendido de fibra óptica como para los equipos a utilizar. En la tabla 4.12 se muestra el costo total de Operación y Mantenimiento.

DESCRIPCIÓN	COSTO TOTAL (USD)	COSTO ANUAL (USD)
Acceso por fibra óptica	1000000	100000,00
Equipos	1045035	104503,50
	TOTAL	204503,50

Tabla 4.12 Costo de Operación y Mantenimiento

En la tabla 4.13 se puede apreciar el costo total a requerirse para la implementación de la red diseñada.

DESCRIPCIÓN	COSTO (USD)
Equipos	1045035,00
Acceso por fibra óptica	1000000,00
Ingeniería & Instalación	9510,00
Operación &Mantenimiento	204503,50
TOTAL	**2259048,50**

Tabla 4.13 Costo total de Implementación

De acuerdo a la tabla 4.13 el costo total del diseño para su implementación es de 2 259 048,50 USD, presupuesto que está sujeto a una evaluación previa por parte de la empresa para la toma de la decisión de implementarlo.

En el ANEXO III se presentan los cálculos para la obtención de los indicadores de rentabilidad para un tiempo de cinco años de operación, se obtuvo de este análisis un VAN (Valor Actual Neto) de 5 472 622 USD a una tasa de interés del 11,82 % vigente en el mercado, lo que da como resultado un TIR (Tasa Interna de Retorno) del 71 % con lo que se demuestra la rentabilidad del proyecto. Además la relación Beneficio/Costo indica el valor de 2,4 USD lo que significa que por cada dólar invertido se ganará 2,4 dólares al año y el período de recuperación de la inversión es de aproximadamente 1 año y 7 meses.

4.4.8 PROTOCOLOS DE ENRUTAMIENTO

Para el enrutamiento, MPLS sugiere los protocolos de estado de enlace ya que facilitan la convergencia y ofrecen mayor escalabilidad haciendo posible la realización de la Ingeniería de Tráfico como es el caso de los protocolos IS-IS y OSPF.

4.4.8.1 Protocolo IS-IS

El protocolo IS-IS pertenece al grupo de protocolos de estado de enlace de la ISO[102], distribuye una imagen de la topología de los ruteadores para el cálculo de la ruta más corta, cada router da a conocer las direcciones de la capa de red que se pueden alcanzar de manera directa utilizando el algoritmo de estado de enlace SPF[103].

A continuación se mencionan las características más importantes del protocolo IS-IS:

- Optimiza las decisiones de enrutamiento mediante una visión global de la red.
- Maneja eficientemente los recursos de la red como por ejemplo el ancho de banda.
- Permite una rápida recuperación de la red en caso de fallas.
- Utiliza puentes designados para eliminar bucles.
- Permite conectar redes con encaminamiento distinto y admite VLSM[104].
- Protocolo de enrutamiento interno e inundación rápida de nueva información.
- Manejo de hasta 1000 rutas dentro de un mismo Sistema Autónomo.
- Soporta MPLS e Ingeniería de Tráfico.

4.4.8.2 Protocolo OSPF

Es un protocolo de enrutamiento de estado de enlace del IETF, basado en código abierto y fue diseñado para cubrir los requerimientos de las grandes redes IP como: VLSM, autenticación del origen de la ruta, publicaciones de ruta para multidifusión, rápida recuperación de fallas, reconocimiento de varias métricas y capacidad de realizar encaminamiento dependiendo del tipo de servicio, etc.

---

[102] **ISO** International Organization for Standardization
[103] **SPF** Shortest Path First
[104] **VLSM** Variable Length Subnet Mask

Otras de las características más importantes se mencionan a continuación:

- Es un protocolo de enrutamiento interno.
- Utiliza complejas bases de datos para el cálculo del camino más corto.
- Ante un cambio de la red las rutas se actualizan en los routers tan pronto como se realiza el cambio.
- Rápido durante la recuperación de fallos.
- Cada router conoce la distancia de los demás routers, de esta manera cuanto un paquete es enviado sigue la ruta con menos saltos.
- Soporta MPLS e Ingeniería de Tráfico.
- OSPF permite que las redes contiguas se agrupen en áreas dentro de un Sistema Autónomo, simplificando la topología y manejando hasta 500 rutas.
- Las publicaciones del estado de enlace de los routers se dan a conocer mediante mensajes *"Hello"* y una vez sincronizados forman una adyacencia.
- La métrica de enrutamiento de OSPF es el costo y se calcula en base al ancho de banda de la interfaz que puede configurarlo el usuario.

Los protocolos IS-IS y OSPF poseen características similares al ser protocolos que utilizan algoritmos de estado de enlace y soportan MPLS e Ingeniería del Tráfico teniendo un tiempo corto de convergencia, pero para efectos del diseño propuesto se utilizará OSPF debido a que la red diseñada tiene 8 puntos de presencia y el número de rutas a utilizar no supera al número máximo de las 500 de OSPF o 1000 de IS-IS, por lo que se utilizará OSPF mencionando también que los equipos de core poseen características de robustez para soportarlo.

Adicional a la elección del protocolo de enrutamiento cabe mencionar que la selección del protocolo de señalización no tiene ninguna restricción ya que MPLS admite algunos protocolos como el caso de RSVP (Resource Reservation Protocol) o LDP (Label Distribution Protocol) por ser una tecnología abierta.

4.5 SIMULACIÓN DE LA RED

Para la simulación de la red propuesta se utilizará el software GNS3[105] el cual permite interactuar con los sistemas operativos de los equipos, de esta manera el PC se convierte en un router al que se lo puede configurar de acuerdo al IOS que se instale, teniendo de esta manera una clara visión de lo que será la implementación con equipos reales.

De acuerdo al compromiso de confidencialidad realizado con la empresa para esta simulación se utilizan otras direcciones IP para el backbone que se muestran en la tabla 4.14 con interfaces Fast Ethernet porque se escogió una plataforma inferior de routers para facilitar el procesamiento del PC.

EQUIPO	INTERFAZ	IP ADDRESS	AREA
LSR1	F0/0	192.168.10.2/30	0
	F0/1	192.168.10.9/30	0
	F1/0	192.168.10.13/30	1
LSR2	F0/0	192.168.10.1/30	0
	F0/1	192.168.10.5/30	0
	F1/0	192.168.10.17/30	2
LSR3	F0/0	192.168.10.10/30	0
	F0/1	192.168.10.6/30	0
	F1/0	192.168.10.21/30	3
LER1	F0/0	192.168.10.14/30	1
	F0/1	172.16.1.1/24	1
LER2	F0/0	192.168.10.18/30	2
	F0/1	172.16.2.1/24	2
LER3	F0/0	192.168.10.22/30	3
	F0/1	172.16.3.1/24	3

Tabla 4.14 Direccionamiento utilizado para la simulación

En la figura 4.17 se presenta la topología de la red a simular en el software.

---

[105] **GNS3** Graphic Network Simulator 3

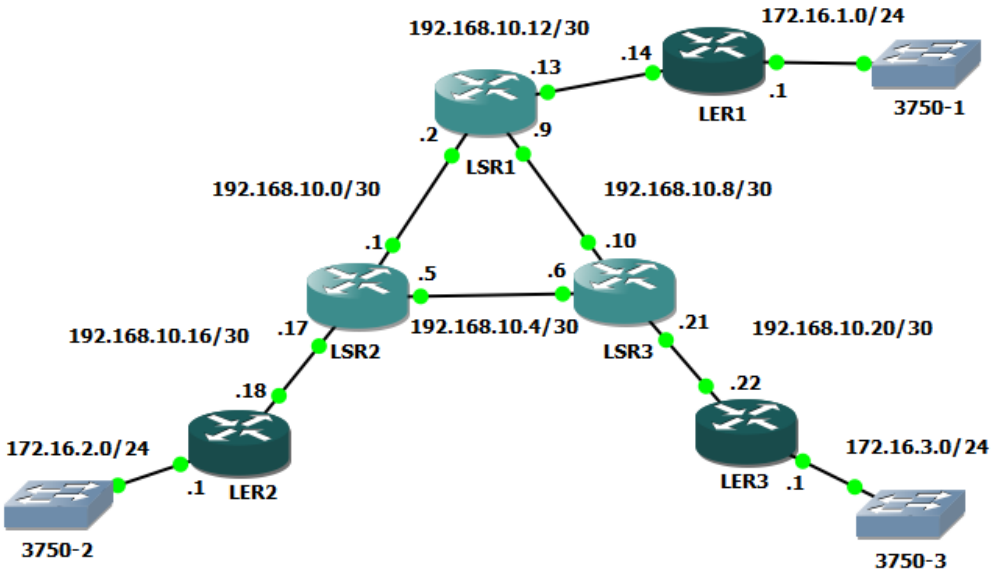


Figura 4.17 Backbone MPLS en GNS3

4.5.1 COMANDOS PARA LA CONFIGURACIÓN DE OSPF Y MPLS

A continuación se presentan los comandos básicos utilizados para la configuración de los equipos tanto para los LSR como para los LER.

1. **Configuración de OSPF**

```
Lsr1> enable
Lsr1# configure terminal
Lsr1(config)# router ospf < identificador del proceso OSPF >
Lsr1(config)# router ospf 1
Lsr1(config-router)# network <dirección IP> < wildcard-mask> area <area-id>
Lsr1(config-router)# network 192.168.10.8 0.0.0.3 area 0
```

2. **Configuración MPLS**

Para activar CEF y poder trabajar en entornos MPLS

```
Lsr1(config)# ip cef
Lsr1(config)# mpls ip
```

Para activar el protocolo de distribución de etiquetas LDP

```
Lsr1(config)# interface fastethernet <nombre de la interfaz>
Lsr1(config)# interface fastethernet1/0
```

```
Lsr1(config-if)# mpls ip
Lsr1(config-if)# mpls label protocol ldp
```

4.5.1.1 Pruebas de la red con el protocolo de enrutamiento OSPF

Una vez realizadas las configuraciones se procede a verificar la conectividad. En la figura 4.18 se puede observar la conectividad desde el LER de Quito hacia las redes de Guayaquil y Cuenca.

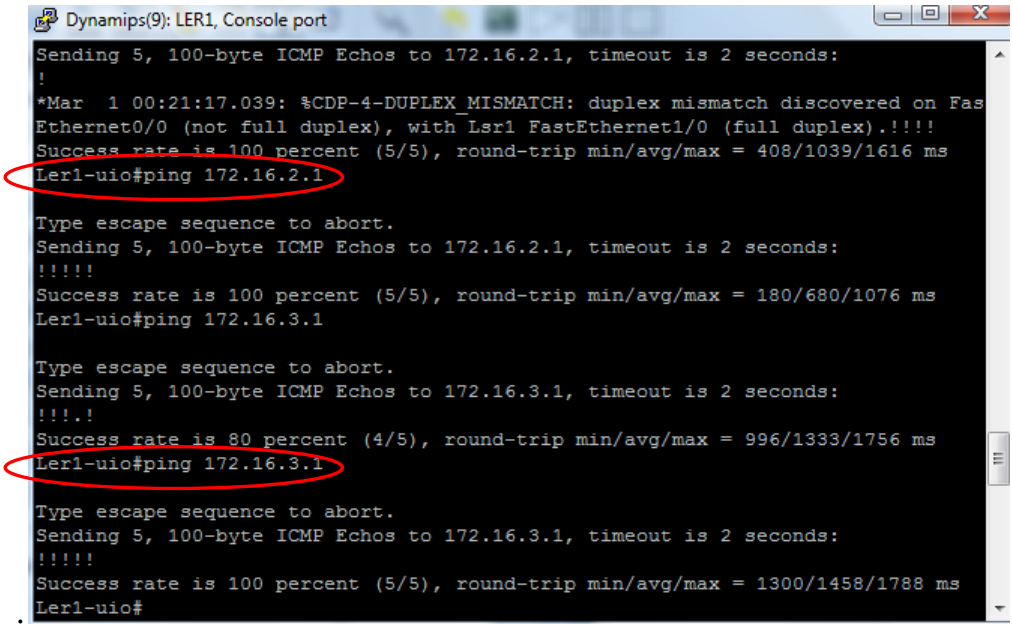


Figura 4.18 Conectividad desde Quito a los nodos de Guayaquil y Cuenca

En la figura 4.19 se presentan las pruebas de la conectividad del LER de Guayaquil hacia Quito y Cuenca.

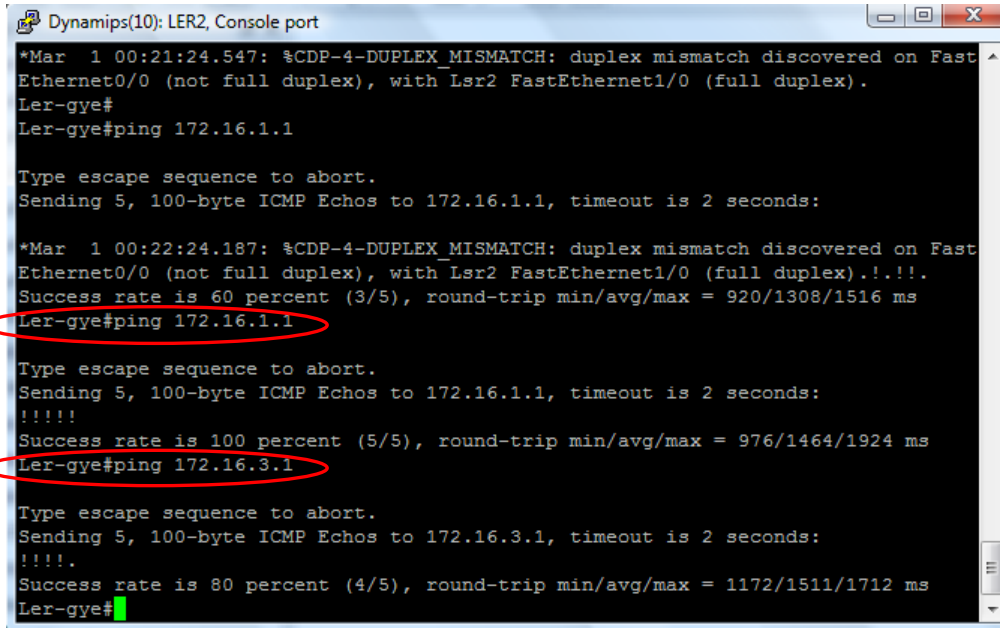


Figura 4.19 Conectividad desde Guayaquil a los nodos de Quito y Cuenca

Con ping se verifica la conectividad desde el LER de Cuenca a los nodos de Quito y Guayaquil como se presenta en la figura 4.20.

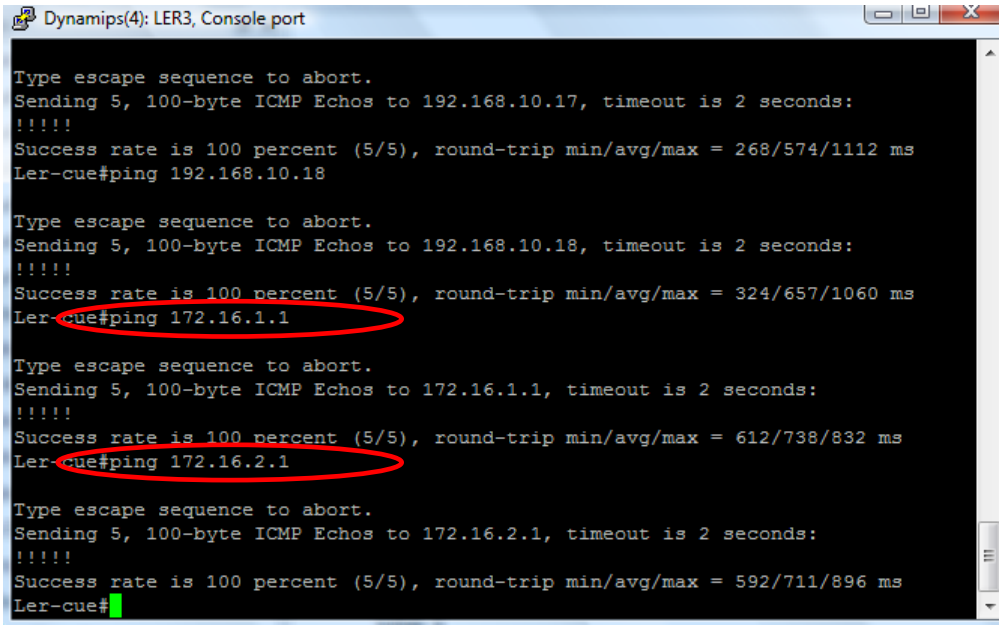


Figura 4.20 Conectividad desde Cuenca a los nodos de Guayaquil y Quito

4.5.1.2 Pruebas de la red con MPLS

Para verificar la configuración de MPLS se utiliza el comando *"show mpls forwarding-table"* el cual muestra la asignación de etiquetas por cada ruta. En la figura 4.21 se muestra la asignación de etiquetas en el LSR de Cuenca.

```
Lsr3#show mpls forwarding
Local  Outgoing    Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     172.16.3.0/24    0          Fa1/0      192.168.10.22
17     Pop tag     192.168.10.0/30  0          Fa0/0      192.168.10.9
       Pop tag     192.168.10.0/30  0          Fa0/1      192.168.10.5
18     16          172.16.1.0/24    1798       Fa0/0      192.168.10.9
19     16          172.16.2.0/24    590        Fa0/1      192.168.10.5
20     Pop tag     192.168.10.12/30 1140       Fa0/0      192.168.10.9
21     Pop tag     192.168.10.16/30 1140       Fa0/1      192.168.10.5
Lsr3#
```

Figura 4.21 Asignación e intercambio de etiquetas en el LSR3

En la figura 4.22 se muestra la asignación de etiquetas en el router LER de Guayaquil.

```
Ler-gye#show mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     192.168.10.0/30  0          Fa0/0      192.168.10.17
17     Pop tag     192.168.10.4/30  0          Fa0/0      192.168.10.17
18     17          192.168.10.8/30  0          Fa0/0      192.168.10.17
19     19          192.168.10.12/30 0          Fa0/0      192.168.10.17
20     18          172.16.1.0/24    0          Fa0/0      192.168.10.17
21     20          192.168.10.20/30 0          Fa0/0      192.168.10.17
22     21          172.16.3.0/24    0          Fa0/0      192.168.10.17
Ler-gye#
```

Figura 4.22 Asignación e intercambio de etiquetas en el LER de Guayaquil

Utilizando el comando *"show mpls interfaces"* se puede apreciar que en las interfaces está habilitado el protocolo LDP (Label Distribution Protocol). En la figura 4.23 se muestra la verificación de LDP tomando como ejemplo el router LSR1 de Quito.

```
Lsr1#show mpls interfaces
*Mar  1 00:05:05.471: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Fast
Ethernet1/0 (not half duplex), with Ler1-uio FastEthernet0/0 (half duplex).
Interface              IP            Tunnel   Operational
FastEthernet0/0        Yes (ldp)     No       Yes
FastEthernet0/1        Yes (ldp)     No       Yes
FastEthernet1/0        Yes (ldp)     No       Yes
Lsr1#
```

Figura 4.23 Protocolo LDP habilitado en la red

Agregando *"detail"* al anterior comando se puede observar más detalles de la configuración como por ejemplo el tamaño del MTU (Maximum Transmission Unit) y que otras opciones de MPLS están desabilitadas para la interfaz como BGP y los túnelrs LSP (Label Switches Path) como se indica en la figura 4.24

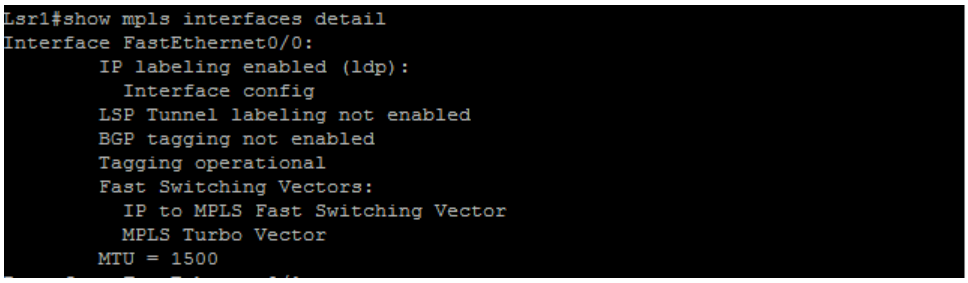


Figura 4.24 Detalles de las interfaces con MPLS

Con el comando *"traceroute"* se verifica los saltos para llegar a una IP de destino y el intercambio en esos saltos del valor de las etiquetas. En la figura 4.25 se muestran los saltos desde el router LER de Guayaquil hasta la IP 172.16.1.1 correspondiente a la interfaz de salida del LER de Quito.

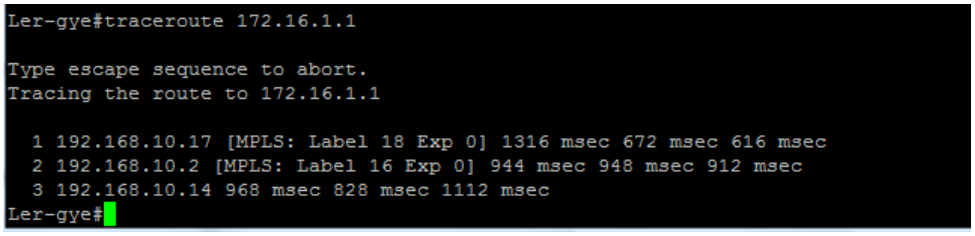


Figura 4.25 Traceroute a 172.16.1.1

Además se puede apreciar en la figura 4.25 que el campo EXP por defecto tiene el valor de 0, posteriormente se manipula este campo para ofrecer QoS mediante DiffSev.

Las configuraciones de cada uno de los routers tanto LSR como LER se muestran en el ANEXO II, además de comandos adicionales para la verificación del funcionamiento de MPLS.

4.5.2 SINCRONIZACIÓN DE OSPF Y MPLS

Esta opción evita la pérdida de paquetes que se puede producir por conflictos de sincronización entre los dos protocolos debido a las adyacencias que se establecen con OSPF antes de formar las rutas virtuales con LDP (Label Distribution Protocol) y se configura con los siguientes comandos:

```
Lsr3(config)# router ospf 1
Lsr3(config-router)# mpls ldp sync
Lsr3(config-router)# end
```

Utilizando el comando *"show mpls ldp igp sync"* se puede observar en la figura 4.26 la sincronización entre MPLS y OSPF y muestra las interfaces del router configuradas con esta opción.

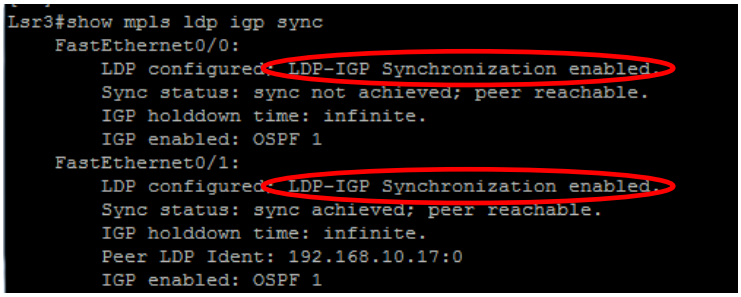


Figura 4.26 Sincronización de OSPF y MPLS

En la tabla 4.15 se muestra una comparación de la red con OSPF y la misma red con OSPF más la implementación de MPLS. Para obtener estos valores se realizó pruebas de ping a todos los nodos y se comprobó que en la red con MPLS se tiene tiempos de retardo inferiores a los de la red que tiene configurado solamente OSPF, por lo que se verifica que la rapidez de envío es alta.

Origen / Destino	OSPF			OSPF & MPLS		
	Ler UIO (ms)	Ler GYE (ms)	Ler CUE (ms)	Ler UIO (ms)	Ler GYE (ms)	Ler CUE (ms)
UIO 172.16.1.1	8	1125	2248	8	724	1651
GYE 172.16.2.1	487	8	2277	448	8	2240
CUE 172.16.3.1	630	2379	8	586	2026	8

Tabla 4.15 Optimización de MPLS

Por ejemplo se observa en la tabla 4.15 que desde Quito hacia Guayaquil en la red con OSPF la demora es de 1125 *ms* mientras que en la red con MPLS es de 724 *ms*.

4.5.3 QoS MEDIANTE LA IMPLEMENTACIÓN DE DIFFSERV

MPLS se adapta perfectamente al Modelo de Servicios Diferenciados (DiffServ), ya que las etiquetas MPLS tienen el campo EXP para poder propagar la Clase de Servicio CoS en el correspondiente LSP (Label Switched Path). De este modo, una red MPLS puede transportar distintas clases de tráfico de acuerdo con la información contenida en los bits del campo EXP.

Dentro de la cabecera del paquete IP existe un campo denominado ToS (Type of Service), formado de 8 bits cuya función es indicar la importancia del paquete. En la figura 4.27 se muestra la ubicación del campo ToS dentro de la cabecera IP.

Ver	Hlen	ToS	Longitud total	
Identificación			Flags	Margen del fragmento
TTL		Protocolo	Checksum	
Direccion IP origen				
Dirección IP destino				
Opciones (opcional)				
DATOS				

Fuente: http://es.wikipedia.org/wiki/IPv4

Figura 4.27 Campo ToS en la Cabecera IP

A continuación en la figura 4.28 se presenta la estructura del campo ToS:

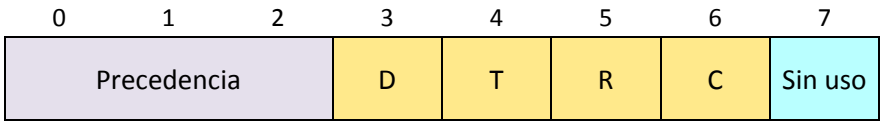


Figura 4.28 Estructura del campo ToS

Como se observa en la figura 4.28 los 3 primeros bits se denominan *"Precedencia"* usado para asignar un nivel de prioridad al datagrama IP. Se tendrían con estos tres bits ocho niveles, pero los dos valores máximos están reservados para la utilización interna de la red, teniendo disponible seis Clases de Servicios.

Los bits D (Delay), T (Throughput), R (Reliability) y C (Cost) fueron creados para especificar el retardo, flujo de salida, fiabilidad y requisitos de coste, actualmente en el modelo DiffServ determinan las características del servicio.

El campo ToS dentro del Modelo de Servicios Diferenciados se lo conoce también como campo DS (DiffServ). Dentro del campo DS los seis primeros bits se denominan DSCP (DiffServ Code Point) mientras que los dos últimos bits están reservados. Con los otros 6 bits restantes es posible obtener 64 combinaciones o posibles tipos de servicios.

CAPÍTULO 4

Para la oferta de Servicios Triple Play en la empresa Ecuanet-MEGADATOS se plantea seis Clases de Servicios para distribuir las aplicaciones de voz, datos y video de acuerdo a la prioridad, en la tabla 4.16 se muestra las Clases de Servicios, nombre DiffServ correspondiente a cada clase en este caso AF (Assured Forwarding) y sus variantes, el tipo de tráfico de cada clase y además el campo EXP de MPLS que indica el nivel de prioridad del tráfico a lo largo del trayecto en la red.

CLASES	DIFFSERV	TRÁFICO	TIPO	EXP
Best Effort	AF11	Aplicaciones que no reciben ninguna garantía de QoS	ICMP	0
Bronce	AF12	Protocolos y aplicaciones para administrar la red	SNMP,TELNET	1
Plata	AF21-AF22	Aplicaciones empresariales	Bases de datos, transacciones web	2, 3
Oro	AF31	Videoconferencia y streaming	HTTP	4
Premium	AF32	VoIP	TCP, UDP	5

Tabla 4.16 Clasificación de los servicios mediante la prioridad

Como se observa en la tabla 4.16 y para la configuración de los equipos: Best Effort corresponderá al nombre AF11, Bronce a AF12, Plata a dos clases AF21 y AF22 (debido a que las aplicaciones empresariales se subdividen para clientes VIP o Corporativos), la clase Oro toma el nombre de AF31 y finalmente la clase Premium corresponde a AF32.

4.5.3.1 Configuración de las Clases de Servicio con DiffServ y MPLS

A continuación se presenta la configuración detallada de DiffServ con MPLS en el router de borde LER1 perteneciente al nodo de Quito.

4.5.3.1.1 Marcado y clasificación del tráfico en el router LER1

De acuerdo al valor Precedence del paquete IP al ingreso por el router LER1 se lo clasifica dentro de las clases definidas DiffServ que son; AF11, AF12, AF21, AF22, AF31 y AF32 aplicando la siguiente configuración:

```
Ler1-uio#configure terminal
Ler1-uio(config)#class-map IP-AF11
Ler1-uio(config-cmap)#match ip precedence 0
Ler1-uio(config-cmap)#exit

Ler1-uio(config)#class-map IP-AF12
Ler1-uio(config-cmap)#match ip precedence 1
Ler1-uio(config-cmap)#exit

Ler1-uio(config)#class-map IP-AF21
Ler1-uio(config-cmap)#match ip precedence 2
Ler1-uio(config-cmap)#exit

Ler1-uio(config)#class-map IP-AF22
Ler1-uio(config-cmap)#match ip precedence 3
Ler1-uio(config-cmap)#exit

Ler1-uio(config)#class-map IP-AF31
Ler1-uio(config-cmap)#match ip precedence 4
Ler1-uio(config-cmap)#exit

Ler1-uio(config)#class-map IP-AF32
Ler1-uio(config-cmap)#match ip precedence 5
Ler1-uio(config-cmap)#exit
```

4.5.3.1.2 Creación de la política de entrada

Una vez que los paquetes están clasificados se someten a ciertas reglas que son especificadas dentro de una política a la entrada por el router. La política configurada en este caso permite primeramente enviar el tráfico a cierta velocidad y copiar el valor Precedence al campo EXP para la transmisión hacia el siguiente salto.

```
Ler1-uio(config)#policy-map politica-1

Ler1-uio(config-pmap)#class IP-AF11
```

```
Ler1-uio(config-pmap-c)#police 8000 conform-action set-mpls-exp-imposition-transmit 0 exceed-action drop
Ler1-uio(config-pmap-c)#exit

Ler1-uio(config-pmap)#class IP-AF12
Ler1-uio(config-pmap-c)#police 10000 conform-action set-mpls-exp-imposition-transmit 1 exceed-action set-mpls-exp-imposition-transmit 0
Ler1-uio(config-pmap-c)#exit

Ler1-uio(config-pmap)#class IP-AF21
Ler1-uio(config-pmap-c)#police 12000 conform-action set-mpls-exp-imposition-transmit 2 exceed-action set-mpls-exp-imposition-transmit 1
Ler1-uio(config-pmap-c)#exit

Ler1-uio(config-pmap)#class IP-AF22
Ler1-uio(config-pmap-c)#police 12000 conform-action set-mpls-exp-imposition-transmit 3 exceed-action set-mpls-exp-imposition-transmit 2
Ler1-uio(config-pmap-c)#exit

Ler1-uio(config-pmap)#class IP-AF31
Ler1-uio(config-pmap-c)#police 12000 conform-action set-mpls-exp-imposition-transmit 4 exceed-action set-mpls-exp-imposition-transmit 3
Ler1-uio(config-pmap-c)#exit

Ler1-uio(config-pmap)#class IP-AF32
Ler1-uio(config-pmap-c)#police 12000 conform-action set-mpls-exp-imposition-transmit 5 exceed-action set-mpls-exp-imposition-transmit 4
Ler1-uio(config-pmap-c)#end
```

4.5.3.1.3 Asignación de la política a la interfaz de entrada

La política es aplicada a la interfaz f0/1 al ingreso a la red de la siguiente manera:

```
Ler1-uio(config)#int f0/1
Ler1-uio(config-if)#service-policy input politica-1
Ler1-uio(config-if)#exit
```

4.5.3.1.4 Clasificación de los paquetes en base al campo EXP

Los paquetes nuevamente son clasificados a la salida del router, para este caso de acuerdo al valor del campo EXP de la etiqueta superior y es colocado en las respectivas clases.

```
Ler1-uio#configure terminal

Ler1-uio(config)#class-map MPLS-AF11
```

```
Ler1-uio(config-cmap)#match mpls experimental topmost 0
Ler1-uio(config-cmap)#exit

Ler1-uio(config)#class-map MPLS-AF12
Ler1-uio(config-cmap)#match mpls experimental topmost 1
Ler1-uio(config-cmap)#exit

Ler1-uio(config)#class-map MPLS-AF21
Ler1-uio(config-cmap)#match mpls experimental topmost 2
Ler1-uio(config-cmap)#exit

Ler1-uio(config)#class-map MPLS-AF22
Ler1-uio(config-cmap)#match mpls experimental topmost 3
Ler1-uio(config-cmap)#exit

Ler1-uio(config)#class-map MPLS-AF31
Ler1-uio(config-cmap)#match mpls experimental topmost 4
Ler1-uio(config-cmap)#exit

Ler1-uio(config)#class-map MPLS-AF32
Ler1-uio(config-cmap)#match mpls experimental topmost 5
Ler1-uio(config-cmap)#exit
```

4.5.3.1.5 Creación de la política a la salida del router LER1

La política a la salida del router especifica el porcentaje de ancho de banda asignado a cada clase y además para las situaciones de congestión se activa el mecanismo de descarte inteligente para evitar oscilaciones llamado WRED (Weighted Random Early Discard).

```
Ler1-uio(config)#policy-map politica-2

Ler1-uio(config-pmap)#class MPLS-AF11
Ler1-uio(config-pmap-c)#bandwidth percent 5
Ler1-uio(config-pmap-c)#random-detect
Ler1-uio(config-pmap-c)#exit

Ler1-uio(config-pmap)#class MPLS-AF12
Ler1-uio(config-pmap-c)#bandwidth percent 10
Ler1-uio(config-pmap-c)#random-detect
Ler1-uio(config-pmap-c)#exit

Ler1-uio(config-pmap)#class MPLS-AF21
Ler1-uio(config-pmap-c)#bandwidth percent 10
Ler1-uio(config-pmap-c)#random-detect
```

```
Ler1-uio(config-pmap-c)#exit

Ler1-uio(config-pmap)#class MPLS-AF22
Ler1-uio(config-pmap-c)#bandwidth percent 15
Ler1-uio(config-pmap-c)#random-detect
Ler1-uio(config-pmap-c)#exit

Ler1-uio(config-pmap)#class MPLS-AF31
Ler1-uio(config-pmap-c)#bandwidth percent 15
Ler1-uio(config-pmap-c)#random-detect
Ler1-uio(config-pmap-c)#exit

Ler1-uio(config-pmap)#class MPLS-AF32
Ler1-uio(config-pmap-c)#bandwidth percent 20
Ler1-uio(config-pmap-c)#random-detect
Ler1-uio(config-pmap-c)#end
```

4.5.3.1.6 Asignación de la política en la interfaz de salida del LER1

La política es aplicada a la interfaz de salida del router LER1, en donde los paquetes son clasificados dependiendo del valor del campo EXP y enviados utilizando un ancho de banda de acuerdo a la prioridad.

```
Ler1-uio(config)#int f0/0
Ler1-uio(config-if)#service-policy output politica-2
Ler1-uio(config-if)#exit
```

En el ANEXO II se presentan los fragmentos de configuración de los demás equipos correspondientes a los trayectos de Quito – Guayaquil y Quito – Cuenca, en donde se mantiene el esquema de configuración del router LER1 en cuanto al marcado, clasificación y políticas.

4.5.3.2 Esquema de Emulación utilizado para DiffServ y MPLS

En la figura 4.29 se muestra el esquema utilizado para la generación de tráfico real a aplicar al backbone MPLS. En el computador portátil se encuentra la aplicación GNS3 con el backbone MPLS a simular mientras que en el PC de escritorio tiene una aplicación de Windows que permite generar tráfico utilizando el DOS llamado QoS Traffic Generator, que se lo puede descargar gratuitamente de la página de Microsoft.

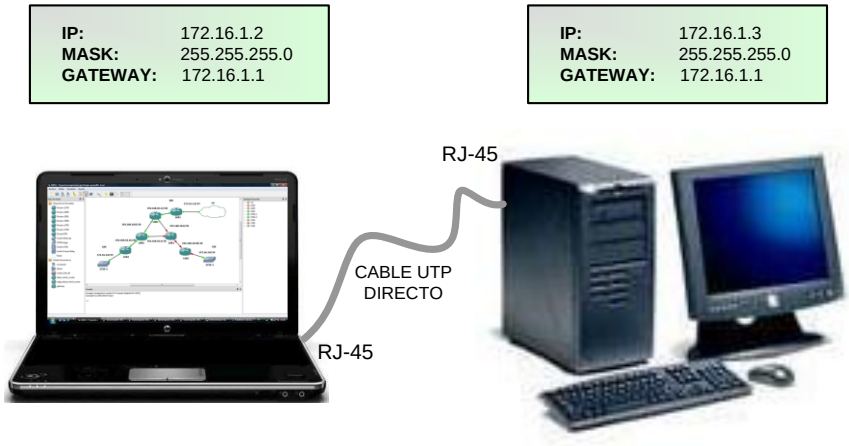


Figura 4.29 Esquema para la simulación de tráfico real

Como se observa en la figura 4.29 antes de generar el tráfico es necesario configurar las tarjetas de red de los computadores. GNS3 ofrece la ventaja de interactuar con redes reales (se explica detalladamente en el ANEXO IV), en este caso el puerto del PC portátil está configurado para que emule al puerto del router de borde LER1 correspondiente a la ciudad de Quito (interfaz por donde ingresa el tráfico generado). Las dos direcciones IP configuradas pertenecen a la subred 172.16.1.0 y como Gateway se configura a la interfaz de entrada del LER1 f0/1 cuya dirección es 172.16.1.1.

Una vez realizada la conexión física utilizando un ping extendido se comprueba la conectividad desde el generador de tráfico hacia la red de destino de Guayaquil cuya dirección IP es 172.16.2.1 como se muestra en la figura 4.30.

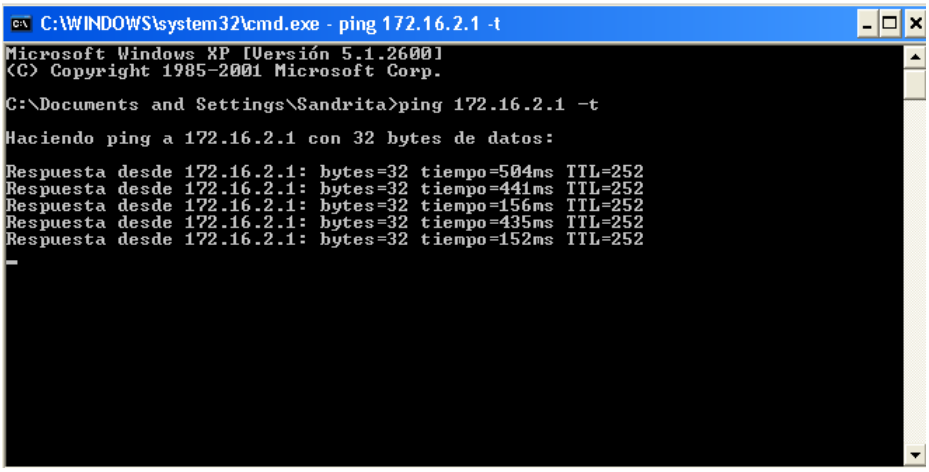


Figura 4.30 Conectividad exterior con el Backbone MPLS

Desde el Símbolo del Sistema se ejecuta la aplicación "QoS Traffic Generator" con el siguiente comando: *qostraffic.exe –source –udp –dest 172.16.2.1 –throttle 1000 –duration 10 –tc 40,4.*

Donde:

-source:	indica que el PC de escritorio es el origen
-udp:	tipo de tráfico, puede también ser tcp
-dest 172.16.2.1:	el destino del tráfico (Nodo de Guayaquil)
-throttle 1000:	velocidad de transmisión en bits por segundo
-duration 10:	10 segundos, tiempo de generación de tráfico
-tc 40,4:	indica que se ha generado tráfico clase 5 que corresponde a AF32 o Premium.

En la tabla 4.17 se muestra la correspondencia de las clases con el Precedence y los valores a utilizar en QoS Traffic Generator.

ToS Bits Precedence	QoS Traffic Generator	Valores QoS Traffic Generator	DiffServ	Clases
000 000 00	CS0	0	AF11	Best Effort
001 000 00	CS1	8	AF12	Bronce
010 000 00	CS2	16	AF21	Plata 1
011 000 00	CS3	24	AF22	Plata 2
100 000 00	CS4	32	AF31	Oro
101 000 00	CS5	40	AF32	Premium

Tabla 4.17 Correspondencia de valores según la Clase de Servicio

Para obtener los valores del QoS Traffic Generator no se toman en cuenta los dos últimos bits del campo ToS ya que están reservados para mecanismos internos y de derecha a izquierda se realiza la equivalencia, a continuación un ejemplo en la tabla 4.18.

1	**0**	**1**	0	0	0	0	0
2^5	2^4	2^3	2^2	2^1	2^0		
32	16	**8**	4	2	1		

Tabla 4.18 Valor a utilizar en el Generador de Tráfico

Con el valor Precedence en binario 101 equivale en decimal a 5, el valor a utilizar en el QoS Traffic Generator es 40, si se desea generar tráfico de clase 2 el Precedence es 010 y el valor a utilizar para generarlo en el DOS es 16, en la figura 4.31 se muestra que se ha generado tráfico Clase 5 satisfactoriamente.

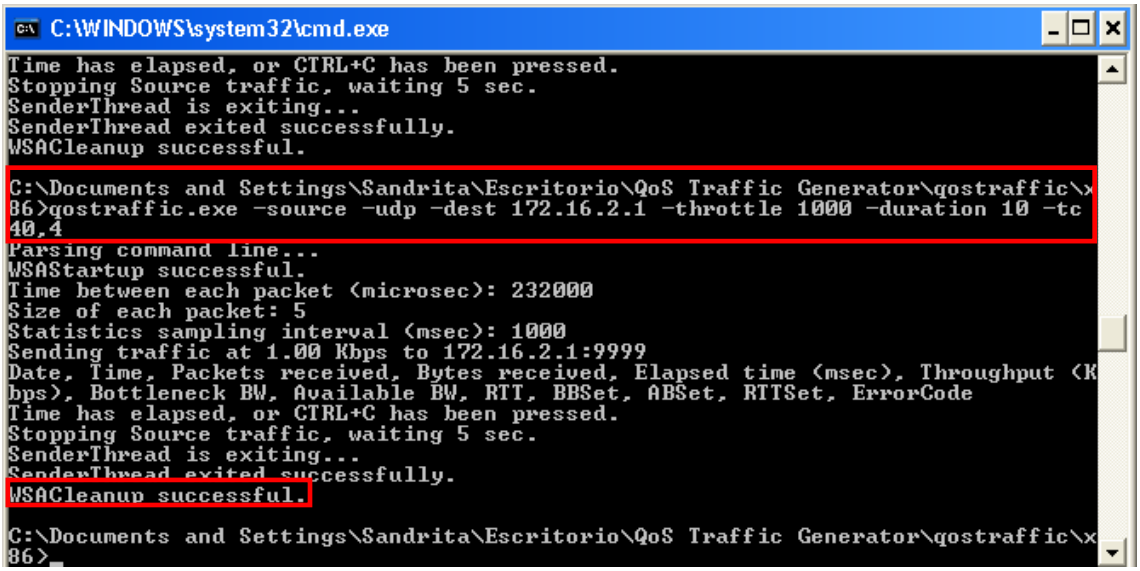


Figura 4.31 Generación de Tráfico satisfactorio

Con la ayuda de Wireshark se comprueba que efectivamente el tráfico generado es de Clase 5 o Premium como lo indica la figura 4.32.

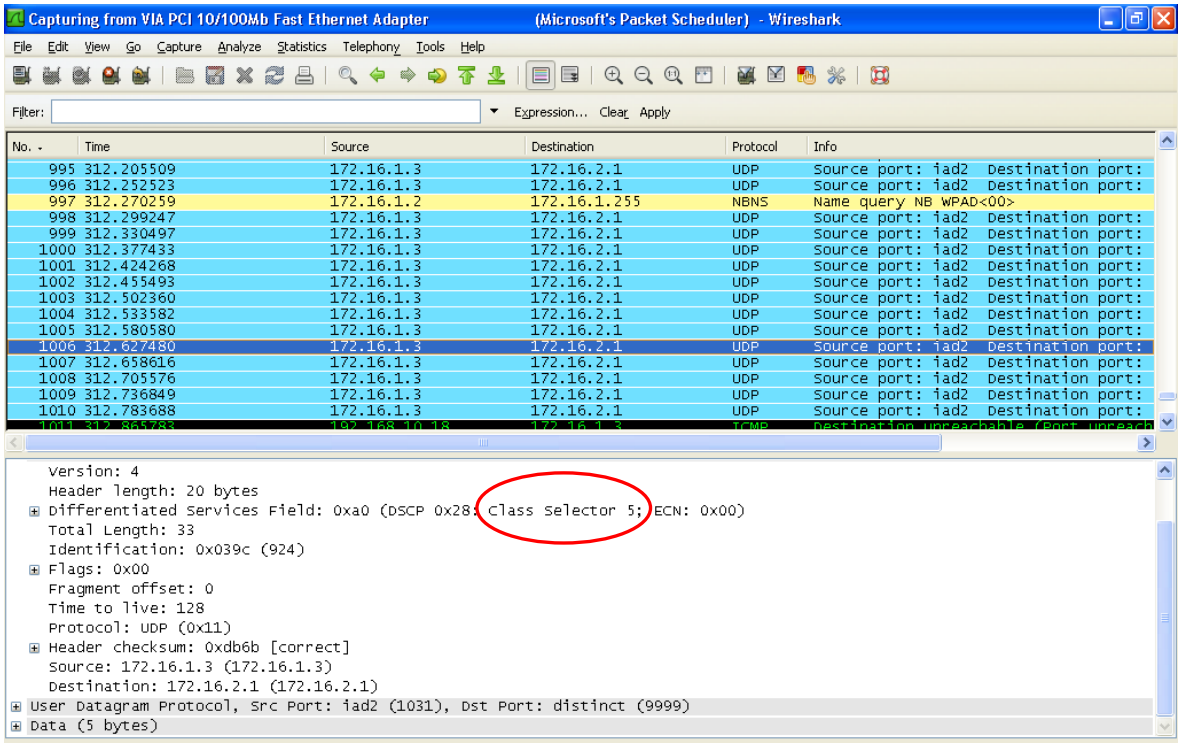


Figura 4.32 Generación de Tráfico Clase 5

4.5.3.3 Verificación del Backbone MPLS con el modelo DiffServ

Ahora se comprueba en la interfaz de entrada f0/1 del router LER1 que el tráfico generado desde el PC de escritorio es encaminado únicamente a la clase a la que pertenece como se indica en la figura 4.33 utilizando el comando *"show policy-map interface f0/1"* en donde además se muestra la política configurada para dicha clase.

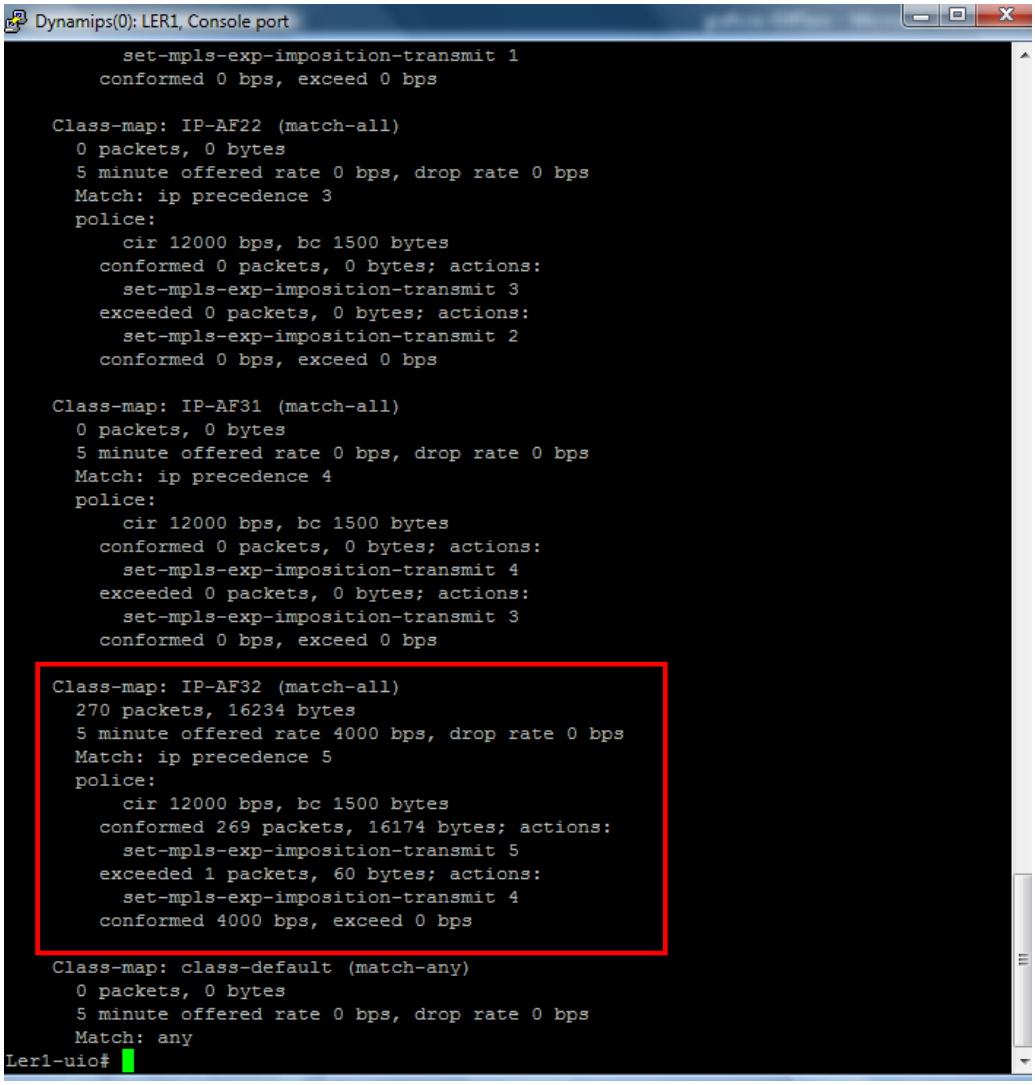


Figura 4.33 Clasificación del tráfico en la interfaz de entrada al router LER1

GNS3 también hace uso de Wireshark al efectuar las simulaciones para capturar el tráfico de la red, con esto se verifica que el tráfico que cursa por la interfaz del LER1 hacia el LSR1 es

etiquetado y su campo EXP ha sido seteado por el valor de 5 por pertenecer a la clase 5 (AF32 o Premium) como se presenta en la figura 4.34.

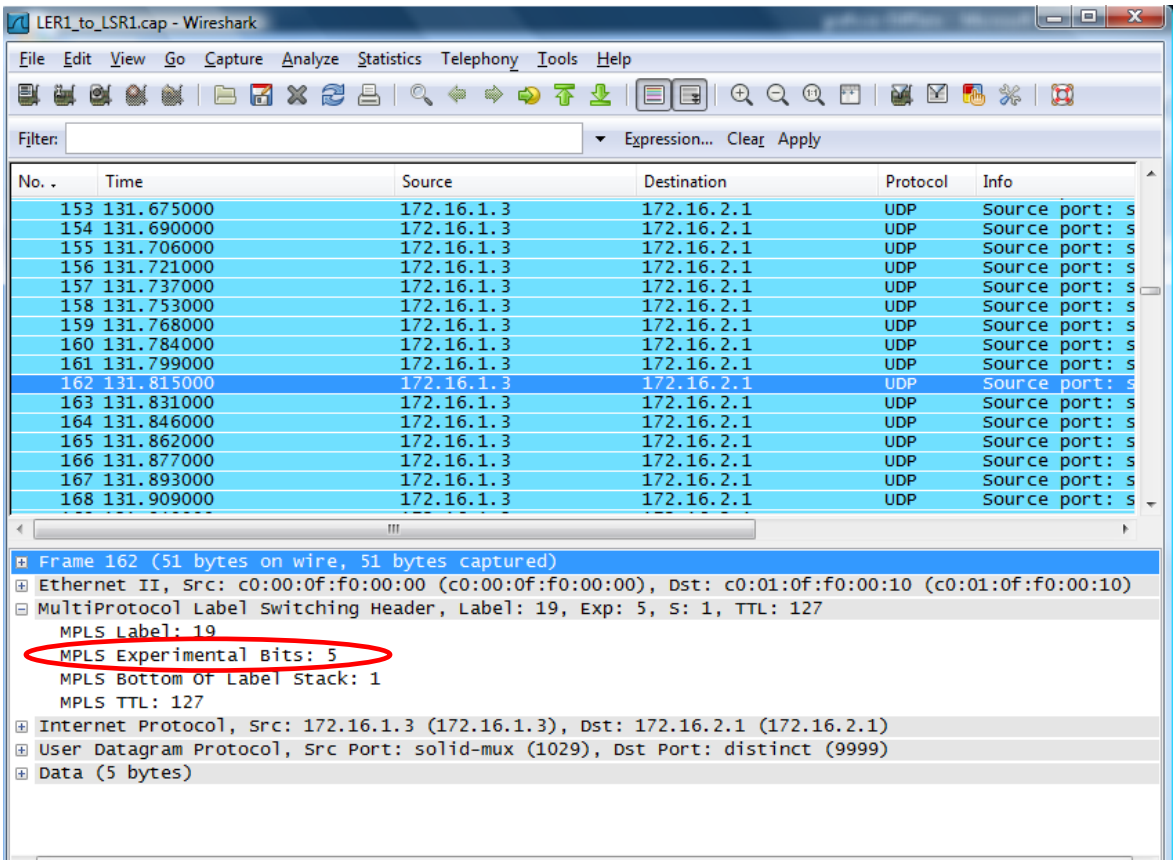


Figura 4.34 Manipulación del campo EXP según la Clase de Servicio

En la figura 4.35 se verifica que la política de clasificación del tráfico se mantiene en el router LSR2 que corresponde a Guayaquil, de la misma manera se utiliza el comando *"show policy-map interface f0/0"*.

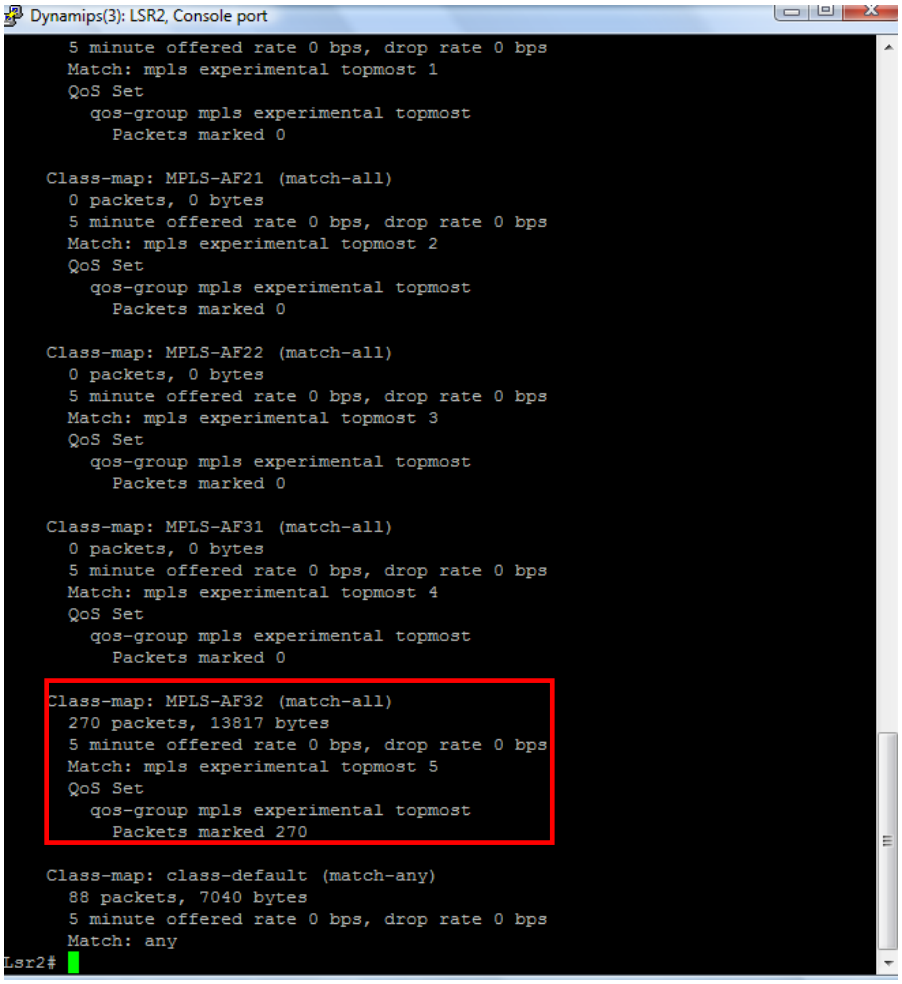


Figura 4.35 Clasificación del tráfico en el LSR2

La figura 4.36 muestra que al router LSR2 le llega el tráfico etiquetado y que el campo EXP mantiene el valor de 5 correspondiente a la Clase 5 o Premium utilizando Wireshark.

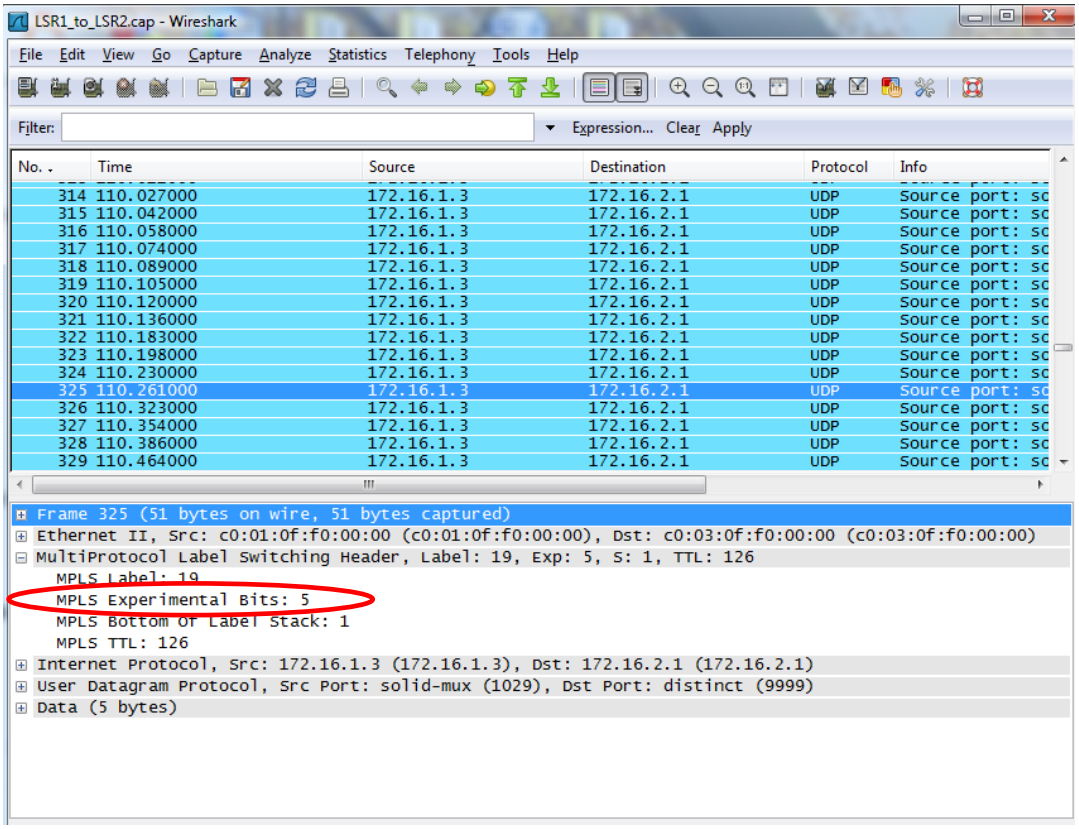


Figura 4.36 Captura de tráfico en el LSR2

4.6 CONSIDERACIONES PARA LA ADMINISTRACIÓN DE LA RED

Es fundamental realizar tareas de administración de red mediante mecanismos para la monitorización con el objetivo de estar al tanto del estado y recursos de la red garantizando la estabilidad y Calidad del Servicio.

Como se mencionó en la sección 4.4.6.2 para el diseño se propone la utilización del Sistema de Administración de red ROSA de Cisco, que además de gestionar los dispositivos de la plataforma de video permite controlar equipos de las demás capas de la red de esta manera se registran las incidencias ocurridas para una respuesta inmediata a través de funciones de control del tráfico nodal, restricciones, administración de encolamiento y planificación. En cuanto a VoIP el Cisco Voice Manager ofrece las mismas ventajas para la administración de los recursos de voz. Estos dos sistemas también proporcionan una interfaz gráfica amigable

por medio de señales de alerta con alarmas sonoras que son visibles para el administrador facilitando informes históricos para la planificación de la capacidad y gestión de los recursos.

En cuanto a la administración del backbone, al contar con MPLS se facilita la gestión de la red ya que se tiene en una sola tecnología el nivel de enlace de los datos con el nivel de red, además la información que proporciona MPLS sobre los túneles LSP, VPNs, rutas para la Ingeniería de Tráfico permiten priorizar el tráfico de acuerdo a las aplicaciones que requiere el usuario.

4.7 BENEFICIOS DE LA IMPLEMENTACIÓN

Una vez realizado el estudio de la red y el diseño del backbone MPLS a continuación se nombran los principales beneficios que se obtendrán con la implementación tanto para los clientes como para la empresa.

4.7.1 USUARIOS

- Posibilita un servicio más personalizado ya que el cliente elige los servicios y contenidos en el momento en que desee utilizarlos.

- La Calidad de Servicio está garantizada de extremo a extremo, es decir los usuarios en sus casas o lugares de trabajo gozan de la calidad contratada conforme al tipo de SLA acordado con la empresa.

- El usuario tiene interactividad con los servicios IPTV al tener una televisión a la carta.

- Con la contratación de los servicios de voz, datos y video a un único proveedor, los clientes reciben facturación unificada.

- El ahorro económico y en tiempo que representa el contratar el servicio de un solo proveedor resulta más cómodo para el usuario.

4.7.2 EMPRESA

- Un dominio MPLS haciendo las labores de troncal posibilita la Calidad de Servicio manteniendo la infraestructura existente y si a futuro las tecnologías implementadas en los nodos de distribución y acceso cambian independientemente la red troncal o dominio MPLS no necesita cambiar ya que soporta cualquier tecnología a nivel físico y enlace.

- Seguridad en el trasporte de datos con la implementación de VPNs basadas en MPLS, las cuales ofrecen conectividad virtual garantizando los LSP para cada usuario.

- Ingeniería de Tráfico para administrar y gestionar los enlaces por medio del balanceo de cargas en la red de core ya que los administradores de red pueden reducir el número de saltos entre los puntos mejorando los tiempos de respuesta y el rendimiento de las aplicaciones, disminuyendo la congestión.

- Calidad de Servicio acorde a las necesidades de los clientes mediante la prioridad de las aplicaciones de tiempo real.

- Menores costos de administración y mantenimiento de la red debido a que bajo una sola infraestructura se operan varios servicios.

- Mejora la rentabilidad de la empresa al aumentar la penetración en el mercado e incrementar los ingresos por usuarios ya que la oferta conjunta de los tres servicios asegura la estabilidad de la cartera de clientes aumentando el volumen del negocio.

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES

En el presente capítulo se exponen las conclusiones y recomendaciones sobre la tecnología MPLS para el soporte de servicios Triple Play, estudio que servirá como base para la implementación a futuro en la empresa y pauta general para la migración de las redes de otros proveedores.

5.1 CONCLUSIONES

- En la actualidad las exigencias de los usuarios ya no son las mismas de años anteriores ya que la integración de servicios de voz, datos y video se han convertido en una necesidad, estas aplicaciones pueden ser ofrecidas a los usuarios con la implementación de nuevas tecnologías que posibilitan la entrega de estos servicios de manera unificada bajo plataformas de red únicas conocidas como NGNs, lo que impulsa a los proveedores de red a buscar alternativas urgentes para su implementación y satisfacer la demanda de los usuarios con la finalidad de permanecer competitivos en el mercado de las Telecomunicaciones o caso contrario simplemente tienden a desaparecer.

- La migración de las redes de los proveedores a NGN no constituye un conjunto de procedimientos esporádicos sino un proceso minucioso y continuo que puede tardarse hasta varios años, este proceso requiere de una planificación adecuada, estrategias de implementación con una clara visión de la estructura jerárquica de una infraestructura de red NGN.

- En el capítulo 1 se ha expuesto un procedimiento general para la migración de las redes actuales de los proveedores a una red NGN, pero en su diseño e implementación hay muchos factores que influyen como la situación económica, la infraestructura actual, la gestión comercial del operador, los objetivos en cuanto a la expansión y cuán

modernizada tecnológicamente quiera ser a futuro, estos definirán la estrategia más adecuada para la migración.

- Para el soporte de las nuevas aplicaciones los operadores de Telecomunicaciones deben incrementar la capacidad de las redes de transporte para soportar todo el tráfico generado en la red de acceso de sus usuarios por el alto consumo de ancho de banda de aplicaciones como: Internet, video bajo demanda, streaming entre otras.

- La convergencia de redes y la convergencia de servicios es posible con la implementación de la tecnología MPLS en el backbone de la red ya que permite unificar la rapidez del reenvío del tráfico con las funciones de enrutamiento además de brindar Calidad de Servicio con la utilización de DiffServ, mejorando la transmisión y priorizando el tráfico de las aplicaciones de voz, datos y video.

- Con la implementación de MPLS también se mejora notablemente el rendimiento de la red ya que los paquetes son conmutados en base a etiquetas obviando la lectura de las cabeceras IP, además facilita la adopción de mecanismos de balanceo de carga para evitar la congestión con la Ingeniería de Tráfico y posibilidad de ofrecer servicios de VPNs a través de túneles virtuales eliminando las dificultades de las VPNs tradicionales.

- Los equipos seleccionados para conformar el backbone MPLS ofrecen escalabilidad y flexibilidad para soportar los requerimientos más exigentes, crecimiento de la demanda y migración a NGN además de adaptarse fácilmente a la red actual por ser de la marca CISCO.

- A nivel mundial las empresas proveedoras de servicios de Telecomunicaciones se están inclinando fuertemente a la provisión de servicios Triple Play, aún sin contar con infraestructuras de transporte pero han adoptado otros mecanismos como estrategias de

mercado, mediantes las alianzas estratégicas con otras empresas para proporcionar los servicios lo antes posible y acaparar un mayor número de usuarios.

- La implementación de la tecnología MPLS en el backbone de una red prácticamente no tiene costos excesivos por su fácil adaptación a cualquier tecnología de red lo que si resulta un costo alto es la incorporación de la plataforma de IPTV y elementos de la capa de Control como el Softswitch y sus componentes, estos últimos para el diseño presentado no se consideraron estrictamente necesarios por el número de usuarios estimados para los dos primeros años ya que se mantendrá el mismo mecanismo de interconexión para la distribución de los servicios de voz a los usuarios finales.

5.2 RECOMENDACIONES

- El diseño se planteó en base a la infraestructura actual de la empresa, en el cual se siguió manteniendo la centralización actual de los nodos, sin embargo es aconsejable mientras crece la demanda por consiguiente la red crear subdominios dentro del dominio de la red propuesta para descentralizar la gestión y administración y poder satisfacer a los usuarios a nivel nacional.

- Se recomienda que la empresa esté continuamente incorporando nuevas tecnologías y adquiriendo equipamiento para ir migrando paulatinamente hacia redes NGN, en especial a nivel de usuario por ejemplo con la implementación de redes ópticas PON (Pasive Optical Network) que permiten un ancho de banda superior a 155Mbps, aumento de cobertura y mejora de la Calidad de Servicio debido a la inmunidad que presenta la fibra óptica a los ruidos electromagnéticos.

- La empresa debería invertir también en lo que respecta a infraestructura de transporte propia porque al alquilar a otros portadores dependen mucho de ellos debido a que si desea MEGADATOS implementar tecnologías tendrá que hacerlo con aquellas que sean compatibles con los portadores, lo ideal sería implementar también tecnologías

ópticas como DWDM mediante la cual una única fibra óptica puede acomodar cientos de señales y puede ser posible incrementar la capacidad de la red de transporte sin necesidad de hacer nuevos tendidos, para esto también se debe realizar un estudio sobre una extensión de MPLS para redes ópticas conocido como GMPLS.

- De la misma manera que se aconseja implementar tecnologías ópticas en las capas inferiores se recomienda robustecer las capas superiores como la de Control con la incorporación del Softswitch y sus componentes a medida que crece la demanda para ampliar la oferta de servicios multimedia e ir integrando varias tecnologías de redes como las WIMAX, 3.5G o 4G, HFC, PSTN y otras.

- Es conveniente antes de realizar el estudio de implementación que la empresa haga un estudio completo de Mercado y Financiero para conocer el porcentaje de aceptación de los servicios Triple Play, fijación de la tarifa y la relación Costo/Beneficio que se obtendrá.

- Para que los proveedores de servicios de Telecomunicaciones puedan ofrecer servicios Triple Play sobre la base legal, en el país se debe establecer un marco regulatorio para la convergencia ya que hasta ahora algunos de los servicios sobre IP han sido regularizados de manera independiente y considerados como servicios de valor agregado. Las nuevas leyes deben ser flexibles y formularse de acuerdo a los avances tecnológicos de los últimos años con una clara visión del futuro, estos acuerdos no deben ser anticompetitivos y deben establecerse en beneficio de todos los operadores y proveedores del país.

REFERENCIAS BIBLIOGRÁFICAS

TEXTOS

- Tanenbaum, A. (2003). *Redes de Computadoras*. (4ta Edición). México: Prentice Hall.
- Davidson, J. (2001). *Fundamentos de Voz sobre IP*. Madrid: Cisco Press.
- Sheppard, S. (2002). *Convergencia de las Telecomunicaciones*. McGraw-Hill.
- Keagy, S. (2001). *Integración de Redes de Voz y Datos*. Cisco Press.
- Stallings, W. (2004). *Comunicaciones y Redes de Computadores*. (7ma Edición). Madrid: Pearson-España.

DOCUMENTOS ESPECIALES

- Rosen E., Viswanathan A., Callon R. *Multiprotocol Label Switching Architecture*. RFC 3031. Enero 2001.
- Anderson, L. *LDP Specification*. IETF RFC 3036. Enero 2001.

DIRECCIONES ELECTRÓNICAS

CAPÍTULO 1

[1] [Y.2001] UIT-T Recomendación Y.2001, Redes de Próxima Generación. Recuperado en mayo 2009 de: http://radiogis.uis.edu.co/gestion/Bliblioteca/Articulos%20NGN/T-REC-Y.2001-200412-I!!PDF-S.pdf

[2] Quintana, B. (2003). *Red Nacional de Comunicaciones Públicas de voz de larga distancia basada en tecnología NGN/VoIP*. Tesis para optar por el título de Ingeniero Civil Electrónico. Universidad Técnica Federico Santa María. Valparaíso-Chile.

[3] URL: http://www.monografias.com/trabajos14/softswitch/softswitch.shtml.htm. Recuperado en septiembre de 2009.

[4] Clemente, R., Ferraris, G. *Automatic Switched Optical Networks: functionality and architectural components*. Recuperado en enero de 2010 de http://www.eurescom.de/~projects-workspace/P1000-series/P1012/presentations/pdf/2nd%20Hungarian%20WDM%20workshop.pdf

[5] NOKIA SIEMENS NETWORK. *Solución WIMAX móvil*. Recuperado en febrero de 2010 de: http://www.sec-nokiasiemensnetworks.com/demos/WiMax_esp.pdf

[6] URL: http://www.monografias.com/trabajos16/telefonia-senalizacion/telefonia- senalizacion.shtml. Recuperado en septiembre de 2009.

[7] URL: http://www.monografias.com/trabajos14/softswitch/softswitch.shtml. Recuperado en septiembre de 2009.

[8] Blacio, G., Jiménez E. y López P. (2004). *Diseño de una red WAN para transmitir voz sobre IP y su utilización futura como red alternativa para la telefonía fija en el Ecuador*. Tesis para optar por el título de Ingeniero en Electrónica y Telecomunicaciones. Escuela Superior Politécnica del Litoral. Recuperado en septiembre de 2009 de: http://www.dspace.espol.edu.ec/handle/123456789/7744

[9] URL: http://www.monografias.com/trabajos65/servicios-ldap-unal/servicios-ldap-unal.shtml. Recuperado en febrero de 2010.

[10] De Oliveira, S. (2004). *Una Propuesta de arquitectura MPLS/DiffServ para proveer mecanismos de Calidad de Servicio (QoS) en el transporte de telefonía IP*. Tesis Doctoral. Universidad Politécnica de Madrid. Recuperado en octubre de 2009 de: http://oa.upm.es/347

[11] Padilla, J. *IntServ*. Recuperado en febrero de 2010 de:

http://arantxa.ii.uam.es/~ferreiro/sistel2008/anexos/Diff&IntServ.pdf

[12] Znaty, S., Dauphin, J. y Geldwerth R. *IP Multimedia Subsystem: Principios y Arquitectura.* Recuperado en febrero de 2010 de: http://efort.com/media_pdf/IMS_ESP.pdf

[13] Huidobro, M. *IPTV, la televisión a través de Internet*. Recuperado en febrero de 2010 de: http://www.acta.es/articulos_mf/43039.pdf

CAPITULO 2

[14] ITU-T Recomendación G.1000. *Calidad de Servicio en Comunicaciones: Marco y Definiciones*. Recuperado en febrero de 2010 de: www.itu.int/itudoc/itu-t/wtsa-res/res2upda_ww9-es.doc

[15] URL: http://pedco2.uncoma.edu.ar/file.php/140/Presentaciones/Servicios_Diferenciados.pdf. Recuperado en febrero de 2010.

[16] Canalis, M. *MPLS "Multiprotocol Label Switching": Una Arquitectura de Backbone para la Internet del Siglo XXI".* Recuperado en octubre de 2009 de: http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MPLS.PDF

[17] URL: http://www.ramonmillan.com/documentos/mpls.pdf. Recuperado en octubre de 2009.

[18] Domínguez, M. *Soporte de Garantía de Servicio (GoS) sobre MPLS mediante Técnicas Activas.* Recuperado en enero de 2010 de: http://www.manolodominguez.com/projects/opensimmpls/content/common/pdf/documentation/gossobrempls.pdf

[19] Delfino, A., Rivero, S. y San Martín, M. *Ingeniería de Tráfico en redes MPLS*. Recuperado en enero de 2010 de: http://telcom2006.fing.edu.uy/trabajos/mvdtelcom-002.pdf

CAPITULO 3

[20] URL:
http://www.mtmnet.com/PDF_FILES/Cisco2950-EI_DataSheet.pdf. Recuperado en febrero de 2010.

[21] URL:
http://www.ciscosystems.kg/application/pdf/en/us/guest/products/ps628/c1650/ccmigration_09186a00801cfb71.pdf. Recuperado en febrero de 2010.

[22] URL:
http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_37_ey/configuration/guide/2960SCG.pdf. Recuperado en febrero de 2010.

[23] URL:
http://www.hcwt.com/cisco/cisco-catalyst-3750-information-sheet.pdf. Recuperado en marzo de 2010.

[24] URL:
http://www2.bt.com/static/i/media/pdf/catalyst_3550_ds.pdf. Recuperado en marzo de 2010.

[25] URL:
http://www.mdac.state.ms.us/ftp/MFC%20Information/Data%20Sheet%20-%20Cisco%20Catalyst%203560%20Switch.pdf. Recuperado en febrero de 2010.

[26] URL:
http://www.cisconation.info/en/US/prod/collateral/routers/ps368/product_data_sheet0900aecd8057f3ad.pdf. Recuperado en marzo de 2010.

[27] URL:
http://www.vsp.state.va.us/downloads/STARSContract/Appendix%2005%20-%2062%20-%20Cisco.pdf. Recuperado en marzo de 2010.

[28] URL:
http://www.vantage.com/pdfs/communications/cisco_3800_router.pdf. Recuperado en marzo de 2010.

[29] URL:
http://www.andovercg.com/datasheets/cisco-3700-routers.pdf. Recuperado en marzo de 2010.

[30] URL:
http://www.cisco.com/warp/public/cc/pd/as/as5300/prodlit/vffc_ds.pdf. Recuperado en marzo de 2010.

[31] SUPERINTENDENCIA DE TELECOMUNICACIONES
http://www.supertel.gov.ec. Recuperado en marzo de 2010.

[32] ASOCIACIÓN ECUATORIANA DE PROVEEDORES DE INTERNET
http://www.aeprovi.org.ec. Recuperado en enero de 2010.

CAPITULO 4

[33] NORTEL NETWORKS. *MPLS Basic Concepts*. Recuperado en marzo de 2010 de:
http://www.nortel.com/products/announcements/mpls/ipt/mpls_basics_nosound.html.

[34] Conde, L. (Marzo 2009). *Las Redes Metro y los servicios en las redes de Nueva Generación*. ETECSA. Recuperado en marzo de 2010.

[35] URL: REVISTA NETWORK WORDL
http://www.networkworld.es/. Recuperado en abril de 2010.

[36] Hinojosa, M., Herrera, F. (2009). *Diseño de una red MPLS utilizando el protocolo IPv6 para proveedores de servicios de Telecomunicaciones*. Tesis por el título de Ingeniería Electrónica y Telecomunicaciones. Escuela Politécnica Nacional. Quito. Recuperado de: http://bieec.epn.edu.ec:8180/dspace/handle/123456789/1344

[37] Marchán, J., Yánez, D. (2008). *Estudio y Diseño para la migración de una red Gigabit Ethernet de datos de una empresa portadora de servicios a la tecnología MPLS*. Tesis por el título de Ingeniería Electrónica y Telecomunicaciones. Escuela Politécnica Nacional. Quito. Recuperado de: http://bieec.epn.edu.ec:8180/dspace/handle/123456789/981

[38] URL:
http://telecom2101.comxa.com/1_8_IPTV.html. Recuperado en marzo de 2010.

[39] CALCULADORA ERLANG. http://www.erlang.com/calculator/lipb/. Recuperado en abril de 2010.

[40] Llumiquinga, D., Mullo, C. (2008) .*Análisis y Diseño del sistema redundante de F.O. Quito-Guayaquil para la red TELCONET S.A.* Tesis por el título de Ingeniería de Electrónica y Telecomunicaciones. Escuela Politécnica Nacional. Recuperado en marzo de 2010 de: http://bieec.epn.edu.ec:8180/dspace/handle/123456789/932

[41] URL:
IPHEADEND DE CISCO. http://tic-tac.teleco.uvigo.es/profiles/blogs/soluciones-end-to-end-cisco. Recuperado en abril de 2010.

[42] URL: MATRIXSTREAM
http://www.matrixstream.com/IPTV_VOD_H.264_IMX_solution_overview.php. Recuperado en abril de 2010.

[43] URL: CISCO
http://www.ciscosystems.com/web/YU/expo2009/docs/Digital_Video_Headend.pdf.
Recuperado en abril de 2010.

[44] URL: PORTAFOLIO ALCATEL
http://www.com-inter.ru/files/uploaded/mpls-ppt-eng23062009.pdf. Recuperado en abril de 2010.

[45] URL: SERIES CISCO 7200-7300
http://es.hardware.com/routers/routers-cisco/cisco-serie-7200-7300/. Recuperado en abril de 2010.

[46] URL: JUNIPER DATASHEET
http://www.juniper.net/us/en/local/pdf/datasheets/1000206-en.pdf. Recuperado en abril de 2010.

[47] URL: 3COM
http://www.3com.com/other/pdfs/products/en/400853.pdf. Recuperado en abril de 2010.

[48] URL: ROSA de CISCO
http://www.cisco.com/en/US/prod/collateral/video/ps9118/ps9128/7003710.pdf. Recuperado en abril de 2010.

[49] URL: Set-Top-Box
http://www.eaglebroadband.com. Recuperado en abril de 2010.

ANEXOS

ANEXO I. GLOSARIO DE TÉRMINOS

ATM: El Modo de Transferencia Asíncrona es una tecnología de Telecomunicación cuyo objetivo es aprovechar al máximo la capacidad de los sistemas de transmisión, la información no es transmitida y conmutada a través de canales asignados en permanencia, sino en forma de cortos paquetes (celdas ATM) de longitud constante y que pueden ser enrutados individualmente mediante el uso de los denominados canales virtuales y trayectos virtuales.

Backup: Sistema o equipo de respaldo que entra en funcionamiento cuando se ha producido fallas o inconvenientes en la red.

Best effort: Es un modelo simple de servicio, en el cual, una aplicación envía información cuando ella lo desea, en cualquier cantidad, sin ningún permiso requerido, y sin informar previamente a la red. En esta clase de servicio el proveedor no se compromete a brindar Calidad de Servicio.

Calidad de Servicio: Serie de cualidades de las redes y servicios de Telecomunicaciones para controlar las perturbaciones más comunes en las comunicaciones para ofrecer a los usuarios servicios más satisfactorios.

CEF: Tecnología de conmutación avanzada de Cisco, utilizada principalmente en las redes troncales y de Internet para aumentar la velocidad de la conmutación de paquetes.

Códec: Es la abreviatura de codificador-decodificador puede ser un software, hardware o una combinación de ambos, capaz de transformar un archivo con un flujo de datos o una señal a un formato más apropiado para la manipulación y transmisión.

Conmutación de circuitos: Es una conexión en la que los equipos de conmutación deben establecer un camino físico entre los medios de comunicación previo a la conexión entre los

usuarios, este camino permanece activo durante la comunicación y se libera al término de la conversación de los usuarios.

Conmutación de paquetes: Se establecen caminos lógicos para la transmisión de la información cuyos datos son unidades discretas formadas por bloques de longitud variable denominados paquetes.

Data Center: Aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización.

DWDM: Es un método de multiplexación en la que varias señales portadoras ópticas se transmiten por una única fibra óptica utilizando distintas longitudes de onda. Cada portadora óptica forma un canal óptico que puede ser tratado independientemente del resto de canales que comparten el medio y contener diferente tipo de tráfico. De esta manera se puede multiplicar el ancho de banda efectivo de la fibra óptica, así como facilitar comunicaciones bidireccionales.

Erlang: es una unidad adimensional utilizada en telefonía como una medida estadística del volumen de tráfico.

Escalabilidad: Propiedad de una red o proceso que indica su habilidad para poder hacerse más grande sin perder calidad en sus servicios.

Extranet: Es una red privada virtual que utiliza protocolos de Internet, protocolos de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, clientes o cualquier otro negocio u organización.

Frame Relay: Es una técnica de comunicación de paquetes a nivel WAN mediante retransmisión de tramas denominadas “frames” de una variedad de tamaños para redes de circuitos virtuales, introducida por la ITU.

Gatekeeper: Es una entidad que permite la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y unidades de control multipunto además de la gestión de ancho de banda.

GMPLS: Es una extensión de MPLS para las diferentes tecnologías de redes de transporte ópticas.

Intradominio: En un mismo Sistema Autónomo o dentro de la misma red de la organización.

Intranet: Es un conjunto de servicios de Internet dentro de una red local, es decir que es accesible sólo desde estaciones de trabajo internas y constituye un sistema de información dentro de una organización o empresa.

Jitter: Variación de los pulsos de la amplitud e intensidad de la señal en una transmisión digital. Inestabilidad o variabilidad del retardo.

Latencia: Se considera la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes.

Media Gateway Controller: Conocido como Softswitch.

Metro Ethernet: Es una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN/WAN de nivel 2, empleando interfaces Ethernet. Estas redes soportan una amplia gama de servicios, aplicaciones, contando con mecanismos donde se incluye soporte a tráfico en tiempo real, como puede ser Telefonía IP y Video IP. Las redes Metro Ethernet están soportadas principalmente por medios de transmisión guiados, como son el cobre y la fibra óptica con velocidades de 10Mbps, 20Mbps, 34Mbps, 100Mbps, 1Gbps y 10Gbps.

Overhead: Es el desperdicio de ancho de banda causado por la información adicional (control, secuencia, etc.) que debe viajar además de la carga útil en los paquetes de un medio de comunicación.

Peer to peer: Conocida también como P2P, redes entre pares o redes punto a punto en las que no existen ni ordenadores clientes ni ordenadores que hagan de servidor permitiendo el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados conocidos como nodos.

PLC: Power Line Communications es un término inglés que puede traducirse por comunicaciones mediante cable eléctrico y que se refiere a las diferentes tecnologías que utilizan las líneas de energía eléctrica convencionales para transmitir señales para propósitos de comunicación. La tecnología PLC aprovecha la red eléctrica para convertirla en una línea digital de alta velocidad de transmisión de datos, permitiendo, entre otras cosas, el acceso a Internet mediante banda ancha.

PPP: Point-to-Point Protocol es un protocolo que permite establecer una comunicación a nivel de enlace estandarizado en la RFC 1661. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso.

Protocolos de Túnel: Se conoce con este nombre a ciertos protocolos de red que encapsulan a otro protocolo. Así, el protocolo A es encapsulado dentro del protocolo B, de forma que el primero considera al segundo como si estuviera en el nivel de enlace de datos, esta técnica se suele utilizar para trasnportar un protocolo determinado a través de una red que en condiciones normales no lo aceptaría y uno de los usos de estos protocolos más importantes es la creación de redes privadas virtuales.

Proxy: Es un sistema de software o hardware que permite la conexión de una LAN entera al exterior con sólo una dirección IP de salida, para proveer el acceso a Internet de todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado al proveedor teniendo la funcionalidad adicional, como puede ser la de mantener los resultados obtenidos por ejemplo de una página web en una caché que permita acelerar sucesivas consultas coincidentes.

SDH/SONET: Es un estándar internacional desarrollado por el Working Group T1X1 de ANSI para líneas de Telecomunicación de alta velocidad sobre fibra óptica (desde 51,84 Mbps a 2,488 Gbps). SONET es su nombre en EE.UU. y SDH es su nombre europeo. Estas normas definen señales ópticas estandarizadas, una estructura de trama síncrona para el tráfico digital multiplexado y los procedimientos de operación para permitir la interconexión de terminales mediante fibras ópticas, especificando para ello el tipo monomodo.

SDSL: La tecnología SDSL es una variante de la DSL y se trata de una línea simétrica permanente con igual ancho de banda para subida de datos (uploads) y para bajada de datos (downloads) con velocidades de hasta 2.048 kbps.

Servicios Portadores: Son servicios que proveen al usuario una capacidad necesaria para el transporte de la información sin importar su contenido y aplicación.

Servidor de Directorio: Es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los recursos de red y permite a los administradores gestionar el acceso de los usuarios. Además, los servicios de directorio actúan como una capa de abstracción entre los usuarios y los recursos compartidos.

Spanning Tree: Es un protocolo de red de nivel 2 de la capa OSI, estandarizada por el IEEE (IEEE 802.1D). Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de bucles.

Spread Spectrum: El espectro ensanchado es una técnica de modulación empleada en Telecomunicaciones para la transmisión de datos, por lo común digitales y por radiofrecuencia.

Streaming: Es una nueva técnica 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 pudiendo observar en tiempo real.

Sumarizar: O resumen de rutas es un proceso que realizan los routers por el cual toman un grupo de direcciones de redes contiguas y las resumen en una sola dirección de red común a todas esas redes. La principal ventaja es la optimización del enrutamiento ya que los routers tienen que mantener menos entradas en sus tablas y en consecuencia se gana en estabilidad, ahorro de recursos, eficiencia y tiempos de proceso. Los protocolos sin clase EIGRP, OSPF, RIP v.2, IS-IS y BGP soportan resumen de rutas.

Tasa de bits: Define el número de bits que se transmiten por unidad de tiempo a través de un sistema de transmisión digital o entre dos dispositivos digitales siendo la velocidad de transferencia de datos.

Token Ring: Es una arquitectura de red desarrollada por IBM en los años 1970 que propone una topología lógica en anillo y técnica de acceso de paso de testigo por medio de una unidad de acceso de estación múltiple MSAU que permite a la red verse como si fuera una estrella. Token Ring se recoge en el estándar IEEE 802.5 y actualmente ya no es empleada para el diseño de redes por la popularización de Ethernet.

Ubicuo: Define la cualidad de existir en cualquier lugar simultáneamente. Las redes ubicuas permiten a los usuarios acceder a Internet desde cualquier sitio y en cualquier momento.

VRF: Es una tabla de ruteo virtual compuesta de una tabla de ruteo IP y de una tabla de reenvío (CEF), la VRF se asocia a una VPN y determina el acceso del cliente.

ANEXO II. CONFIGURACIONES

1. CONFIGURACIÓN DE LOS ROUTERS LER

LER1 (UIO)

```
hostname Ler1-uio
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
interface FastEthernet0/0
 ip address 192.168.10.14 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 172.16.1.0 0.0.0.255 area 1
 network 192.168.10.12 0.0.0.3 area 1
```

LER2 (GYE)

```
hostname Ler-gye
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
interface FastEthernet0/0
 ip address 192.168.10.18 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
```

```
 mpls ip
!
interface FastEthernet0/1
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 172.16.2.0 0.0.0.255 area 2
 network 192.168.10.16 0.0.0.3 area 2
```

LER3 (CUE)

```
hostname Ler-cue
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
interface FastEthernet0/0
 ip address 192.168.10.22 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet0/1
 ip address 172.16.3.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 172.16.3.0 0.0.0.255 area 3
 network 192.168.10.20 0.0.0.3 area 3
```

2. CONFIGURACIÓN DE LOS ROUTERS LSR

LSR1 (UIO)

```
hostname Lsr1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
```

```
memory-size iomem 5
ip cef
!
interface FastEthernet0/0
 ip address 192.168.10.2 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet0/1
 ip address 192.168.10.9 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet1/0
 ip address 192.168.10.13 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 192.168.10.0 0.0.0.3 area 0
 network 192.168.10.8 0.0.0.3 area 0
 network 192.168.10.12 0.0.0.3 area 1
```

LSR2 (GYE)

```
hostname Lsr2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet0/1
```

```
 ip address 192.168.10.5 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet1/0
 ip address 192.168.10.17 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 192.168.10.0 0.0.0.3 area 0
 network 192.168.10.4 0.0.0.3 area 0
 network 192.168.10.16 0.0.0.3 area 2
```

LSR3 (CUE)

```
hostname Lsr3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
interface FastEthernet0/0
 ip address 192.168.10.10 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet0/1
 ip address 192.168.10.6 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet1/0
 ip address 192.168.10.21 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
```

```
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 192.168.10.4 0.0.0.3 area 0
 network 192.168.10.8 0.0.0.3 area 0
 network 192.168.10.20 0.0.0.3 area 3
```

3. QoS MEDIANTE LA IMPLEMENTACIÓN DE DIFFSERV

A continuación se presentan los fragmentos de configuración en los equipos para la implementación de DiffServ en el backbone MPLS a excepción del LER1 cuya configuración se encuentra detallada en el capítulo 4.

FRAGMENTO DE CONFIGURACIÓN EN EL ROUTER LSR1

```
!
class-map match-all mpls-in
 match mpls experimental topmost 3
!
policy-map mpls-in
 class mpls-in
  set mpls experimental topmost 2
!
interface FastEthernet1/0
 service-policy input mpls-in
!
```

FRAGMENTO DE CONFIGURACIÓN EN EL ROUTER LSR2

La misma configuración corresponde también al LSR3 de Cuenca.

```
!
class-map match-all MPLS-AF11
  match mpls experimental topmost 0
class-map match-all MPLS-AF12
  match mpls experimental topmost 1
class-map match-all MPLS-AF21
  match mpls experimental topmost 2
class-map match-all MPLS-AF22
  match mpls experimental topmost 3
class-map match-all MPLS-AF31
  match mpls experimental topmost 4
class-map match-all MPLS-AF32
  match mpls experimental topmost 5
```

```
 class-map match-all qos-group-AF11
  match qos-group 0
class-map match-all qos-group-AF12
  match qos-group 1
class-map match-all qos-group-AF21
  match qos-group 2
class-map match-all qos-group-AF22
  match qos-group 3
class-map match-all qos-group-AF31
  match qos-group 4
class-map match-all qos-group-AF32
  match qos-group 5
!
policy-map politica-3
 class MPLS-AF11
   set qos-group mpls experimental topmost
 class MPLS-AF12
   set qos-group mpls experimental topmost
 class MPLS-AF21
   set qos-group mpls experimental topmost
 class MPLS-AF22
   set qos-group mpls experimental topmost
 class MPLS-AF31
   set qos-group mpls experimental topmost
 class MPLS-AF32
   set qos-group mpls experimental topmost

policy-map politica-4
 class qos-group-AF11
   bandwidth percent 5
   random-detect
   set mpls experimental topmost qos-group
 class qos-group-AF12
   bandwidth percent 10
   random-detect
   set mpls experimental topmost qos-group
 class qos-group-AF21
   bandwidth percent 10
   random-detect
   set mpls experimental topmost qos-group
 class qos-group-AF22
   bandwidth percent 15
   random-detect
   set mpls experimental topmost qos-group
 class qos-group-AF31
   bandwidth percent 15
```

```
   random-detect
   set mpls experimental topmost qos-group
 class qos-group-AF32
   bandwidth percent 20
   random-detect
   set mpls experimental topmost qos-group
!
interface FastEthernet0/0
 service-policy input politica-3
!
interface FastEthernet1/0
 service-policy output politica-4
!
```

FRAGMENTO DE CONFIGURACIÓN EN EL ROUTER LER2

Para el router borde LER3 de Cuenca se utiliza la misma configuración.

```
!
class-map match-all MPLS-AF11
  match mpls experimental topmost 0
class-map match-all MPLS-AF12
  match mpls experimental topmost 1
class-map match-all MPLS-AF21
  match mpls experimental topmost 2
class-map match-all MPLS-AF22
  match mpls experimental topmost 3
class-map match-all MPLS-AF31
  match mpls experimental topmost 4
class-map match-all MPLS-AF32
  match mpls experimental topmost 5

class-map match-all qos-group-AF11
  match qos-group 0
class-map match-all qos-group-AF12
  match qos-group 1
class-map match-all qos-group-AF21
  match qos-group 2
class-map match-all qos-group-AF22
  match qos-group 3
class-map match-all qos-group-AF31
  match qos-group 4
class-map match-all qos-group-AF32
  match qos-group 5
!
policy-map politica-5
```

```
 class MPLS-AF11
   set qos-group mpls experimental topmost
 class MPLS-AF12
   set qos-group mpls experimental topmost
 class MPLS-AF21
   set qos-group mpls experimental topmost
 class MPLS-AF22
   set qos-group mpls experimental topmost
 class MPLS-AF31
   set qos-group mpls experimental topmost
 class MPLS-AF32
   set qos-group mpls experimental topmost
```

policy-map politica-6

```
 class qos-group-AF11
   bandwidth percent 5
   random-detect
   set precedence qos-group
 class qos-group-AF12
   bandwidth percent 10
   random-detect
   set precedence qos-group
 class qos-group-AF21
   bandwidth percent 10
   random-detect
   set precedence qos-group
 class qos-group-AF22
   bandwidth percent 15
   random-detect
   set precedence qos-group
 class qos-group-AF31
   bandwidth percent 15
   random-detect
   set precedence qos-group
 class qos-group-AF32
   bandwidth percent 20
   random-detect
   set precedence qos-group
!
interface FastEthernet0/0
 service-policy input politica-5
!
interface FastEthernet0/1
service-policy output politica-6
```

4. CONFIGURACIÓN DE INGENIERÍA DE TRÁFICO

Con la siguiente configuración se habilita un túnel virtual en el que se designa un ancho de banda y una prioridad, lo cual brinda otro mecanismo para ofrecer Calidad de Servicio en el envío de los paquetes por la red. Los comandos utilizados se presentan a continuación:

4.1 CONFIGURACIÓN EN EL LER1

Configuración Global

```
Ler1-uio#config t
Ler1-uio(config)#mpls traffic-eng tunnels
Ler1-uio(config)#exit
```

Configuración de una interfaz

Se requiere una interfaz a ser utilizada como router ID, ésta debe ser una interfaz de loopback y su utilidad es siempre estar arriba sin importar el estado de las otras interfaces.

```
Ler1-uio#config t
Ler1-uio(config)#interface Loopback0
Ler1-uio(config-if)#ip address 23.1.1.1 255.255.255.255
Ler1-uio(config-if)#no ip directed-broadcast
Ler1-uio(config-if)#exit
```

Luego se habilita mpls traffic-eng tunnels dentro del proceso OSPF

```
Ler1-uio#config t
Ler1-uio(config)#router ospf 1
Ler1-uio(config-router)#mpls traffic-eng area 1
Ler1-uio(config-router)#mpls traffic-eng router-id Loopback0
Ler1-uio(config-router)#exit
```

Se configura la reserva de recursos tanto en las interfaces de entrada como de salida

```
Ler1-uio#config t
Ler1-uio(config)#int f0/0
Ler1-uio(config-if)#mpls traffic-eng tunnels
Ler1-uio(config-if)#ip rsvp bandwidth 140000 140000 sub-pool 60000
Ler1-uio(config-if)#exit
```

Configuración de Túneles (ruta dinámica)

```
Ler1-uio(config)#
```

Ler1-uio(config)#interface Tunnel1
Ler1-uio(config-if)#bandwidth 110000
Ler1-uio(config-if)#ip unnumbered Loopback0
Ler1-uio(config-if)#tunnel destination 27.1.1.1
Ler1-uio(config-if)#tunnel mode mpls traffic-eng
Ler1-uio(config-if)#tunnel mpls traffic-eng priority 0 0
Ler1-uio(config-if)#tunnel mpls traffic-eng bandwidth sub-pool 40000
Ler1-uio(config-if)#tunnel mpls traffic-eng path-option 1 dynamic *(puede ser estática)*

Los paquetes en este caso destinados a la subred 172.16.3.0 son enviados por el subtúnel mediante ruteo estático

Ler1-uio(config)#ip route 172.16.3.0 255.255.255.0 Tunnel1
Ler1-uio(config)#exit

4.2 CONFIGURACIÓN EN EL LSR1

Lsr1#config t
Lsr1(config)#mpls traffic-eng tunnels
Lsr1(config)#interface Loopback0
Lsr1(config-if)#ip address 24.1.1.1 255.255.255.255
Lsr1(config-if)#exit

Lsr1(config)#router ospf 1
Lsr1(config-router)#mpls traffic-eng area 0
Lsr1(config-router)#mpls traffic-eng router-id Loopback0
Lsr1(config-router)#exit

Lsr1(config)#int f1/0
Lsr1(config-if)#mpls traffic-eng tunnels
Lsr1(config-if)#ip rsvp bandwidth 140000 140000 sub-pool 60000
Lsr1(config-if)#exit

Lsr1(config)#int f0/1
Lsr1(config-if)#mpls traffic-eng tunnels
Lsr1(config-if)#ip rsvp bandwidth 140000 140000 sub-pool 60000
Lsr1(config-if)#exit

4.3 CONFIGURACIÓN EN EL LSR3

Lsr3(config)#mpls traffic-eng tunnels
Lsr3(config)#interface Loopback0
Lsr3(config-if)#ip address 25.1.1.1 255.255.255.255
Lsr3(config-if)#exit

```
Lsr3(config)#router ospf 1
Lsr3(config-router)#mpls traffic-eng area 0
Lsr3(config-router)#mpls traffic-eng router-id Loopback0
Lsr3(config-router)#exit

Lsr3(config)#int f0/0
Lsr3(config-if)#mpls traffic-eng tunnels
Lsr3(config-if)#ip rsvp bandwidth 140000 140000 sub-pool 60000
Lsr3(config-if)#exit

Lsr3(config)#int f1/0
Lsr3(config-if)#mpls traffic-eng tunnels
Lsr3(config-if)#ip rsvp bandwidth 140000 140000 sub-pool 60000
Lsr3(config-if)#exit
```

4.4 CONFIGURACIÓN EN EL LER3

```
Ler-cue(config)#mpls traffic-eng tunnels
Ler-cue(config)#interface Loopback0
Ler-cue(config-if)#ip address 27.1.1.1 255.255.255.255
Ler-cue(config-if)#exit

Ler-cue(config)#router ospf 1
Ler-cue(config-router)#mpls traffic-eng area 3
Ler-cue(config-router)#mpls traffic-eng router-id Loopback0
Ler-cue(config-router)#exit

Ler-cue(config)#int f0/0
Ler-cue(config-if)#mpls traffic-eng tunnels
Ler-cue(config-if)#ip rsvp bandwidth 140000 140000 sub-pool 60000
Ler-cue(config-if)#exit
```

Rutas Explícitas

En el nodo de cabecera se configura las características del túnel como la prioridad y el ancho de banda, esta configuración ayuda a establecer manualmente los nodos implicados en el trayecto en caso de que el protocolo de enrutamiento falle. A continuación se indica de manera explícita la ruta que seguirá el túnel.

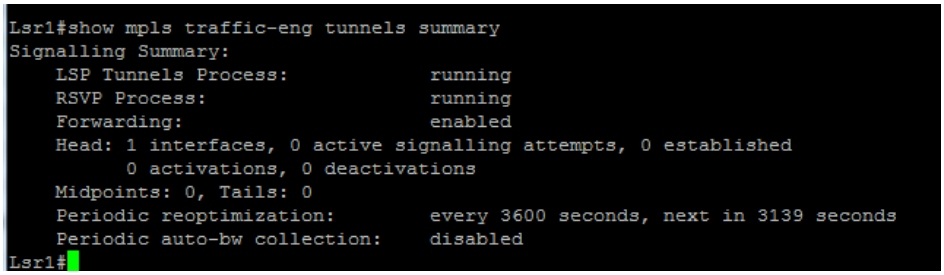
```
Ler1-uio(config-if)#tunnel mpls traffic-eng path-option 1 explicit name ruta-larga
Ler1-uio(config)#ip explicit-path name ruta-larga enable
        next address [IP]
        next address [IP]
```

Para verificar la configuración de Ingeniería de Tráfico se deben aplicar los siguientes comandos:

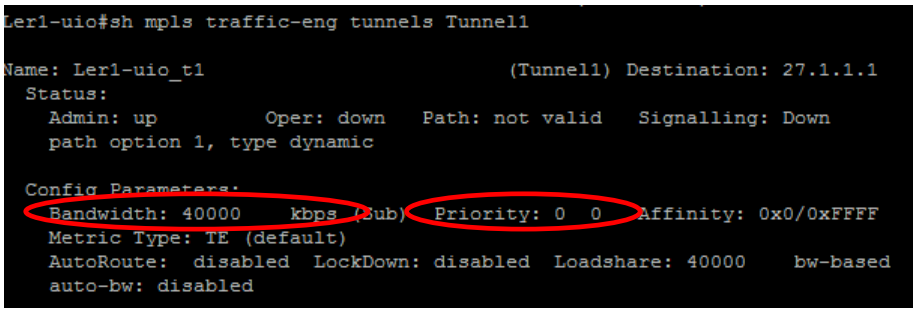
- show mpls interface
- show mpls traffic-eng tunnels summary
- show mpls traffic-eng tunnels tunnel1
- show mpls traffic-eng tunnels brief

4.5 PRUEBAS DE LA RED CON INGENIERÍA DE TRÁFICO

A continuación se muestra que el proceso LSP túnel está activado mediante el comando *"show mpls traffic-eng tunnels summary"*.



En el router LER1 se configuró un LSP con un túnel, éste túnel tiene un ancho de banda y una prioridad asignados dependiendo del tipo de tráfico, en la siguiente figura se puede observar estas configuraciones para el Tunnel1.



5. CONFIGURACIÓN VPN/MPLS

MPLS permite construir VPNs en redes de paquetes utilizando un modelo de puertos en el que los routers CE envían sus rutas a los routers PE, siendo el proveedor del servicio el que lo encamina hacia el destino sin la necesidad de utilizar túneles punto a punto ofreciendo un servicio no orientado a conexión.

5.1 CONFIGURACIÓN DE BGP EN LOS ROUTERS CE

El router CE o router borde del cliente puede o no estar configurado con MPLS, depende de los requerimientos propios de la red interna del cliente, pero si es necesario que en el modo de configuración global se implemente ip cef.

```
CE-1#configure terminal
CE-1(config)#router bgp 65001
CE-1(config-router)#network 10.0.0.0
CE-1(config-router)#redistribute connected
CE-1(config-router)# neighbor 10.0.1.1 remote-as 65000
CE-1(config-router)# no auto-summary
CE-1(config-router)#exit
```

5.2 CONFIGURACIÓN DE LOS ROUTERS PE (LER)

Luego de que los routers CE envían las rutas a los routers PE, los PE trabajan con la información de BGP dentro del Sistema Autónomo del proveedor para intercambiar las rutas de cada VPN, realizándose las siguientes configuraciones:

```
PE-1#configure terminal
```

Creación de una Loopback en el router PE

```
PE-1(config)# interface Loopback0
PE-1(config-if)#ip address 1.1.1.1 255.255.255.255
PE-1(config-if)#no shutdown
```

Inclusión de la Loopback en la red del proveedor con OSPF

```
PE-1(config)#router ospf 1
PE-1(config-router)#network 1.1.1.1 255.255.255.255
PE-1(config-router)#exit
```

5.2.1 Definición de las VRFs

Las VRFs (Virtual Forwarding and Routing), son tablas de ruteo virtual que permite tener varias tablas de rutas independientes en un router, estas tablas virtuales determinan la membresía de un cliente de una VPN. En las siguientes líneas se configura el distinguidor de ruta y a continuación las route targets para la VRF.

```
PE-1(config)#ip vrf empresa-1
PE-1(config-vrf)#rd 100:100
PE-1(config-vrf)#route-target export 100:100
PE-1(config-vrf)#route-target import 100:100
PE-1(config-vrf)#exit
```

5.2.2 Configuración de VRF en la interfaz del router PE

Se debe asociar una VRF a una interfaz del router PE de frente con el router del cliente.

```
PE-1(config)#interface FastEthernet0/1
PE-1(config-if)#ip vrf forwarding empresa-1
PE-1(config-if)#exit
```

5.3 CONFIGURACIÓN DEL PROTOCOLO DE RUTEO ENTRE EL CE Y PE

En el router PE se configura BGP y como vecino la interfaz loopback del router PE-2 de destino.

```
PE-1(config)#router bgp 65000
PE-1(config-router)#neighbor 2.2.2.2 remote-as 65000
PE-1(config-router)#neighbor 2.2.2.2 update-source Loopback0
PE-1(config-router)#no auto-summary
PE-1(config-router)#exit
```

Se configura la familia de direcciones BGP y se activa los anuncios de VPNv4 hacia el destino.

```
PE-1(config-router)#address-family vpnv4
PE-1(config-router-af)#neighbor 2.2.2.2 activate
PE-1(config-router-af)#neighbor 2.2.2.2 send-community both
PE-1(config-router-af)#neighbor 2.2.2.2 next-hop-self
```

PE-1(config-router-af)#exit-address-family

Se crea la familia de direcciones para una VRF configurando los parámetros BGP para la sesión entre el PE y CE para asegurarse de que las direcciones aprendidas a través de BGP sobre un router PE desde un CE sean tratadas como direcciones VPN-IPv4.

```
PE-1(config-router)#address-family ipv4 vrf empresa-1
PE-1(config-router-af)#neighbor 10.0.1.2 remote-as 65001
PE-1(config-router-af)#neighbor 10.0.1.2 activate
PE-1(config-router-af)#neighbor 10.0.1.2 as-override
PE-1(config-router-af)#exit-address-family
PE-1(config-router-af)#end
```

6. COMANDOS PARA LA VERIFICACIÓN DE MPLS

COMANDO	FUNCIÓN
show ip cef summary	Indica un resumen de la tabla de forwarding.
show ip cef [IP]	Muestra la tabla de forwarding. Si se indica una IP, muestra detalles de la entrada de forwarding para esa IP.
show mpls ip binding	Muestra para cada prefijo las etiquetas conocidas recibidas de distintos vecinos (se estén usando o nó).
show mpls interfaces [detail]	Muestra información de MPLS de las distintas interfaces (protocolo de etiquetas, si está corriendo MPLS, etc). Con la palabra opcional "detail" muestra más información de cada interfaz (MTU, etc).
show mpls ldp neighbor [detail]	Muestra información de los vecinos LDP (Identidad, datos de la conexión TCP, IPs asociadas al vecino, etc).
show mpls label range	Para verificar el rango de etiquetas asignadas.
show tag forwarding [detail]	Muestra si las etiquetas han sido asignadas por cada ruta.
show tag interface [detail]:	Permite verificar si MPLS está habilitado en las interfaces.

ANEXO III. INDICADORES DE RENTABILIDAD

Antes de calcular los indicadores de rentabilidad es necesario representar el Flujo de Caja donde se presentan los ingresos y egresos en períodos iguales. Tanto los ingresos como los egresos se obtienen de los diferentes análisis del proyecto, calculado tanto para usuarios corporativos como residenciales tomando en cuenta el crecimiento anual de la demanda del 21%. En la tabla a. se muestra los ingresos por los nuevos servicios.

	INSTALACIÓN	SERVICIO
RESIDENCIAL	100 USD	70 USD
CORPORATIVO	300 USD	400 USD

Tabla a. Costos de los servicios

En la tabla b. se puede apreciar el ingreso que se obtendrá por concepto de Instalación e Ingreso anual de las mensualidades del servicio, en el ítem Instalación se ha tomado en cuenta únicamente los nuevos usuarios por año, por ejemplo en el segundo año el total de usuarios se estima en 478 pero con relación al primer año son 85 los nuevos usuarios que se les instalará el servicio.

TIEMPO (Años)	USUARIOS	INSTALACIÓN (USD)	INGRESO MENSUAL (USD)	INGRESO ANUAL (USD)
1	393	117900	157200	1886400
2	478 (85n)	25500	191200	2294400
3	578 (100 n)	30000	231200	2774400
4	699 (121 n)	36300	279600	3355200
5	845 (146 n)	43800	338000	4056000

Tabla b. Ingresos por usuarios Corporativos

En la tabla c. de igual manera se presenta los ingresos por concepto de Instalación y el valor anual que representan las mensualidades del servicio para los clientes residenciales.

TIEMPO (Años)	USUARIOS	INSTALACIÓN (USD)	INGRESO MENSUAL (USD)	INGRESO ANUAL (USD)
1	200	20000	14000	168000
2	242 (42 n)	4200	16940	203280
3	293 (51 n)	5100	20510	246120
4	355 (62 n)	6200	24850	298200
5	430 (75 n)	7500	30100	361200

Tabla c. Ingresos por usuarios Residenciales

Para realizar el Flujo de Caja se toman en cuenta los Ingresos y Egresos. Como Ingresos están los valores obtenidos por la instalación y mensualidades de los servicios considerados anualmente y como Egresos se consideran los valores por concepto de equipos, fibra óptica y todos los valores involucrados para la implementación del proyecto. En el tercer año se ha considerado la adquisición de un softswitch que permitirá el enrutamiento de las llamadas IP a la PSTN sin la interconexión actual a CNT.

Además como egreso también se toma en cuenta los valores a cancelar anualmente por razón de un préstamo bancario que realizaría la empresa para financiar el proyecto a una tasa de interés anual del 12 % para cinco años.

FLUJO DE CAJA

	INICIO	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
INGRESOS						
INSTALACIÓN (CORP+RESID)		137900	29700	35100	42500	51300
SERVICIO (CORP+RESD)		2054400	2497680	3020520	3653400	4417200
TOTAL INGRESOS		2192300	2527380	3055620	3695900	4468500
EGRESOS						
EQUIPOS	1045035			40000		
TENDIDO DE F.O	1000000					
INGENIERÍA & INSTALACIÓN	9510					
OPERACIÓN & MANTENIMIENTO		204504	204504	204504	204504	204504
PAGO A CARRIER	3000	13600	14800	16200	22300	45900
INTERCONEXIÓN		3500	4100	5600	8350	10050
PRÉSTAMO BANCARIO		560000	560000	560000	560000	560000
OTROS GASTOS DE EMPRESA		8000	13000	18000	23000	28000
I.V.A (12%)	246905	94752	95568	101316	98178	101814
TOTAL EGRESOS	2304450	884356	891972	945620	916332	950268
FLUJO NETO (USD)	-2304450	1307944	1635408	2110000	2779568	3518232

Para conocer sobre la rentabilidad esperada del proyecto se analizan los siguientes indicadores para determinar su viabilidad. Estos indicadores son:

- Valor Actual Neto (VAN)
- Tasa Interna de Retorno (TIR)
- Relación Beneficio Costo (B/C)
- Período de Recuperación de la Inversión (PRI)

1. VALOR ACTUAL NETO

Se entiende por VAN a la diferencia entre el valor actual de los ingresos esperados de una inversión y el valor actual de los egresos. El proyecto es rentable cuando se tiene un VAN positivo, cuando se tiene un VAN igual a cero es indiferente aceptar o no el proyecto, pero si el VAN es menor a cero el proyecto no es viable, para calcularlo se utiliza la siguiente fórmula:

$$VAN = -I_O + \sum_{n=1}^{m} \frac{Fn}{(1+i)^n}$$

Donde:

I_0= Inversión Inicial

F_n= Flujos Netos

m= Número de períodos considerados

i= Tasa de interés

La tasa de interés a utilizarse es la vigente en el mercado i=11,82 % anual, considerando que no varía en los próximos 5 años, tiempo en el que se realiza el análisis de rentabilidad.

$$VAN = -2304450 + \frac{1307944}{(1+0{,}1182)^1} + \frac{1635408}{(1+0{,}1182)^2} + \frac{2110000}{(1+0{,}1182)^3} + \frac{2779568}{(1+0{,}1182)^4} + \frac{3518232}{(1+0{,}1182)^5}$$

$$VAN = 5\,472\,622\ USD$$

Como el VAN es >0, entonces el proyecto es rentable.

2. TASA INTERNA DE RETORNO

Es la tasa de interés que iguala en el tiempo los ingresos y egresos de un flujo de caja; es decir, el TIR es el tipo de interés que anula el VAN de una inversión, haciéndolo cero. Un proyecto es rentable cuando el TIR es mayor que la tasa de interés mínima vigente en el mercado. Para calcular el TIR se utiliza la siguiente fórmula:

$$-I_0 + \sum_{n=1}^{m} \frac{Fn}{(1+r)^n} = 0$$

Donde:

I_0= Inversión Inicial

F_n= Flujos Netos

m= Número de períodos totales

r= Tasa interna de retorno

$$-2304450 + \frac{1307944}{(1+r)^1} + \frac{1635408}{(1+r)^2} + \frac{2110000}{(1+r)^3} + \frac{2779568}{(1+r)^4} + \frac{3518232}{(1+r)^5}$$

Utilizando MATLAB se encuentra el valor de r=0.71, es decir el valor TIR.

```
>> d=[2304450 10214256 16177316 8180612 -5615318 -9046702];
>> roots (d)

ans =

  -1.7789 + 0.5183i
  -1.7789 - 0.5183i
  -0.7934 + 0.9879i
  -0.7934 - 0.9879i
   0.7122

>>
```

$$TIR = 71\%$$

Como es mayor que la tasa de interés utilizada de 11,82%, entonces el proyecto es viable.

3. RELACIÓN BENEFICIO COSTO

Esta relación determina la rentabilidad del proyecto en términos generales, el resultado expresa el dinero ganado en cada dólar que se invierte en el proyecto y se calcula de la siguiente manera:

$$B/C = \frac{\sum_1^n VAN_n}{I_0}$$

Donde:

VAN= Valor actual neto

n= Duración del proyecto en años

I_0= Inversión Inicial

Reemplazando por los resultados del proyecto:

$$^{B}/_{C} = \frac{5472622}{2304450} = 2{,}4\ USD$$

Por cada dólar invertido en el proyecto se gana 2,4 dólares al año.

4. PERÍODO DE RECUPERACIÓN DE LA INVERSIÓN

Este período indica el tiempo necesario para recuperar el capital invertido; es decir, entre más corto sea el periodo para la recuperación de lo invertido más viable es el proyecto. Una forma de calcular el PRI es ir acumulando los flujos netos hasta llegar a cubrir la inversión. En la tabla d. se muestran los flujos netos y acumulados.

AÑO	Flujos Netos (USD)	Flujos Netos Acumulados (USD)
1	1307944	1307944
2	1635408	2943352
3	2110000	5053352
4	2779568	7832920
5	3518232	11351152

Tabla d. Flujos Netos y Acumulados

En la tabla d. se observa que el flujo neto acumulado en el año 2 es mayor que la inversión, por lo tanto el período de recuperación de la inversión se daría aproximadamente entre el primer y segundo año. Para determinar el PRI con mayor exactitud se escoge el flujo neto del año 1 donde aún no se cubre la inversión y se lo resta de la inversión.

$$2304450 - 1307944 = 996506$$

Se divide el valor no recuperado en el año 1 para el flujo neto del año 2 y se tiene:

$$\frac{996506}{1635408} = 0{,}61$$

Este valor se lo suma al número de años a partir de la inversión que sería de un año:

$$PRI = 1 \text{ año} + 0{,}61 \text{ años}$$
$$0{,}61 \text{ x } 12 \text{ meses} = 7{,}32 \text{ meses}$$
$$0{,}32 \text{ x } 30 \text{ días} = 10 \text{ días}$$

Por lo tanto el PRI es de 1.61 años, es decir la inversión se recupera en 1 año, 7 meses y 10 días.

ANEXO IV. MANUAL GNS3

Partes de este tutorial fueron tomados del excelente tutorial de Dynagen de Greg Anuzelli.

1. INTRODUCCIÓN

GNS3 es un simulador gráfico de redes que permite diseñar fácilmente topologías de red y luego ejecutarlas. Hasta este momento GNS3 soporta el IOS de routers, ATM/Frame Relay switches Ethernet y PIX firewalls. Para realizar esta magia, GNS3 está basado en:

- ***Dynamips***

  Es un emulador de routers Cisco para las plataformas 1700, 2600, 3600, 3700 y 7200 ejecutándo imágenes de IOS estándar. También provee un switch virtual simple, no emula switches Catalyst (aunque si emula la NM-16ESW).

- ***Dynagen***

  Es un front end basado en texto para Dynamips elaborado por Greg Anuzelli para interactuar con Dynamips. GNS3 también utiliza el formato .INI de configuración e integra la consola de administración de Dynagen que permite a los usuarios listar los dispositivos, suspender y recargar instancias, determinar los valores de Idle-PC, realizar capturas, entre otros.

- ***Pemu***

  Un servidor de seguridad PIX de Cisco, para salvar las configuraciones.

2. INSTALANDO GNS3

GNS3 se ejecuta en Windows, Linux y Mac OS X y requiere de las siguientes dependencias:

- Qt >= 4.3, disponible en: http://trolltech.com/developer/downloads/qt/inex

- Python >= 2.4, disponible en: http://www.python.org
- Sip>=4.5, si se necesita compilar PyQt, disponible en: http://www.riverbankcomputing.co.uk/sip
- PyQt >= 4.1 disponible en: http://www.riverbankcomputing.co.uk/pyqt

Existe un solo instalador para Windows que incluye WinPcap, Dynamips, Pemu y una versión compilada de GNS3, eliminando de esta manera el tener que instalar Python y Qt. Los usuarios de Windows deben instalar el paquete Windows all-in-one. Esto provee lo necesario para que GNS3 se ejecute en máquinas locales o remotas.

Los usuarios Linux deben descargar Dynamips y extraerlo en alguna ubicación, luego instalar las dependencias de GNS3 y finalmente ejecutar GNS3. Los usuarios Debian/Ubuntu pueden instalar el paquete python-qt4 o instalar el paquete GNS3 .deb siguiendo las instrucciones de http://gpl.code.de/oswiki/GplcodedeApt.

3. IMÁGENES IOS

En Windows, la imagen se debe ubicar en C:\Program Files\Dynamips\images o en cualquier ubicación que se desee, en los laboratorios se buscará esta locación. En sistemas Linux/Unix ubicar las imágenes en los lugares designados (de preferencia /opt/images).

Las imágenes Cisco IOS están comprimidas. Estas imágenes comprimidas funcionan bien con Dynamips, aunque el proceso de arranque es significativamente más lento debido a la descompresión (igual que en los routers reales). Es recomendable descomprimir las mismas de antemano así el emulador no tiene que realizar esa tarea. En sistemas Linux/Inx/Cygwin puede utilizar el utilitario “unzip”:

```
Unzip –p c7200-g6ik8s-mz.124-2.T1.bin > c7200-g6ik8s-mz.124-2.T1.image
```

Recibe un mensaje de advertencia del unzip, pero puede ignorarlo. En Windows se puede descomprimir las imágenes utilizando el WinRAR. Hay que tener en cuenta que las imágenes

actuales de los routers 1700 y 2600 deben ser descomprimidas antes de utilizarlas en Dynamips. Siempre se debe probar las imágenes directamente con Dynamips antes de usarlas con GNS3:

./Dynamips –P <chassis> <path-to –the-ios-image>

4. UTILIZACIÓN DE LOS RECURSOS

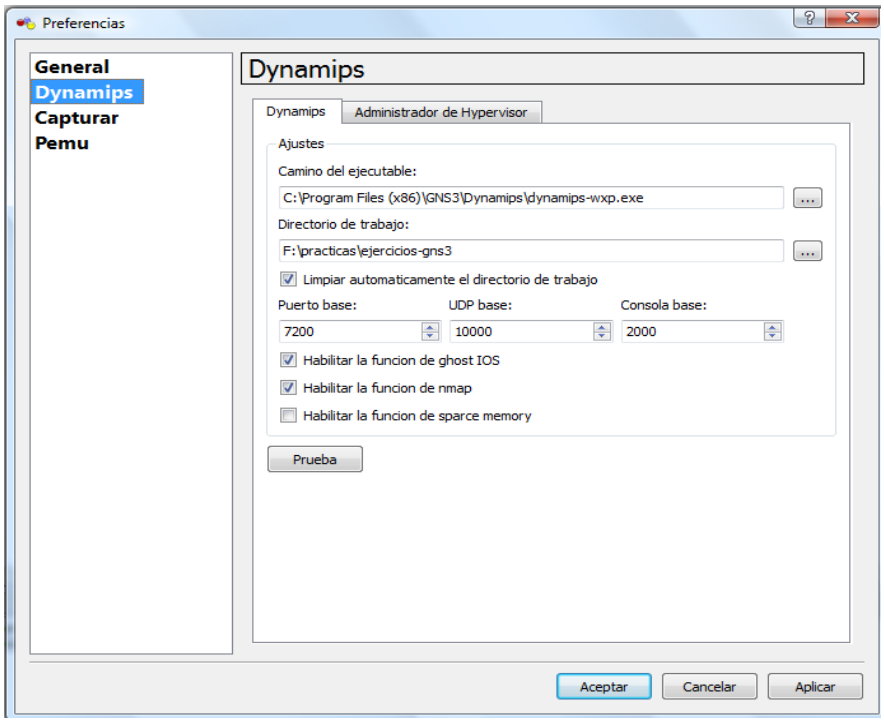
Dynamips hace uso intensivo de memoria RAM y CPU en orden de lograr la magia de la emulación. Si la intención es ejecutar una imagen de IOS que requiere 256 MB de RAM en un router 7200 real, y dedica 256 MB de RAM a la instancia de su router virtual, este utilizará 256 MB de memoria para funcionar. Dynamips también utiliza por defecto 64 MB de RAM por cada instancia en sistemas Unix y 16 MB en Windows para cachear (caché) las transacciones JIT. Este será el tamaño total de trabajo; esto se debe a que Dynamips debe trazar un mapa de la memoria virtual de los routers.

En el Directorio de Trabajo se encuentran los archivos temporales “ram” cuyo tamaño es igual a la memoria RAM de los routers virtuales. El Sistema Operativo cacheará en la RAM las secciones de los archivos nmap que están siendo utilizados. (Ver la sección Optimización del Uso de Memoria) las opciones de configuración, estas pueden reducir en forma significativa la utilización de la memoria.

Dynamips también hace uso intensivo del CPU porque está emulando la CPU de un router instrucción-por-instrucción. En principio no tiene manera de saber cuando el router virtual esta en estado ocioso (idle), por esa razón ejecuta diligentemente todas las instrucciones que constituyen las rutinas de idle del IOS, igualmente que las instrucciones que conforman el “real” funcionamiento. Pero una vez que se haya ejecutado el proceso de “Idle-PC” para una determinada imagen de IOS, la utilización del CPU decrecerá en forma drástica.

5. CONFIGURANDO LAS PREFERENCIAS DE DYNAMIPS

Para utilizar Dynamips en GNS3, se debe configurar el camino para alcanzarlo y el puerto base. Estos valores serán utilizados por el Hypervisor Manager y para cargar los archivos .net. Buscar la opción Preferencias del menú Editar:



Luego hacer click en Prueba y si es satisfactorio este ítem, se ha configurado de la forma correcta.

El Directorio de Trabajo es el lugar en donde Dynamips almacena todos los archivos generados, esto incluye a la NVRAM de los router virtuales, también la bootflash, los logfiles, y otros archivos de trabajo.
Opciones:

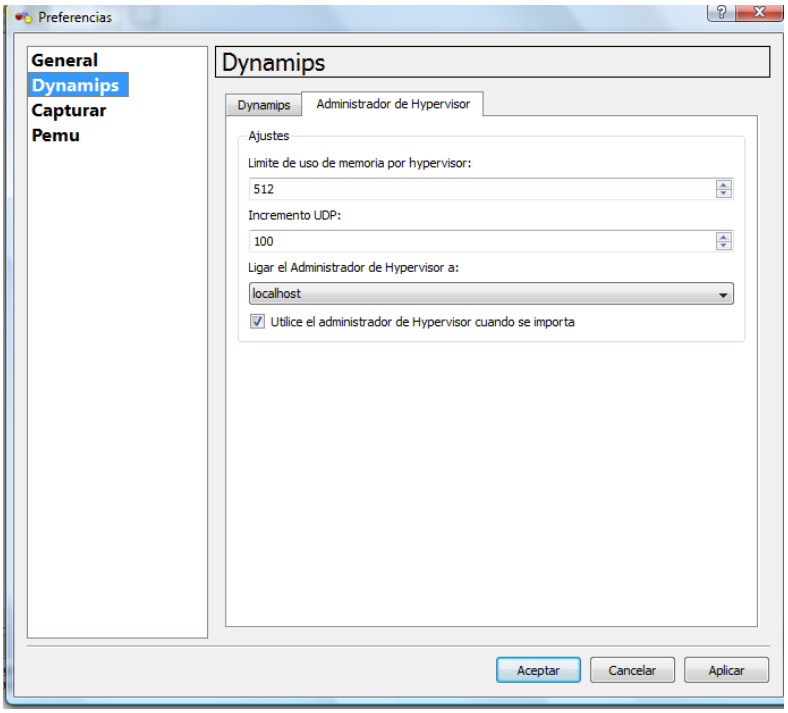
- “Habilitar la función de ghost IOS” es para utilizar la función ghost de Dynamips en forma global (o no).
- “Habilitar la función de nmap” es para utilizar la función nmap de Dynamips en forma global (o no).

- “Habilitar la función de sparce memory” es para utilizar esta función de Dynamips en forma global (o no).

Estas opciones se explican detalladamente en Optimización del uso de la memoria. El administrador Hypervisor es utilizado por GNS3 para ejecutar los hypervisors en forma interna, esto significa que no se necesita iniciarlos en forma manual. Este administrador también ayuda a resolver el problema de direccionar el límite del uso de la memoria por cada proceso cuando varias instancias de IOS se ejecutan en un solo hypervisor, balanceando la carga de las instancias en múltiples hypervisors.

Por ejemplo se desea ejecutar 5 instancias de IOS, y cada instancia utiliza 256 MB, también se ha configurado el límite del uso de la memoria por hypervisor en 512 MB. Cuando se inicia el lab, el hypervisor creará 3 procesos de hypervisor basándose en la siguiente fórmula (el redondeo se realiza hacia el siguiente número entero):

Número de hypervisors = (256 * 5 /512)

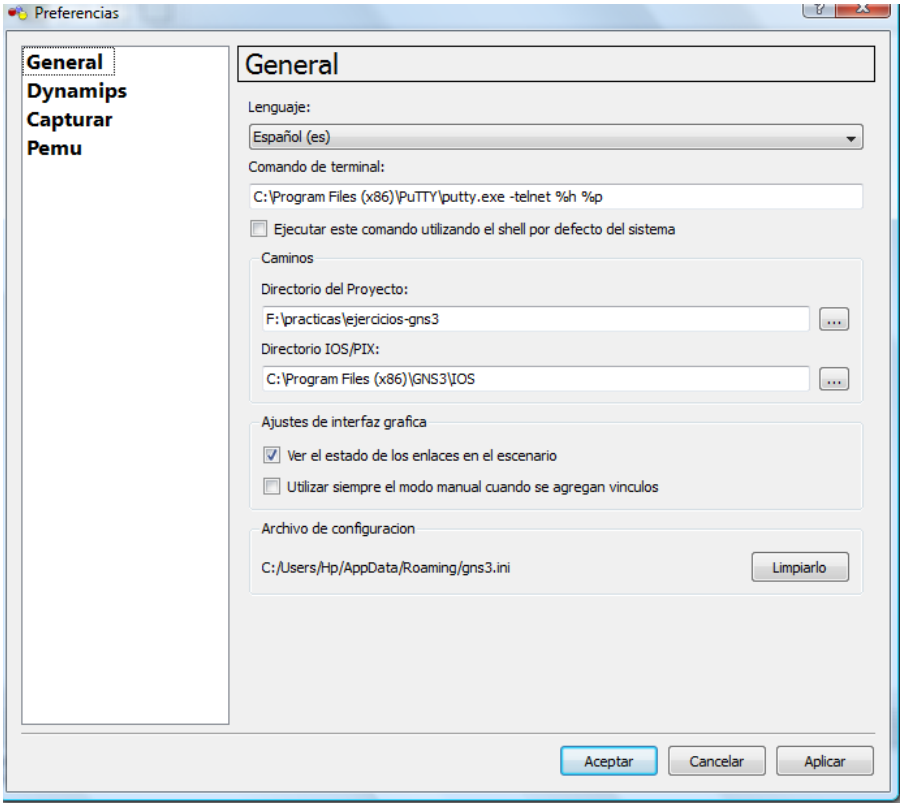


Existen dos ajustes en las Preferencias de Dynamips. “Incremento UDP” que le indica al Administrador de Hypervisor como incrementar el puerto base de Dynamips por cada proceso que el Hypervisor crea (si en las Preferencias de Dymanips el puerto base udp es de 10000 y el incremento de 100, entonces para 3 hypervisors el puerto base para el primero será de 10000, para el segundo 10100 y así sucesivamente).

La opción “Utilizar el Administrador de Hypervisor cuando se importa” se utiliza cuando se carga un archivo de topología (.net) en GNS3. Si esta opción esta marcada se ha definido que los hypervisors se ejecuten en localhost, entonces GNS3 considerara que esos hypervisors deben ser iniciados por el Administrador de Hypervisor. Si no esta marcado, esos hypervisors deben ser iniciados como hypervisors externos y además manualmente.

6. CONFIGURANDO LAS PREFERENCIAS GENERALES

Para poder conectarse a las consolas de los routers virtuales, también es necesario configurar los comandos de Terminal.



GNS3 propone un comando por defecto pero se lo puede modificar. Las siguientes son las sustituciones que se realizan:

%h = host
%p = puerto
%d = nombre de dispositivo

Ejemplos de Comandos de Terminal

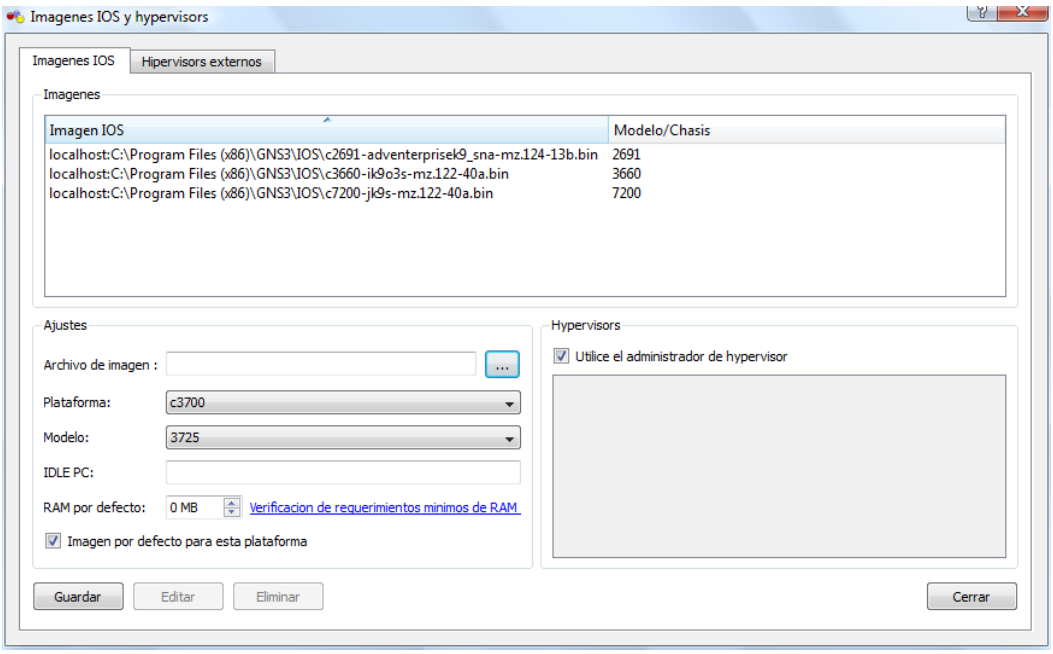
- **En Windows (sin cmd.exe):**
  Usuarios TerraTerm SSH: C:\Archivos de Programa\TTERMPRO\ttssh.exe %h %p /W=%d /T=1

  Usuarios PuTTY : C:\Archivos de Programa\PuTTY\putty.exe –telnet %h %p

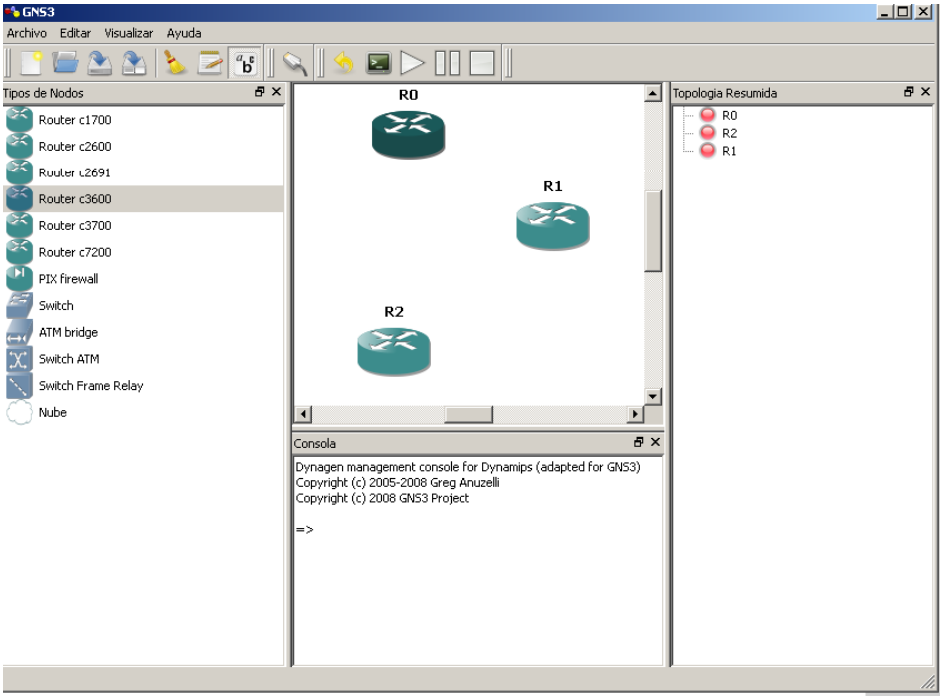
- **En linux**
  Usuarios Gnome: gnome-terminal –t " + name + " –e 'telnet " + host + " " + str(port) + " ' > /dev/null 2> &1 &

7. EJECUTANDO UN LABORATORIO SIMPLE

Primero se debe registrar al menos una imagen de IOS, seleccionando Editar- Imágenes IOS e hipervisors del menú. Luego ajustar el camino al IOS, elegir la plataforma y el modelo (si es necesario) y si se conoce el valor de IDLE PC ingresarlo o caso contrario haciendo click derecho sobre el nodo y escoger el valor Idle PC más adecuado. (Más adelante se explica con más detalle).

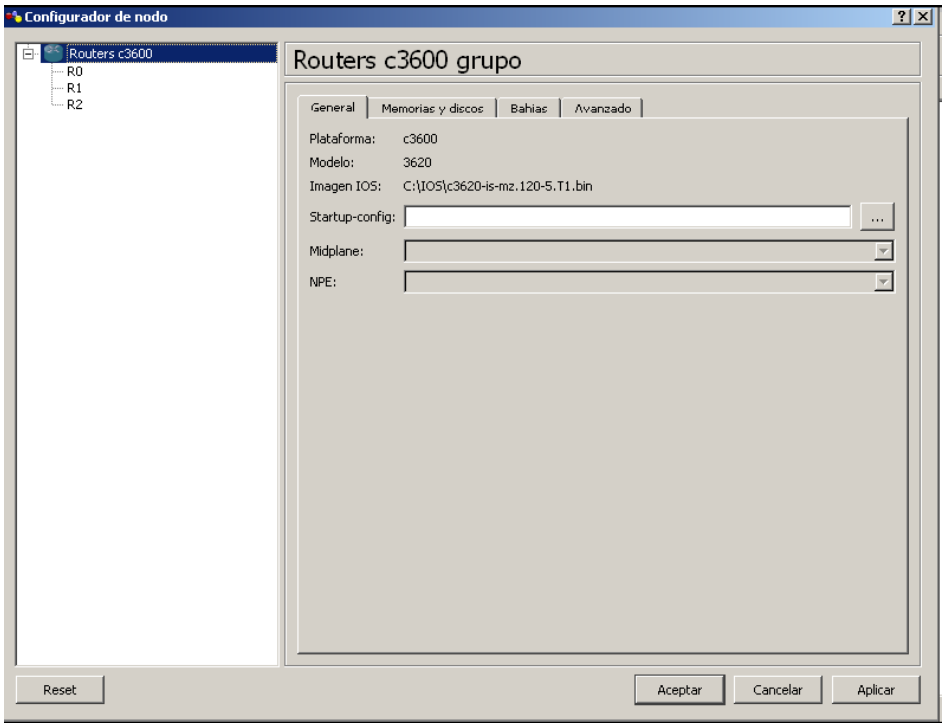


Toda la información referida a los IOS y los hypervisors será guardada en el archivo gns3.ini, por eso solo debe hacerse una vez solamente. Ahora es posible crear la topología de red solamente arrastrando los nodos que se encuentran en la lista situada a la izquierda y depositarlos en el área de trabajo.



Cuando la topología está creada, se procede a configurar cada nodo (sobre el nodo indicado botón derecho del mouse y seleccionar configurar).

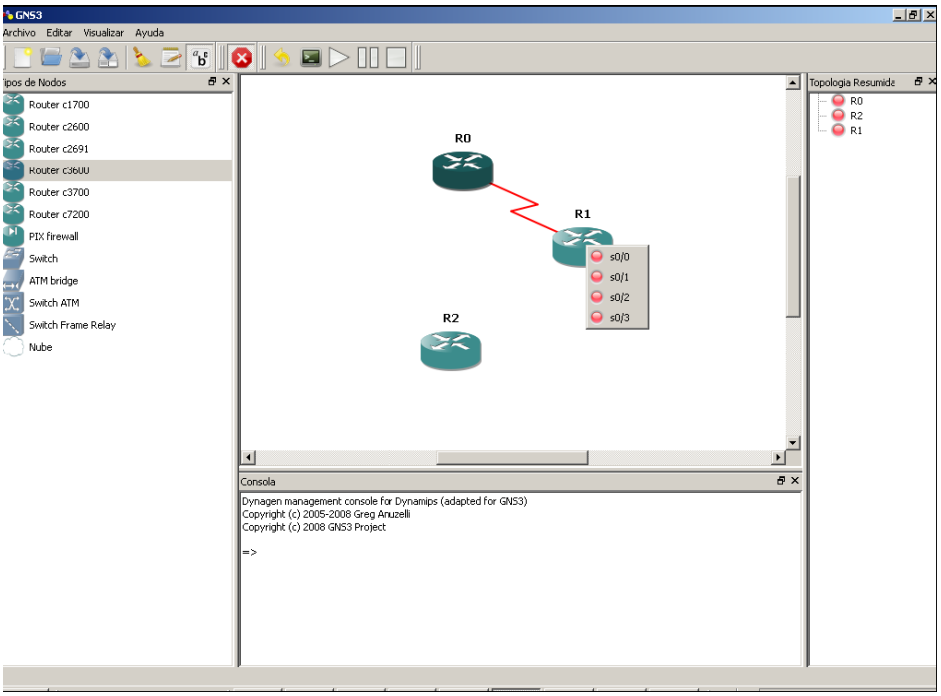
Se puede aplicar la misma configuración a todos los routers seleccionando “Routers” en el árbol expandido del panel izquierdo o seleccionando un router en particular por su nombre.



En el modo de configuración se podrá configurar varios elementos como las bahías, el tamaño de la RAM, etc.

Paso siguiente es adicionar los vínculos de cada nodo (hacer clic en el botón “Agregar un vinculo” en la barra de menú y seleccionar el nodo origen y destino). Se puede elegir el tipo de vínculo (Ethernet, serial, entre otros). GNS3 asigna automáticamente los módulos correctos correspondientes a los tipos de vínculos en las bahías de los routers y elige la primera interfaz disponible para realizar el vínculo.

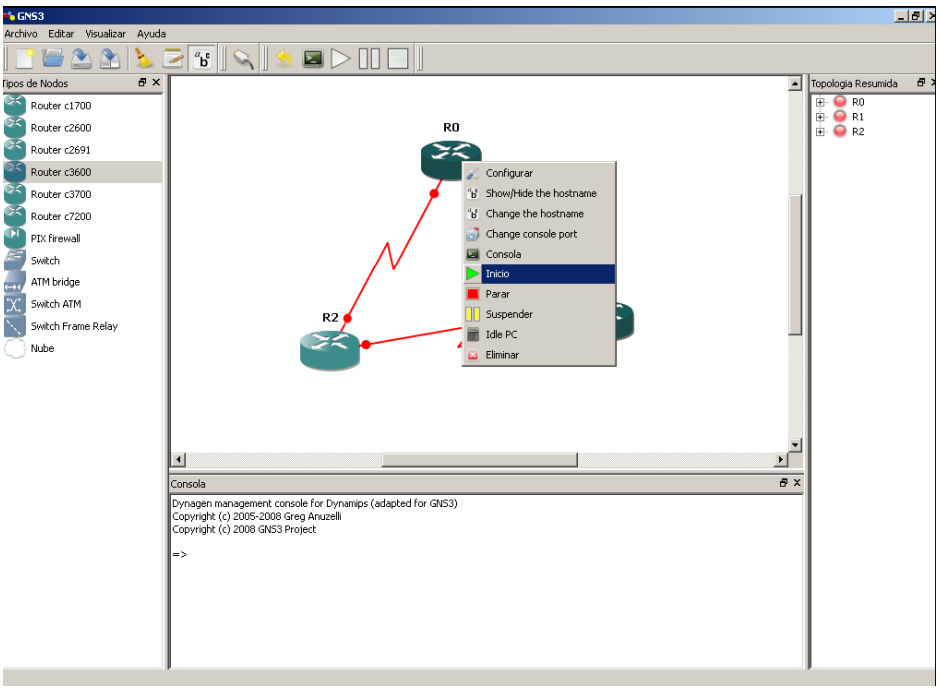
Se puede seleccionar manualmente que interfaz se desea conectar al vínculo, seleccionando el método manual del menú desplegable, pero se tendrá que configurar las bahías de los routers en forma manual también.



Nota: Las interfaces ya utilizadas están señaladas con color verde y las disponibles en rojo.

La topología de red con todos los ajustes realizados se crea en los hypervisors, es posible iniciar/parar/suspender una instancia de IOS oprimiendo el botón derecho de mouse sobre un nodo indicado. Si ha iniciado un IOS, a continuación puede iniciar una sesión de consola en el dispositivo.

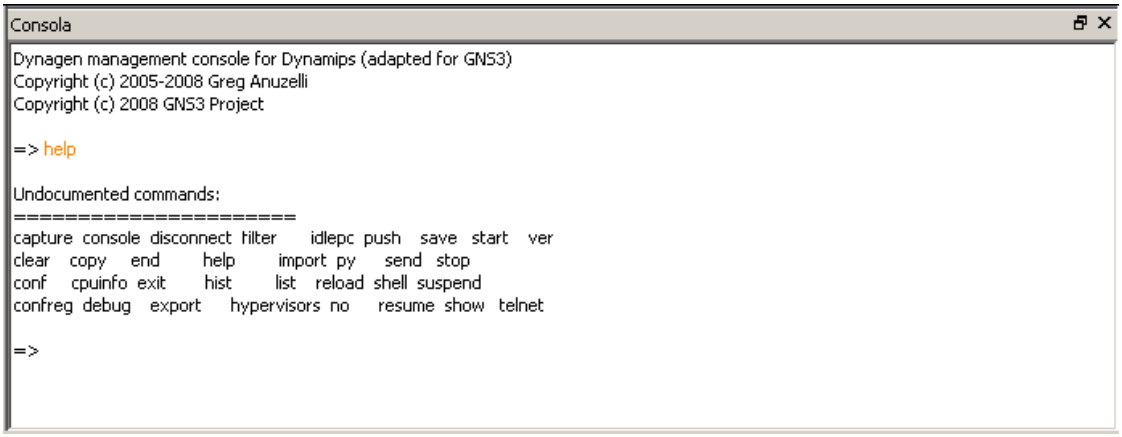
Nota: múltiples nodos pueden ser seleccionados si desea realizar las operaciones simultáneamente.



Una vez que se haya conectado a los routers vía consola, se podrá asignar una dirección IP apropiada a las interfaces seriales (puede visualizar que interfaces están conectadas en el panel derecho "Topología resumida" o desplazando el mouse sobre el vínculo), y realizar el "no shutdown", porque están conectadas.

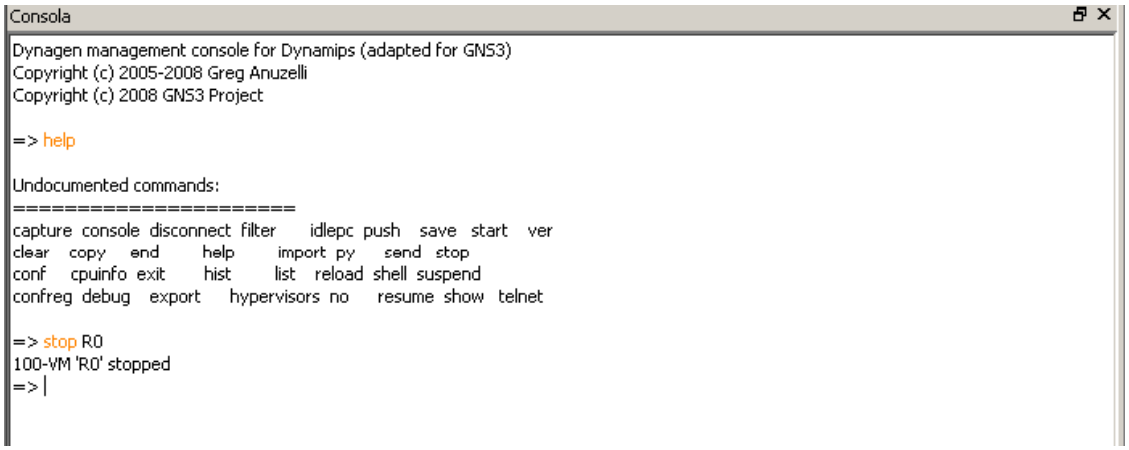
8. TRABAJANDO CON LA CONSOLA DE GNS3

El panel de la Consola estará disponible si se esta a modo emulación, desde aquí se puede utilizar el comando **help** para visualizar los comandos válidos:



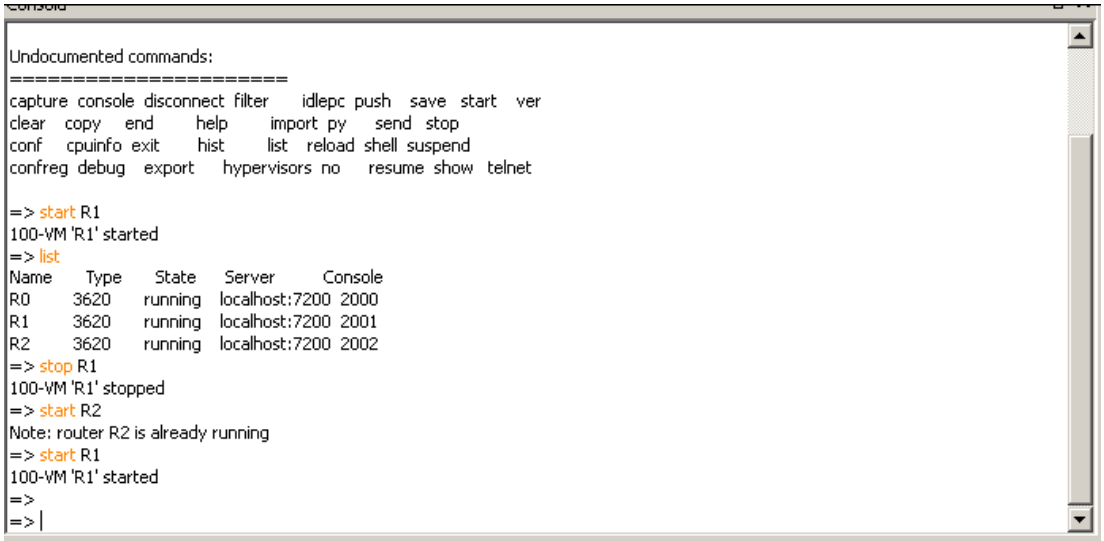
Estos comandos ayudan a operar de manera mucho más rápida las topologías representadas en GNS3. Para obtener una ayuda sobre un comando en particular escribir **help *comando*** o ***comando* ?**

Por ejemplo para detener un router **stop *nombre del router*.**

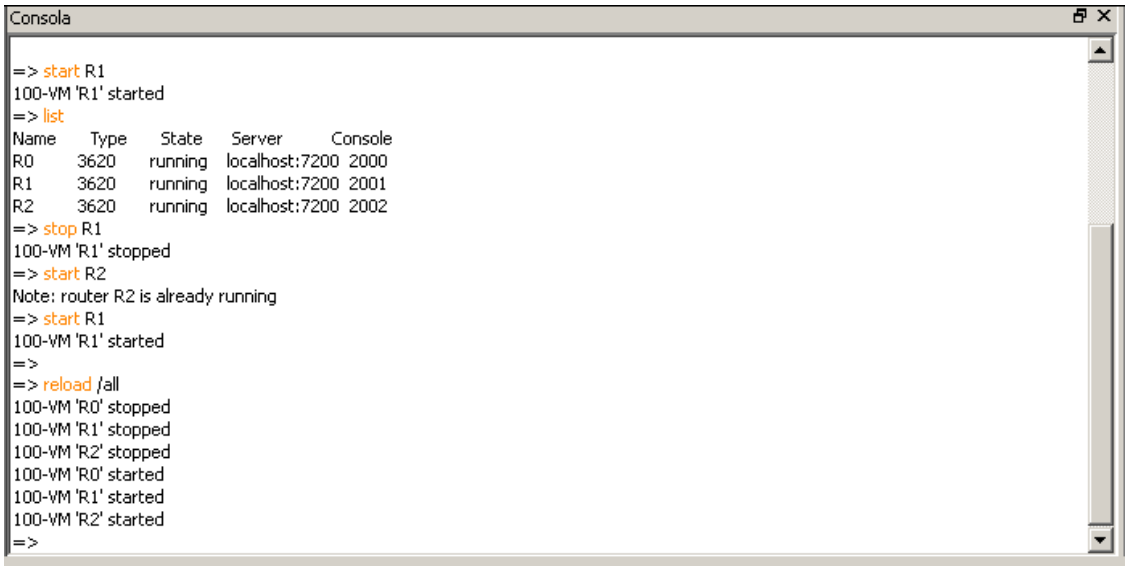


También utilizando stop/all para detener todas las instancias o un grupo de IOS.

Para reiniciar R1 se utiliza el comando start:



El comando de IOS reload no está soportado por Dynamips en los routers virtuales. Pero se puede usar el comando **reload** en la consola, realizando un stop y a continuación un start para reiniciar los routers del laboratorio.

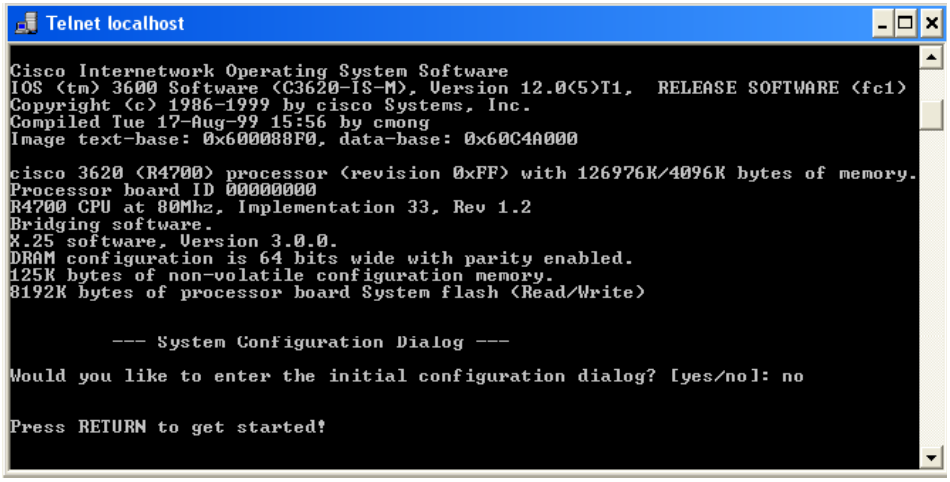


9. CALCULANDO LOS VALORES DE IDLE-PC

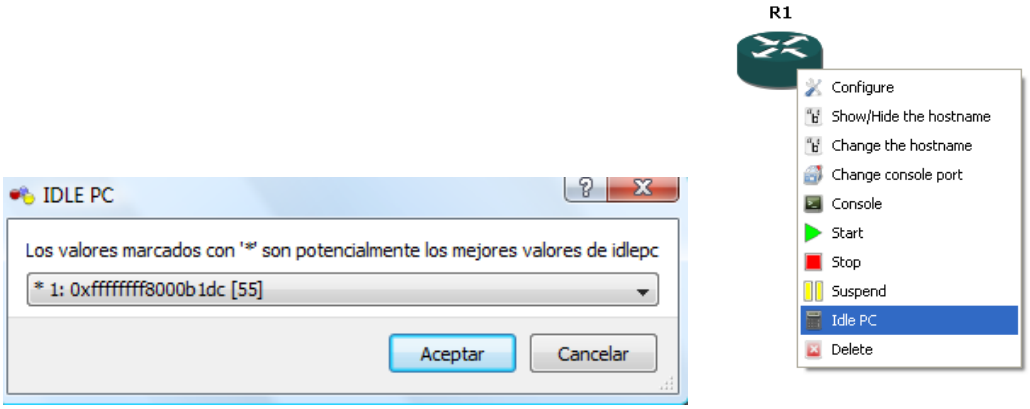
En previas simulaciones el consumo de CPU del sistema alcanza el 100% y permanece allí. Esto se debe a que Dynamips no detecta cuando el router virtual está en estado de Idle o cuando esta operando realmente.

El comando “Idle PC” efectúa un análisis en la imagen que se está ejecutando para determinar cuáles son los posibles puntos en el código que representan un bucle de idle en el IOS. Una vez aplicado, Dynamips “duerme” ocasionalmente al router virtual cuando el bucle idle es ejecutado, reduciendo significativamente el consumo de CPU del host sin reducir la capacidad del router virtual de realizar sus tareas.

Esta es la forma en que se debe realizar el proceso. Primero, crear un router correspondiente a un IOS específico para el cual se desea calcular el valor de Idle PC. Iniciar el router y proceder a una sesión Telnet.



A continuación, volver a GNS3, oprimir el botón derecho del mouse sobre el router y seleccionar "Idle PC", se observará una pantalla en donde se recolecta una estadística, transcurridos unos segundos en donde se lista los valores potenciales de Idle PC:



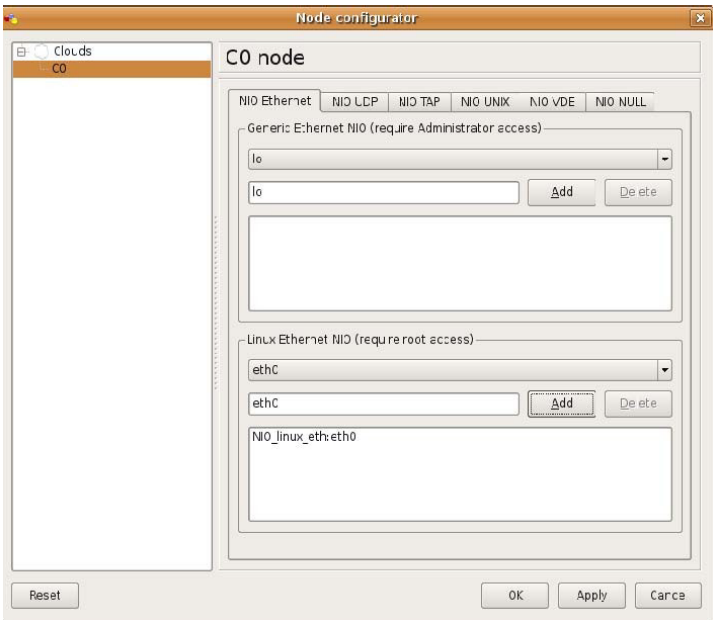
Los valores que proveerán mejores resultados se verán marcados con un asterisco, seleccionar y oprimir el botón Aceptar. En seguida se notará que la utilización de CPU caerá drásticamente, observando el rendimiento en el Administrador de Tareas, si el consumo no se ha reducido volver a buscar un nuevo valor.

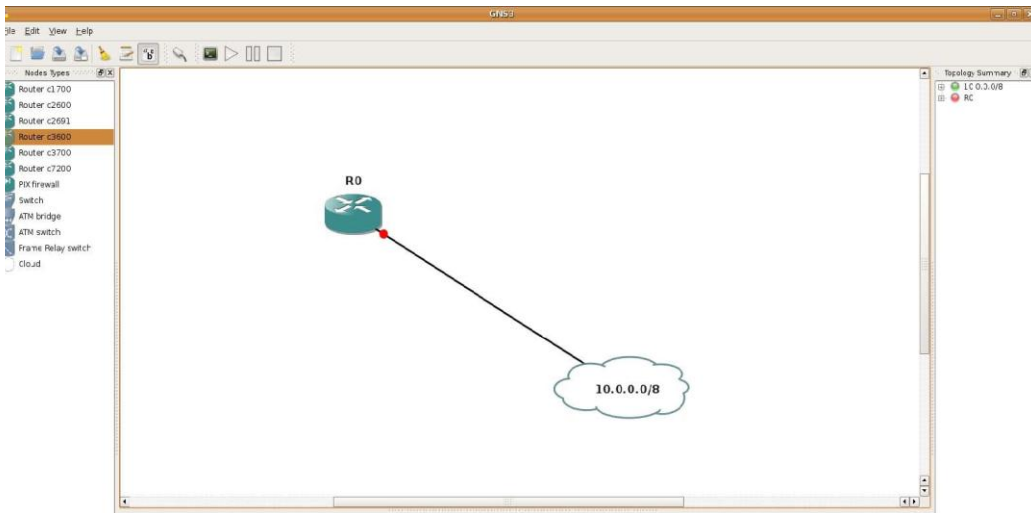
Los valores de Idle-PC son particulares a cada imagen IOS. Varían según la versión de IOS, incluso para IOS de la misma versión pero con diferentes funciones. Por ello los valores de Idle-PC no son particulares para su PC, Sistema Operativo o versión de Dynamips.

10. COMUNICACIÓN CON LAS REDES REALES

Dynamips puede conectar las interfaces de los routers virtuales con interfaces reales de los hosts, posibilitando la comunicación entre la red virtual con el mundo real. En sistemas Linux, esto es realizado por medio del descriptor NIO_linux_eth NIO (Network Input Ouput). Para hacer uso de esta función con GNS3, se debe crear un dispositivo "Nube". Una nube representa las conexiones externas.

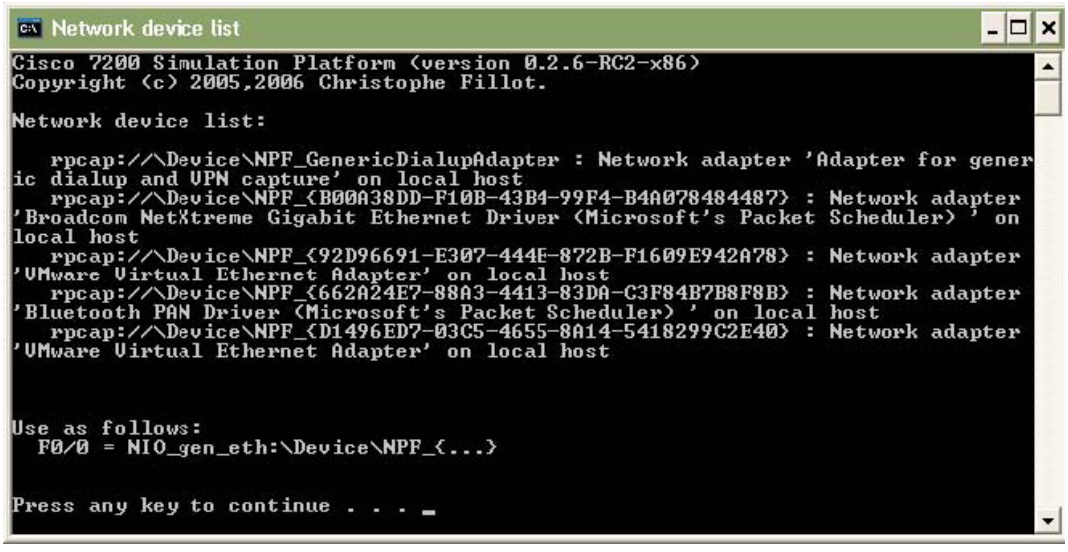
En el siguiente ejemplo se ha conectado la interfaz del router e0/0 a la interfaz eth0 del host. Los paquetes que egresan de e0/0 son volcados en la red real a través de la interfaz eth0 del host, y los paquetes que regresan son encaminados de la misma manera a la instancia del router virtual.





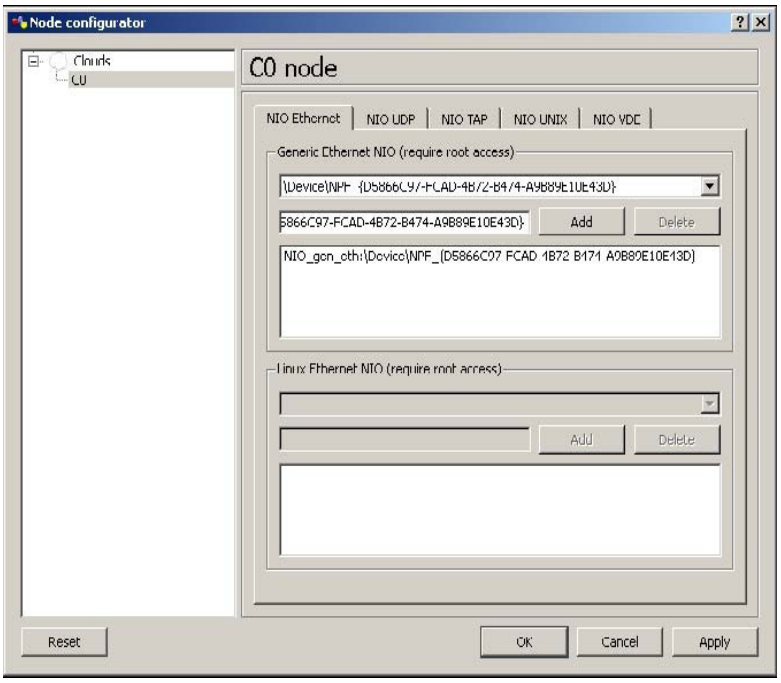
En sistemas Windows, la librería WinPcap es utilizada para realizar esta tarea. El formato de la interfaz es un poco más compleja que en los sistemas Linux. GNS3 procederá a la auto detección con la ayuda de la lista de interfaces disponibles de Dynamips. Si la detección no funciona, se utiliza el acceso directo creado por el instalador GNS3 de Windows (gracias a Dynagen). Luego se abre el acceso directo "Network Device List":

En Windows, se utilizará:



\Device\NPF_{B00A38DD-F10B-43B4-99F4-B4A078484487}

Para conectar al adaptador local Ehternet solo se necesita poner este valor en el cuadro de texto Generic Ethernet NIO, cuando se configura el dispositivo “nube”. Seleccionar el dispositivo del cuadro de opciones, o copiarlo en el cuadro a la izquierda del botón de Agregar desde el acceso directo “Network Device List”. Luego oprimir Agregar para incluir el dispositivo como se muestra en la figura.

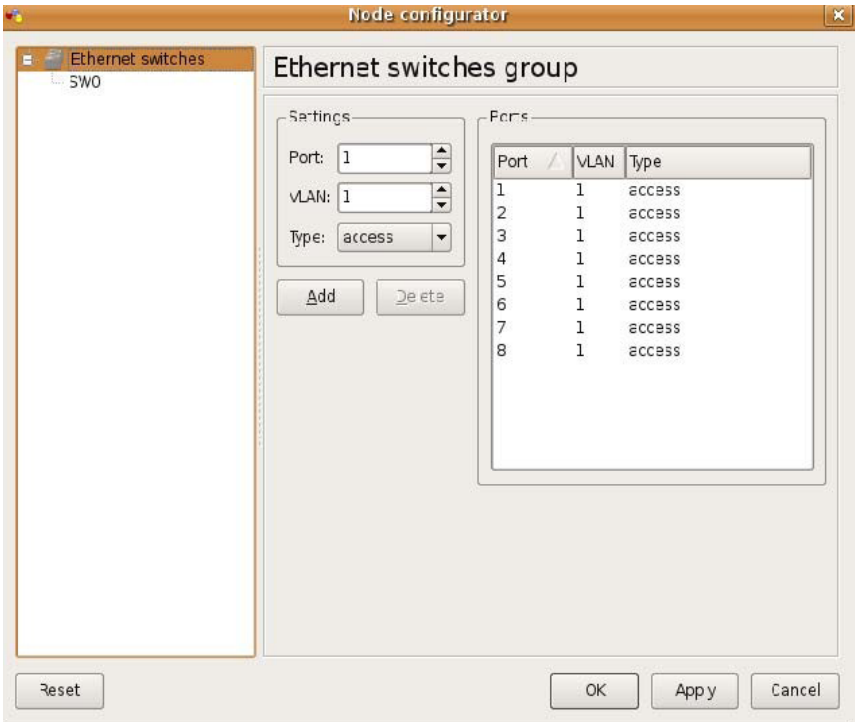


11. UTILIZANDO EL DISPOSITIVO SWITCH ETHERNET

Dynamips también provee un switch virtual Ethernet integrado que soporta VLANs con encapsulación 802.1q. El puerto 1 y 2 del switch son puertos de acceso en VLAN 1. El puerto 4 es un puerto trunk (se especifica con el valor dot1q) con una VLAN native de 1. Los puertos trunk ven el tráfico de todas las VLANs del switch. Por defecto en GNS3, el switch tiene 8 puertos configurados en VLAN 1.

También se puede conectar un puerto del switch al “mundo real”, conectando el switch a un dispositivo “Nube”. Aquí se conecta un puerto trunk (encapsulación dot1q) con VLAN 1 como native al host eth1, en Windows utilizando NIO_gen_eth WinPcap NIO (ver la sección Comunicación con las Redes Reales). Si esta interfaz esta conectada a un switch real

configurado para trunking, puede fácilmente conectar cualquier instancia de router a cualquier VLAN.



Módulos WIC

Dynamips agregó soporte para varios módulos WIC, actualmente son WIC-1T y WIC-2T en las plataformas 1700, 2600, 2691 y 3700 y el modulo WIC-1ENET en 1700. Ver la sección Hardware actualmente emulado para un módulo en particular y que bahías WIC corresponden a cada plataforma.

Nota: En GNS3, cuando un módulo WIC es insertado a un router no puede ser removido.

12. OPTIMIZACIÓN DEL USO DE MEMORIA

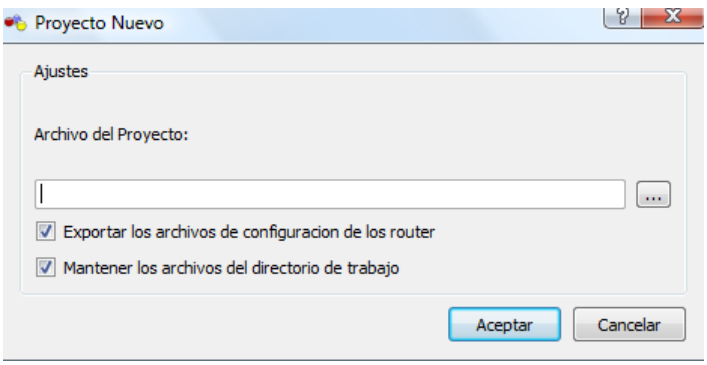
Como se describió anteriormente los laboratorios pueden consumir gran cantidad de memoria real y virtual. Las opciones de “ghost IOS” y “sparce memory” fueron añadidas para mejorar el funcionamiento respectivamente.

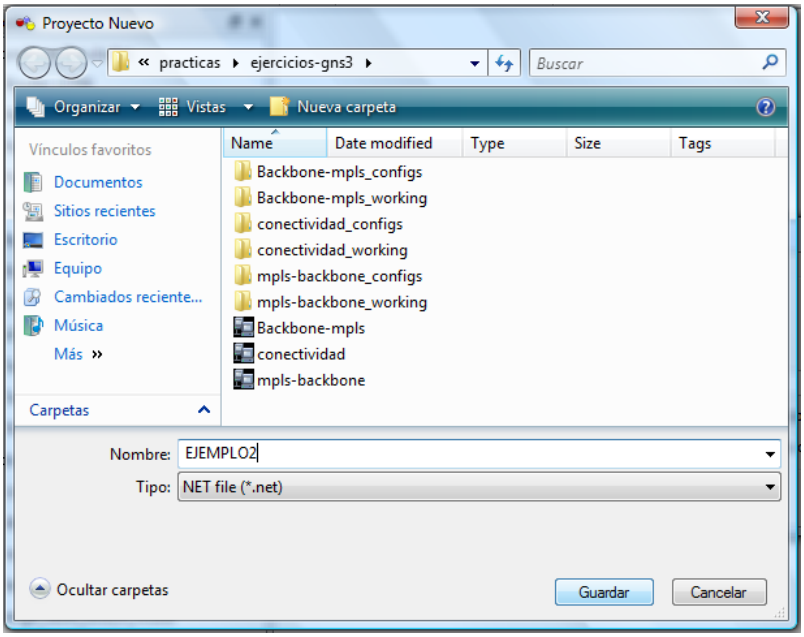
La opción de Ghost IOS puede reducir significativamente el uso de memoria real necesaria para los labs que corren con la misma imagen de IOS. Con esta función, en vez de que se almacene una copia idéntica del IOS en la RAM virtual, el host utilizará una región compartida de memoria para todos. Por ejemplo, si se desea ejecutar 10 routers con la misma imagen de IOS y la misma es de un tamaño de 60 MB, utilizará 9*60 = 540 MB de memoria real RAM para ejecutar el lab. Habilitando fácil y simplemente el ghost IOS en las Preferencias de Dynamips. Esta opción esta habilitada por defecto y aplicada a todas las instancias de routers en los laboratorios.

La función de "sparce memory" no conserva memoria real pero si reduce la cantidad de memoria virtual utilizada por los IOS. Esto es importante porque los Sistemas Operativos limitan el uso de memoria virtual a 2 GB en Windows-32 bits, y 3 GB en Linux-32 bits. Por ejemplo, en Windows, después del espacio VM que es utilizado por cygwin y otras librerías Dynamips, deja espacio para 4 instancias de routers a 256 MB cada uno. Habilitando sparce memory solo reserva memoria virtual en el host donde actualmente es utilizado por el IOS en esa instancia de router, en vez de toda la memoria RAM configurada. Esto posibilita más instancias por Dynamips antes de tener que ejecutar múltiples procesos.

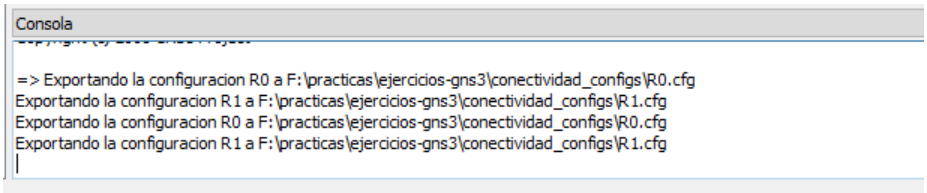
13. GUARDAR Y CARGAR UNA TOPOLOGÍA

GNS3 puede guardar y cargar las topologías en el formato de configuración (extensión .net). Una vez que se han configurado los routers se procede a guardar el proyecto, en Archivo-Nuevo Proyecto y buscar la dirección del Directorio de Proyecto configurada en Preferencias-General.

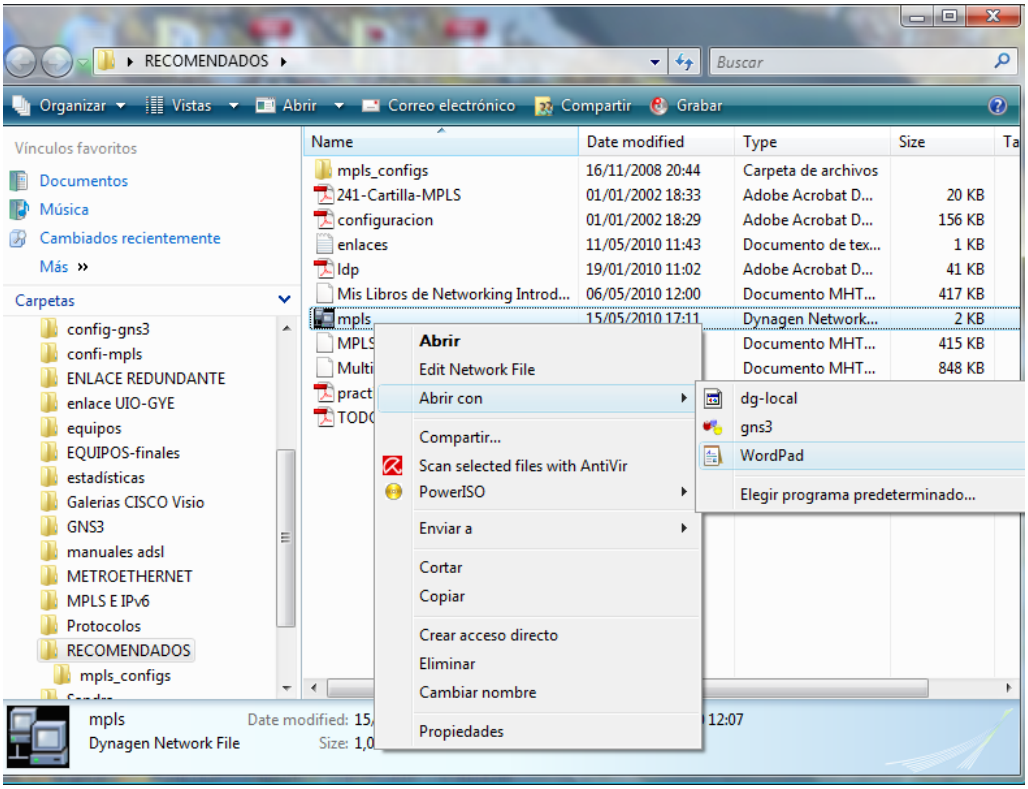




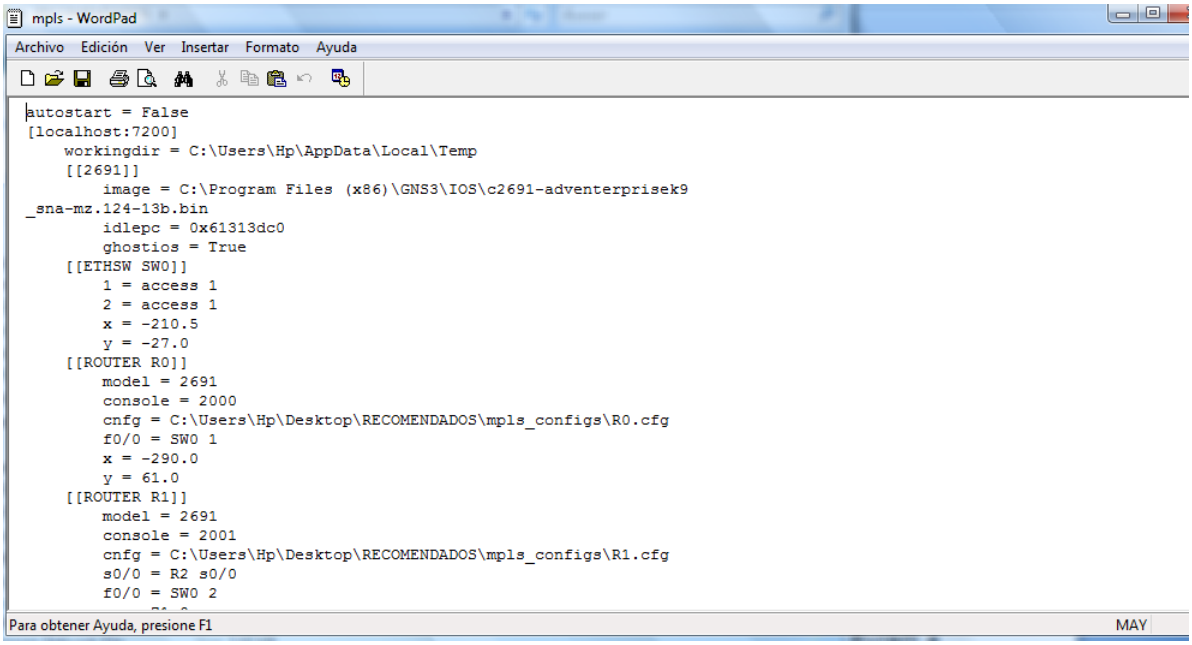
Al aceptar y cuando se guarde un lab en la consola de GNS3 se observará que las configuraciones de los equipos se exportarán a la carpeta direccionada en el Directorio de Trabajo, configurada en Preferencias-Dynamips.



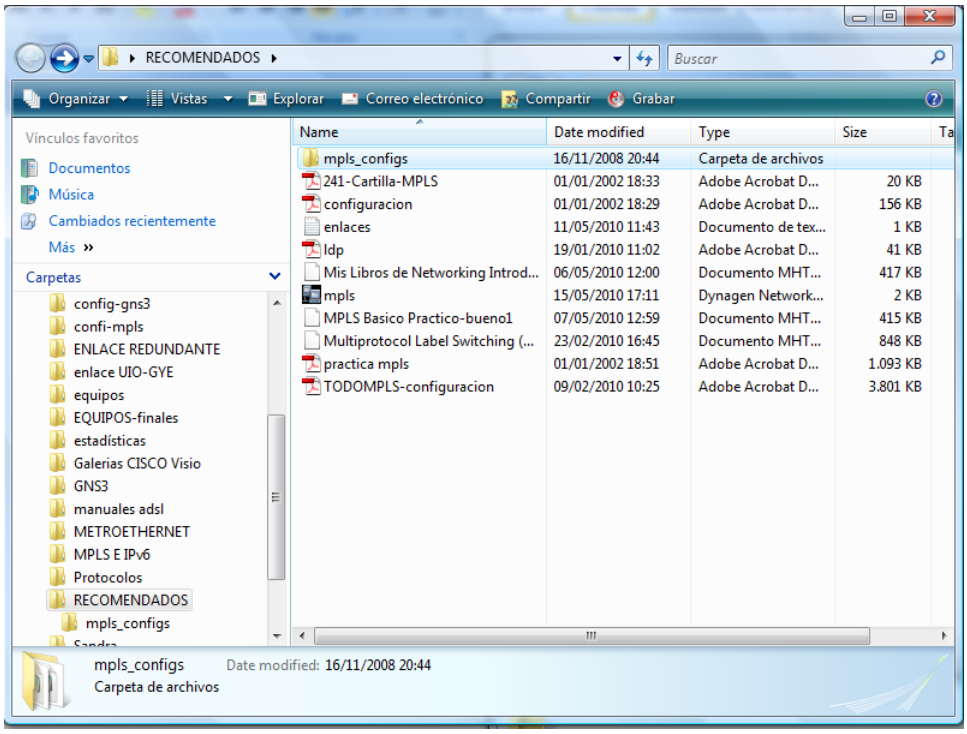
Cuando se vuelve a abrir el laboratorio, se puede buscar directamente el lab en la carpeta del proyecto o simplemente desde Archivo- Abrir de GNS3.

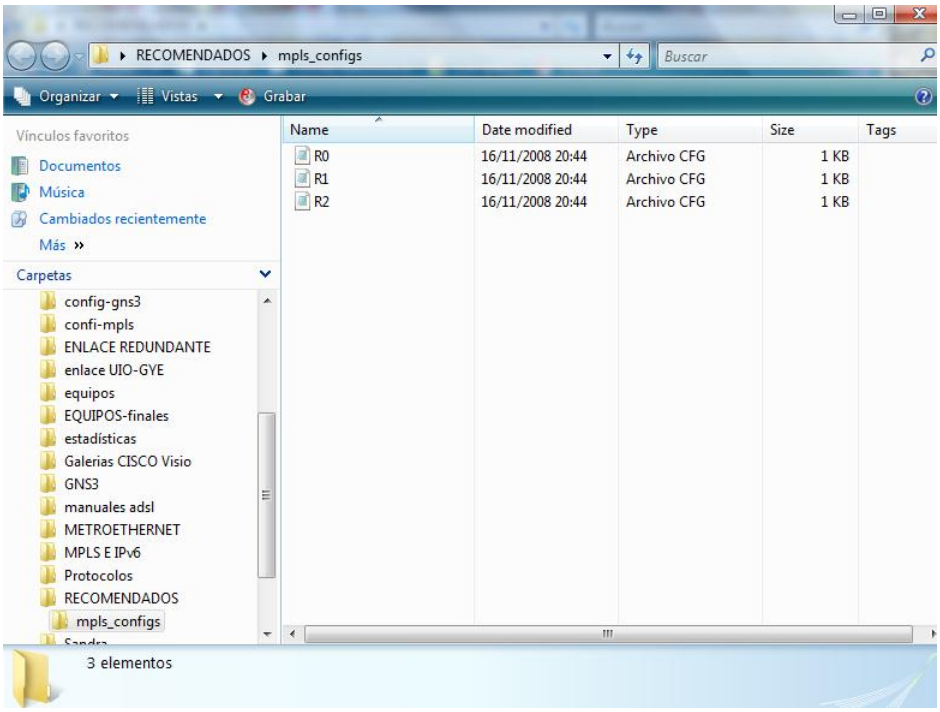


En WordPad se observa el resultado del archivo .net, es decir las configuraciones y parámetros para cada IOS:

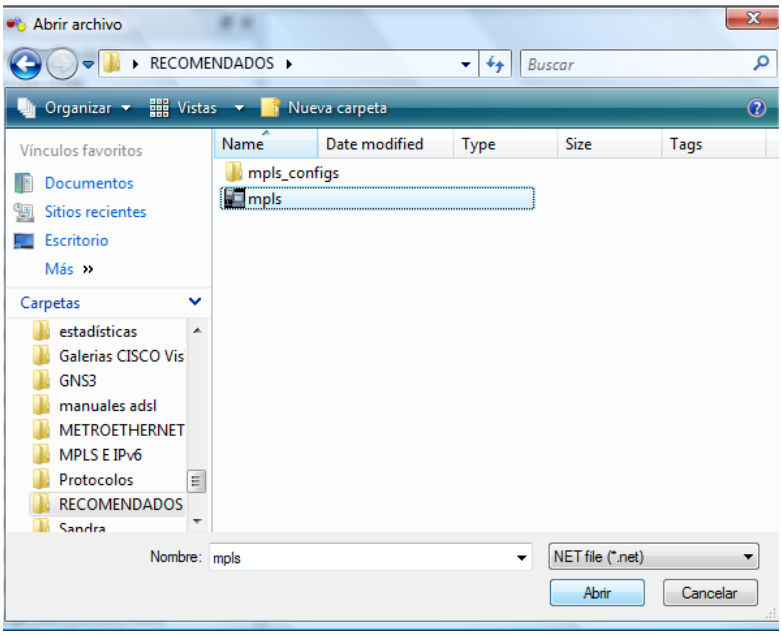


Mientras que en la carpeta configs están almacenadas las configuraciones de cada uno de los routers:





Cuando se desee abrir y cargar una topología simplemente hay que abrirla desde Archivo-Abrir y seleccionar el ejemplo.



14. HARDWARE ACTUALMENTE EMULADO

1710, 1720, 1721, 1750, 1751

Slots: 0 (disponible)

WIC slots: 0

CISCO1710-MB-1FE-1E (1 puerto FastEthernet y 1 Ethernet, uso automático)

1760

Slots: 0 (disponible)

WIC slots: 2

C1700-MB-1ETH (1 puerto FastEthernet, uso automático)

Tarjetas: WIC-1T (1 Serial port), WIC-2T (2 Serial ports), WIC-1ENET (1 Ethernet ports)

2610

Slots: 1 (disponible)

WIC slots: 2

CISCO 2600-MB-1E (1 puerto Ethernet, uso automático)

2611

Slots: 1 (disponible)

WIC slots: 2

CISCO2600-MB-2E (2 puertos Ethernet, uso automático)

2620

Slots: 1 (disponible)

WIC slots: 2

CISCO2600-MB-1FE (1 puerto FastEthernet, uso automático)

2621

Slots: 1 (disponible)

WIC slots: 2

CISCO2600-MB-2FE (2 puertos FastEthernet, uso automático)

2610XM

Slots: 1 (disponible)

WIC slots: 2

CISCO2600-MB-1FE (1 puerto FastEthernet, uso automático)

2611XM

Slots: 1 (disponible)

WIC slots: 2

CISCO2600-MB-2FE (2 puertos FastEthernet, uso automático)

2620XM

Slots: 1 (disponible)

WIC slots: 2

CISCO2600-MB-1FE (1 puerto FastEthernet, uso automático)

2621XM

Slots: 1 (disponible)

WIC slots: 2

CISCO2600-MB-2FE (2 puertos FastEthernet, uso automático)

2650XM

Slots: 1 (disponible)

WIC slots: 2

CISCO2600-MB-1FE (1 puerto FastEthernet, uso automático)

2651XM

Slots: 1 (disponible)

WIC slots: 2

CISCO2600-MB-2FE (2 puertos FastEthernet, uso automático)

Tarjetas: NM-1E (Ethernet, 1 puerto), NM-4E (Ethernet, 4 puertos), NM-1FE-TX (FastEthernet, 1 puerto), NM-16ESW (Ethernet switch module, 16 puertos), NM-NAM, NM-IDS, WIC-1T (1 puerto serial), WIC-2T (2 puertos seriales)

3660: Slots: 6 (disponibles)

3640: Slots: 4 (disponibles)

3620: Slots: 2 (disponibles)

Tarjetas: NM-1E (Ethernet, 1 puerto), NM-4E (Ethernet, 4 puertos), NM-1FE-TX (FastEthernet, 1 puerto), NM-16ESW (Ethernet switch module, 16 puertos), NM-4T (Serial, 4 puertos), Leopard-2FE (Cisco 3660 FastEthernet un slot 0, uso automático)

2691 (Es prácticamente un 3700 con un slot),

Slots: 1 (disponible)

WIC slots: 3

3725

Slots: 2 (disponibles)

WIC slots: 3

3745

Slots: 4 (disponibles)

WIC slots: 3

Tarjetas: NM-1FE-TX (FastEthernet, 1 puerto), NM-4T (4 puertos seriales), NM-16ESW (Ethernet switch module, 16 puertos), GT96100-FE (2 puertos integrados, uso automático), NM-NAM, NM-IDS, WIC-1T (1 puerto serial), WIC-2T (2 puertos seriales).

7206

Slots: 6 (disponibles)

Tipos de chasis: STD, VXR

NPEs: NPE-100, NPE-150, NPE-175, NPE-200, NPE-225, NPE-300, NPE-400, NPE-G2 (Requiere de NPE-G2 IOS imagen)

Tarjetas: C7200-IO-FE (FastEthernet, slot 0, únicamente), C7200-IO-2FE (FastEthernet, 2 puertos, slot 0 únicamente), C7200-IO-GE (GigabitEthernet, slot 0 únicamente), PA-FE-TX (FastEthernet), PA-2FE-TX (FastEthernet, 2 puertos), PA-4E (Ethernet, 4 puertos), PA-8E (Ethernet, 8 puertos), PA-4T (Serial, 4 puertos), PA-8T (Serial, 8 puertos), PA-A1 (ATM), PA-POS-OC3 (POS), PA-GE (GigabitEthernet).

PIX firewall: 5 interfaces Ethernet.