ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO Y CONFIGURACIÓN DE CALIDAD DE SERVICIO EN LA TECNOLOGÍA MPLS PARA UN PROVEEDOR DE SERVICIOS DE INTERNET

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

LUISANA BERTILDA NIETO PORRAS
luisanita2001@hotmail.com

DIRECTOR: ING. PABLO WILLIAM HIDALGO LASCANO
phidalgo@ieee.org

Quito, Mayo 2010

DECLARACIÓN

Yo, Luisana Bertilda Nieto Porras, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

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

Luisana Bertilda Nieto Porras

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Luisana Bertilda Nieto Porras bajo mi supervisión.

Ing. Pablo William Hidalgo Lascano
Director del Proyecto

AGRADECIMIENTOS

Mi particular agradecimiento al personal de la empresa Telconet S.A., en especial a quienes hicieron posible la realización de este proyecto, Ing. Hugo Proaño e Ing. Julia Marchán, por su guía y disponibilidad para alcanzar cada una de las metas planteadas durante este proceso.

Mi eterno agradecimiento al Ing. Pablo Hidalgo por sus enseñanzas, consejos e infinita paciencia en la conclusión de una etapa de mi vida.

A mis hermanos y sus esposas, que con sus consejos me enseñaron a sobreponerme de las adversidades que se presentan en la vida.

DEDICATORIA

A mi papá, que a pesar de la distancia siempre lo he sentido cerca en cada momento y en cada lugar como un susurro del viento, y que hoy puedo decirle con satisfacción que el deber ha sido cumplido.

A mi mamá, que con su ejemplo y ganas de superación me enseñó a buscar el camino adecuado para alcanzar cada propósito en mi vida.

A mis sobrinos, que con fe, esfuerzo y dedicación pueden alcanzar todos los sueños que se propongan por más simples o complejos que sean.

A mis queridos amigos Daniel, Diana, Leonardo, Briegit, Cristian, Sebastián, Carlos Daniel, Jonathan, Soraya y María Beatriz, que con su compañía supieron ser soporte en cada momento de aprendizaje, alegría, tristeza, diversión y desvelos, manteniendo en mi la fuerza necesaria para recorrer este camino que ahora llega a su conclusión.

CONTENIDO

CAPÍTULO 1

CONCEPTOS Y FUNDAMENTOS DE MPLS Y CALIDAD DE SERVICIO (QoS)

CAPÍTULO 3

DISEÑO DE UN ESQUEMA DE CALIDAD DE SERVICIO (QoS) EN LA TECNOLOGÍA MPLS

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

RESUMEN

El presente proyecto de titulación tiene como objetivo principal realizar el diseño y la configuración de un esquema de Calidad de Servicio (QoS) para un Proveedor de Servicios de Internet (ISP), la empresa Telconet S.A., que maneja tecnología IP y MPLS en su red de datos, con el propósito de cumplir con los parámetros comprometidos con los clientes en los servicios de transmisión de datos e Internet.

En el primer capítulo se describe la base teórica para el desarrollo del presente proyecto. Se analizan las características, funcionamiento, enrutamiento y aplicaciones de la tecnología MPLS, así como de los protocolos, servicios y aplicaciones del modelo TCP/IP; adicionalmente se estudian los conceptos, parámetros, procedimientos y arquitecturas para brindar Calidad de Servicio (QoS) al tráfico de Internet.

El segundo capítulo aborda los conceptos, tipos de servicios, formas de acceso, tipos de clientes y Acuerdos de Nivel de Servicio (SLAs) que conciernen a un Proveedor de Servicios de Internet (ISP). Se realiza un análisis de los diferentes agregados de tráfico que circulan por la red de Telconet S.A. y los requerimientos de QoS para su transmisión.

En el tercer capítulo, a partir del análisis y los requerimientos de los agregados de tráfico, se procede a realizar el diseño del esquema de Calidad de Servicio (QoS) sobre el núcleo de la red IP/MPLS de la empresa Telconet S.A.

El diseño incluye los procesos de clasificación de tráfico de acuerdo a los SLAs y a la administración de la red, la definición de los servicios que recibirán las diferentes aplicaciones, los puntos desde donde se brindará la Calidad de Servicio (QoS), los valores específicos con los que se marcará el tráfico, los acondicionadores de tráfico que se utilizarán para cumplir con los parámetros establecidos y los mecanismos de control y evasión de congestión que se emplearán para el correcto funcionamiento del ISP.

En el cuarto capítulo se describe y analiza paso a paso los comandos de configuración para el desarrollo del esquema de Calidad de Servicio (QoS) propuesto. Además, se indica la topología de la red utilizada para la configuración, los modelos de los equipos Cisco configurados, la versión de IOS que deben tener para el soporte de Calidad de Servicio (QoS) y los parámetros utilizados en los comandos de configuración.

El quinto capítulo expone las conclusiones y recomendaciones obtenidas durante el desarrollo del presente proyecto.

Finalmente, el mencionado proyecto concluye con los anexos, donde se encuentra información del análisis y el cálculo del tráfico de las aplicaciones.

PRESENTACIÓN

El rápido crecimiento del mercado de las comunicaciones y la gran demanda de nuevos servicios con mayores requerimientos, exige que los Proveedores de Servicios de Internet (ISPs) busquen nuevas tecnologías, capaces de cumplir con los requerimientos solicitados por los usuarios de sus servicios y que respondan de forma eficiente ante periodos de congestión.

La tecnología *MultiProtocol Layer Switching* (MPLS) surge como un estándar de gran escalabilidad, bajo coste y alto rendimiento, gracias a su simplicidad, rapidez y capacidades significativas ante el servicio de "mejor esfuerzo", entregado tradicionalmente por las redes IP. Estas ventajas han hecho que esta tecnología sea ampliamente aceptada por las grandes corporaciones de telecomunicaciones de nuestro país, como es el caso de la empresa Telconet S.A.

La Calidad de Servicio (QoS) es un área donde la tecnología MPLS permite satisfacer requisitos de congestión, retardo de paquetes y variación en la entrega de tráfico, lo que faculta que empresas como Telconet S.A. puedan escalar en sus ofrecimientos actuales y diversificar sus servicios, permitiéndoles alcanzar un alto grado de satisfacción con los clientes y superar sus expectativas.

La definición de un esquema de optimización que brinde QoS sobre la tecnología MPLS, establece los criterios para asegurar las prestaciones ofrecidas a los clientes, obteniendo una infraestructura confiable y flexible para la implementación de nuevos servicios. Además, permite plantear soluciones escalables y mejorar los niveles de calidad, a través de arquitecturas de QoS como Servicios Diferenciados (DiffServ).

Por los motivos expuestos anteriormente, se pone a consideración el presente proyecto como una solución alternativa para empresas proveedoras de servicios de Internet dentro de sus planes de expansión y desarrollo, con el fin de entregar servicios de calidad y contribuir al desarrollo de nuestro país.

CAPÍTULO 1

CONCEPTOS Y FUNDAMENTOS DE MPLS Y CALIDAD DE SERVICIO (QoS)

1.1 TECNOLOGÍA *MULTIPROTOCOL LABEL SWITCHING* (MPLS)

1.1.1 INTRODUCCIÓN

El crecimiento de la red Internet y la demanda de nuevos servicios exigen el uso de redes convergentes que combinen el tráfico multimedia con el tráfico de datos, requisito que requiere cambios en las tecnologías desarrolladas a mediados de los años 90 como la del *Internet Protocol* (IP).

IP fue desarrollado para brindar un servicio de "mejor esfuerzo", que no permite ofrecer diferentes niveles de servicio para los distintos tipos de aplicaciones; esto ha determinado que los Proveedores de Servicios de Internet (ISPs) ofrezcan tradicionalmente el mismo nivel de servicio a todos los usuarios.

Sin embargo, en los últimos años los ISPs han visto la necesidad de escalar en sus servicios, ofreciendo nuevos servicios y administrando las redes para un óptimo rendimiento, por lo que han surgido tecnologías que realizan cambios tecnológicos fundamentales para suplir estas necesidades, como es el caso de *MultiProtocol Label Switching* (MPLS).

MPLS es un estándar creado por el Grupo de Trabajo de MPLS establecido en el *Internet Engineering Task Force* (IETF) en 1997, cuyo objetivo era obtener un estándar que pudiera trabajar sobre diferentes infraestructuras y que sea interoperativo entre productos de distintos fabricantes. El resultado del Grupo de Trabajo fue la definición en 1998 del estándar conocido como MPLS, establecido en la *Request for Comments* (RFC) 3031[7].

Esta tecnología combina la simplicidad y rapidez de la conmutación de capa 2 y las funciones de control del enrutamiento de Capa 3 en una sola entidad, ofreciendo capacidades significativas en las áreas de Redes Privadas Virtuales (VPNs), Ingeniería de Tráfico y Calidad de Servicio (QoS), entre otras.

1.1.2 DEFINICIÓN DE MPLS[12][15]

MPLS es una arquitectura de transporte de datos estándar que opera entre la capa Enlace y la capa Red del modelo *Open System Interconnection* (OSI), ofreciendo niveles de rendimiento diferenciados y priorización de tráfico. Esta arquitectura se basa en la traducción de las direcciones IP en etiquetas simples de longitud fija, logrando una eficiente conmutación al reducir la cantidad de procesamiento por cada paquete.

MPLS funciona sobre cualquier tecnología de transporte de datos de capa Enlace, por lo que soporta múltiples protocolos tales como: *Asynchronous Transfer Mode* (ATM), *Frame Relay*, *Ethernet*, entre otros. En la figura 1.1 se indica el soporte a MPLS por parte de varias tecnologías.

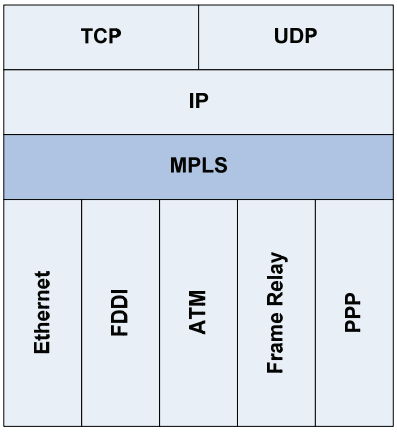

Figura 1.1 Tecnologías que soportan a MPLS

1.1.3 COMPONENTES DE MPLS[3][4][5]

La arquitectura MPLS está formada por varios componentes que permiten su funcionamiento, como se indica en la figura 1.2.

1.1.3.1 Dominio MPLS

Un dominio MPLS es un conjunto contiguo de nodos que soportan capacidades de conmutación de etiquetas y pertenecen a un mismo dominio de encaminamiento IP o están bajo una misma administración.

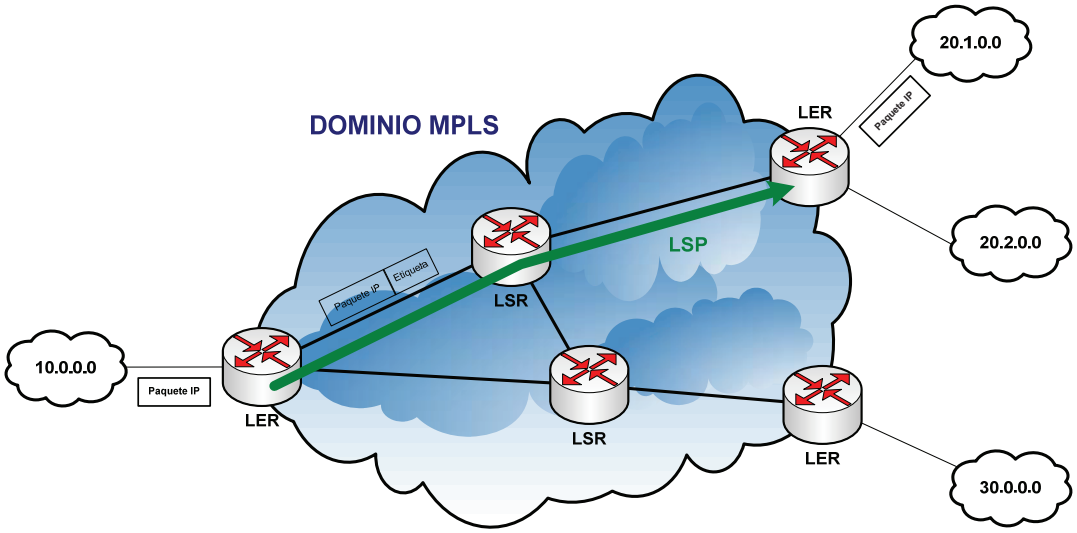

Figura 1.2 Componentes de MPLS

1.1.3.2 *Label Edge Router* (LER)

Los LERs son equipos que se encuentran ubicados en la periferia o frontera de la red MPLS; es decir, son el elemento de entrada/salida de la red. El equipo de entrada se lo conoce como *router* de Ingreso y el de salida como *router* de Egreso.

Estos equipos son el punto de interconexión entre la red MPLS y otras redes de acceso como *Ethernet*, *Frame Relay*, ATM, etc. Entre sus funciones está asignar las etiquetas a la entrada de la red MPLS, enviar el tráfico etiquetado, retirar las etiquetas a la salida y distribuir el tráfico saliente entre las distintas redes.

1.1.3.3 *Label Switched Router* (LSR)

Los LSRs son equipos de gran velocidad ubicados en el núcleo de la red MPLS, que conmutan los paquetes en función de la etiqueta, aunque en algunas implementaciones se puede conmutar en función de la cabecera del paquete IP.

Las funciones que realizan son participar en el establecimiento de los circuitos extremo a extremo de la red, intercambiar las etiquetas de los paquetes que reciben por otras y enviar el paquete al siguiente salto LSR; estos equipos utilizan un protocolo de distribución de etiquetas para establecer los circuitos, que no necesariamente debe ser el mismo en todos los LSRs.

1.1.3.4 *Forwarding Equivalence Class* (FEC)

Una FEC es un subconjunto de paquetes que comparten los mismos atributos para su transporte, de modo que todos recibirán similar tratamiento durante la ruta a su destino; algunos de los atributos que pueden compartir son dirección IP de origen o destino, número de puerto de origen o destino, campo de protocolo de IP, la misma VPN, igual clase de tráfico o requieren el mismo servicio.

La asignación de un paquete a una determinada FEC se la realiza una sola vez cuando el paquete ingresa a la red MPLS, por lo que todos los paquetes de una determinada FEC circularán por el mismo trayecto.

Las FECs permiten agrupar paquetes en clases que se puedan utilizar para establecer prioridades, de tal forma que se pueda dar más prioridad a unas FECs sobre otras, lo que permite dar soporte a operaciones eficientes de QoS. Las FECs pueden agrupar varios flujos de tráfico, pero un mismo flujo no puede pertenecer a más de una FEC al mismo tiempo.

En la figura 1.3 se puede apreciar la asignación de un paquete IP a una FEC de acuerdo al atributo de dirección destino y la colocación de la correspondiente etiqueta.

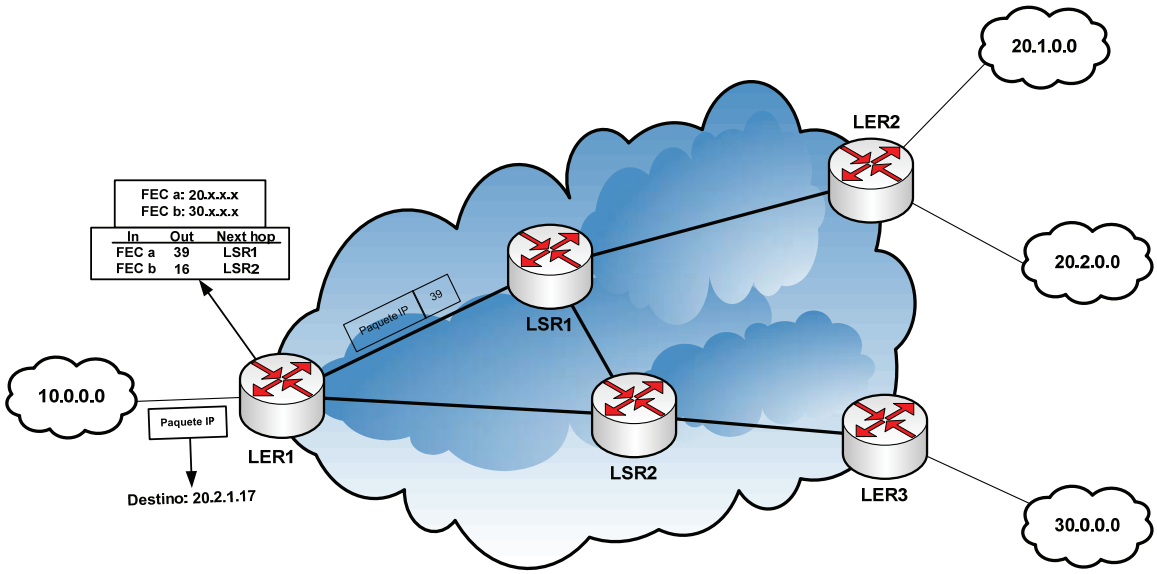

Figura 1.3 Asignación de un paquete a una FEC

1.1.3.5 *Label Switched Path* (LSP)

Un LSP es un camino lógico unidireccional a través de uno o más LSRs que siguen los paquetes de una FEC particular. El tráfico de retorno debe usar un LSP diferente debido a que se trata de caminos de una sola dirección.

Los LERs al recibir un paquete verifican a qué FEC pertenece y lo encaminan por el LSP correspondiente; en el núcleo de la red MPLS, los LSRs ignoran la cabecera IP de los paquetes y simplemente los envían basados en la etiqueta del paquete, utilizando conmutación de etiquetas.

La conmutación de etiquetas permite diseñar LSPs personalizados capaces de soportar aplicaciones y requerimientos específicos. Un LSP puede ser asignado a un mínimo de saltos, reunir ciertos requerimientos para el ancho de banda o simplemente, forzar el tráfico a cruzar ciertos enlaces o nodos de la red.

1.1.3.6 Etiqueta

Una etiqueta es “un identificador corto, de longitud fija, con significado local, que se utiliza para identificar a una FEC. La etiqueta de un determinado paquete representa la FEC a la cual el paquete fue asignado”[7].

La etiqueta es una percepción simplificada de la cabecera de un paquete IP, aún cuando la etiqueta contiene toda la información asociada al direccionamiento de un paquete hasta su destino final en la red MPLS. A diferencia de una cabecera IP, las etiquetas no contienen una dirección IP, sino más bien un valor numérico acordado entre dos nodos consecutivos para proporcionar una conexión a través de un LSP.

Las etiquetas son asociadas a una FEC como resultado de algún evento o política que indique una necesidad para tal asociación; estos eventos pueden ser vinculados por el flujo de datos (*data-driven bindings*) o por el tráfico de control (*control-driven bindings*).

1.1.3.6.1 Formato de la etiqueta

La figura 1.4 muestra el formato de la etiqueta MPLS de 32 bits distribuidos en cuatro campos.

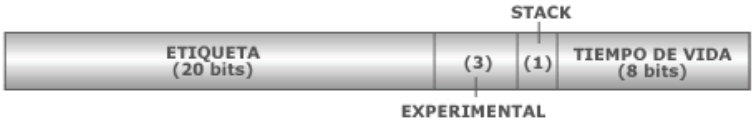

Figura 1.4 Formato de la etiqueta MPLS[8]

Etiqueta.- Constituye los primeros 20 bits. Este campo corresponde a la etiqueta en sí y sirve para identificar una FEC. Existen valores de etiquetas que se encuentran reservados y son los siguientes[9]:

- **0:** Representa la etiqueta explícita nula (*NULL*). Esta etiqueta se encuentra en caso de que sea la única entrada en la pila de etiquetas y el paquete es reenviado basándose en la cabecera del paquete IPv4.
- **1:** Representa la etiqueta de alerta del encaminador y no puede estar en el último lugar de la pila de etiquetas.
- **2:** Representa la etiqueta explícita nula IPv6. Es igual que el primer caso excepto que se reenvía el paquete basándose en la cabecera IPv6.
- **3:** Representa la etiqueta implícita nula.
- **4-15:** Valores reservados.

Experimental (EXP).- Campo formado por 3 bits y considerado de uso experimental. Actualmente, una propuesta para este campo es transmitir información de Servicios Diferenciados (DiffServ).

***Stack* (S).-** Campo de 1 bit que permite apilar etiquetas para realizar un encaminamiento jerárquico. Toma el valor de 1 en la etiqueta que se encuentra en la cima de la pila y 0 para el resto de etiquetas.

Tiempo de vida (TTL).- Campo conformado por 8 bits que tiene el mismo significado que en IP. El TTL se obtiene a partir del TTL definido en el paquete IP, es decrementado en uno con cada LSR y si la cuenta cae a 0 el paquete es excluido, permitiendo evitar lazos.

1.1.3.6.2 Pila de etiquetas[4]

Un paquete etiquetado puede transportar un cierto número de etiquetas organizadas en una estructura jerárquica de pila, que recibe el nombre de “pila de etiquetas”. Las etiquetas se anidan en el paquete formando una pila con funcionamiento *Last-In First-Out* (LIFO), como se indica en la figura 1.5. El procesamiento está siempre basado en la etiqueta superior, sin tener en cuenta que cierto número de etiquetas puedan haber estado sobre ella en la pila anteriormente o que otras tantas estén bajo ella actualmente. Un paquete sin etiquetar se puede ver como un paquete con la pila de etiquetas vacía.

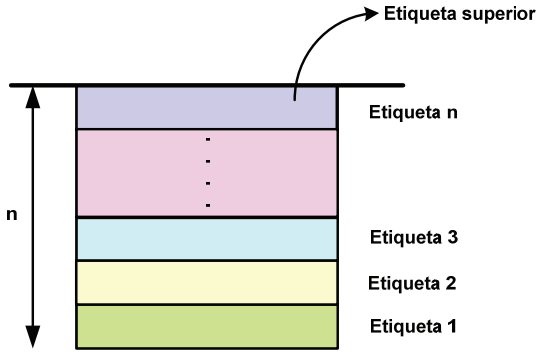

Figura 1.5 Pila de etiquetas con funcionamiento LIFO

1.1.3.6.3 Operaciones sobre etiquetas[11]

Cuando un paquete etiquetado es recibido por un *router* MPLS, sólo la etiqueta que se encuentra en el tope de la pila es examinada. Basado en el contenido de la etiqueta, el *router* efectúa una operación *push*, *pop* o *swap*.

En una operación *push*, una nueva etiqueta es empujada encima de otra (si existe). Si en efecto había otra etiqueta antes de efectuar esta operación, la nueva etiqueta "encapsula" la anterior.

En una operación *pop*, la etiqueta es removida del paquete lo cual puede revelar una etiqueta interior (si existe). A este proceso se lo llama "desencapsulado" y es usualmente efectuado por el *router* de Egreso.

En una operación *swap*, la etiqueta es cambiada por otra y el paquete es enviado en el camino asociado a esta nueva etiqueta.

1.1.3.6.4 Encapsulación de etiquetas

La encapsulación de la etiqueta depende de la tecnología utilizada y presenta dos alternativas:

Cabecera *shim*.- Este mecanismo es adoptado por tecnologías como *Ethernet* y *Point-to-Point* (PPP), que no permiten transportar información de etiqueta en la cabecera del paquete de capa física y requieren de una etiqueta de inserción.

Cabecera *Packet Data Unit* (PDU).- Las etiquetas o encabezados de determinadas tecnologías como el *Virtual Path Identifier*/*Virtual Channel Identifier* (VPI/VCI) de ATM y el *Data Link Control Identifier* (DLCI) de *Frame Relay*, pueden ser usadas como etiquetas MPLS.

1.1.3.6.5 Ubicación de la cabecera MPLS

La cabecera MPLS se ubica después de la cabecera de la capa Enlace y antes de la cabecera de la capa Red, independientemente de la tecnología que se utilice, ya que no está restringida únicamente a la de capa 2, como se muestra en la figura 1.6. El paquete de la capa Red sigue inmediatamente a la entrada de la pila de etiquetas que tiene el bit S en 1.

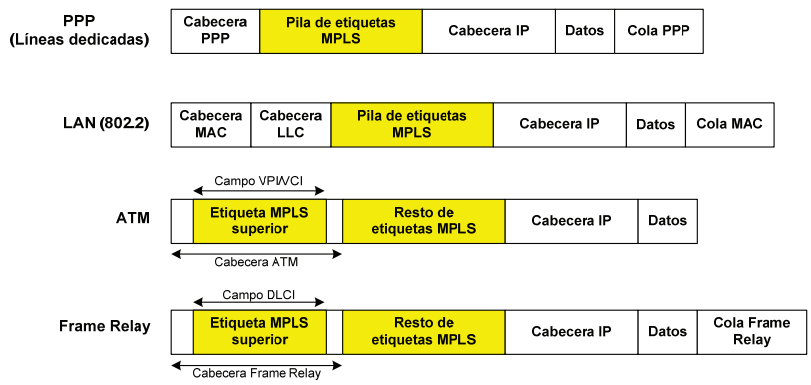

Figura 1.6 Situación de la etiqueta MPLS[12]

1.1.3.7 Componentes de un LSR[5]

La implementación de MPLS en los *routers* mediante la separación de los componentes de control y de envío de información, permite que los nodos

manejen funcionalmente su arquitectura. Al separar los componentes, cada uno de ellos se puede modificar independientemente. La figura 1.7 muestra un diagrama de los componentes de Control y Envío, así como las funciones que realizan en los nodos.

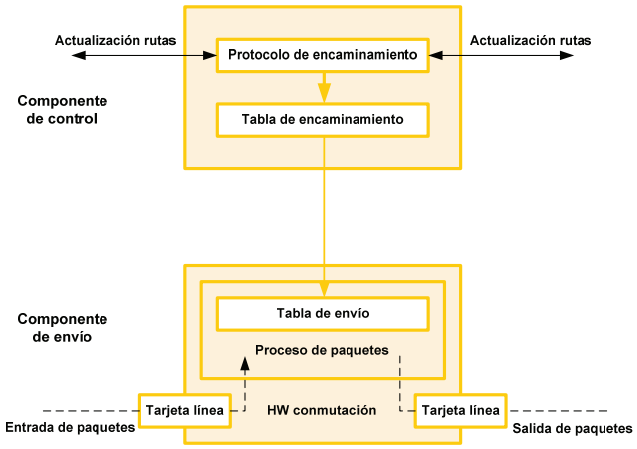

Figura 1.7 Funciones de los componentes de Control y Envío[12]

1.1.3.7.1 Componente de Control

El componente de Control, denominado también como Plano de Control, es el responsable de:

- Generar y mantener las tablas de enrutamiento que permiten establecer los LSPs, las cuales se calculan utilizando los datos de los estados de los enlaces y las políticas de control de tráfico como patrón de tráfico, topología, etc; estas tablas usan la información de enrutamiento que manejan los *Interior Gateway Protocol* (IGP) como *Open Shortest Path First* (OSPF) e *Intermediate System-Intermediate System* (IS-IS).
- Distribuir información de señalización sobre las etiquetas a los LSRs, debido a que si se quiere establecer un circuito virtual, se necesita de algún tipo de señalización para marcar el camino, es decir para realizar la distribución de etiquetas entre los nodos.

Los principales componentes del Plano de Control son los siguientes:

Tabla de enrutamiento.- Esta tabla es calculada utilizando los estados de enlace almacenados en la base de datos y políticas de ingeniería de tráfico. En MPLS, la

tabla de enrutamiento IP proporciona información sobre la red de destino y los prefijos de subred que se utilizan para la asociación de etiquetas.

***Label Information Base* (LIB).-** Tabla donde se almacenan las etiquetas asignadas por el nodo MPLS local y las asignaciones de dichas etiquetas a las etiquetas recibidas de los vecinos, que se usan como índice para asignar a las FECs.

1.1.3.7.2 Componente de Envío

El componente de Envío o Plano de Datos tiene como función conmutar los paquetes MPLS entrantes, basándose en las tablas de enrutamiento ofrecidas por el componente de Control.

Este componente utiliza dos fuentes de información:

***Label Forwarding Information Base* (LFIB).-** Contiene la información requerida para poder realizar la conmutación basada en etiquetas, tales como etiquetas entrantes y salientes, FECs, interfaces entrantes y salientes y su encapsulación, y la dirección del próximo salto. La LFIB usa un subconjunto de etiquetas contenidas en la LIB para el envío del paquete.

La etiqueta transportada por el paquete.- Los LSRs internos intercambian las etiquetas según la tabla de envío LFIB, construida a partir de la información de enrutamiento proporcionada por el Plano de Control.

1.1.4 OPERACIONES DE MPLS

1.1.4.1 Asignación de Etiquetas[5]

Existen tres formas para la asignación de etiquetas que son:

Derivadas del tráfico.- Este tipo de asignación es una forma dinámica de asignación dependiendo de la situación presente en el tráfico. Dicha asignación se inicia con una nueva comunicación que demande el uso de etiquetas. El LSP se establece bajo demanda únicamente cuando hay tráfico por enviar. A este tipo de asignación se le considera como un ejemplo de *data-driven bindings*.

Derivadas de la topología.- El establecimiento de etiquetas se presenta de una manera muy ordenada utilizando para esto una señalización entre nodos de la red. Esta asignación sucede ante situaciones anormales en la red o en el nodo.

Derivadas por solicitud.- Asignación que se da cuando un LSR cambia sus etiquetas en las tablas de envío.

Las dos últimas formas de asignación de etiquetas son ejemplos de *control-driven bindings*, donde la escalabilidad es significativamente mejor, debido a que el número de LSPs es proporcional al número de entradas en la tabla de envío y no al número de flujos de tráfico individuales. MPLS usa el modelo de *control-driven bindings*.

1.1.4.2 Selección del LSP[3][9]

MPLS soporta dos opciones para seleccionar el LSP de una FEC:

Enrutamiento *hop by hop*.- Este enrutamiento es el utilizado en redes IP y emplea protocolos ordinarios como OSPF. Cada LSR elige el siguiente salto hacia donde reenviar los paquetes de una FEC de forma independiente. Se distingue por una conmutación rápida y tratamiento diferencial de paquetes de diferentes FECs, pero no soporta fácilmente ingeniería de tráfico o políticas de enrutamiento.

Enrutamiento explícito (ER-LSP).- En este tipo de enrutamiento, un LSR no puede elegir el siguiente salto. En su lugar, un LER especificará el conjunto de saltos a usar en el LSP. El encaminamiento explícito permite dos modos de operación:

- **Enrutamiento explícito estricto:** Se especifica el LSP entero.
- **Enrutamiento explícito parcial:** Se especifica parte del LSP.

La secuencia de LSRs que se debe seguir en un LSP especificado mediante enrutamiento explícito estricto, podrá ser elegida dinámicamente por un nodo o por configuración, haciéndolo útil para la ingeniería de tráfico y el soporte de QoS.

1.1.4.3 Extracción de la etiqueta en el penúltimo LSR[9]

Una etiqueta puede ser extraída de la pila de etiquetas en el penúltimo LSR del LSP; esta característica sólo es soportada por algunos motores hardware de conmutación, por lo que no se trata de un requisito universal.

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

La extracción en el penúltimo salto tiene una ventaja: si no se realiza, cuando el *router* de Egreso reciba el paquete, éste mirará la etiqueta de la cima de la pila y determinará que es el *router* de salida. Entonces deberá realizar una extracción de la pila y examinar lo que quede del paquete. Si hubiera otra etiqueta en la pila, el *router* de Egreso observaría esta etiqueta y reenviaría el paquete basándose en la información que ha obtenido. Si no hubiera etiquetas en la pila, entonces se reenviaría el paquete utilizando la dirección de destino del nivel de red. Esto obliga a que el LSR de salida haga dos consultas: bien dos consultas de etiquetas o una consulta de etiqueta seguida de una consulta de dirección.

La figura 1.8 indica cómo el *router* de Egreso realiza dos consultas: una consulta de etiqueta seguida de una consulta de dirección, lo que repercute en el rendimiento de dicho nodo.

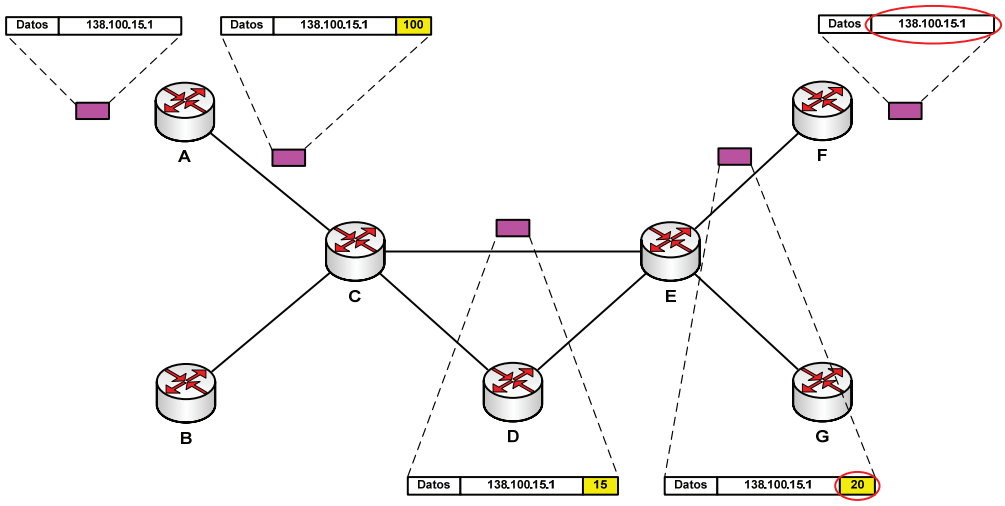

Figura 1.8 Doble consulta por no extraer la etiqueta en el penúltimo salto[9]

Usando la técnica de extracción en el último salto, el *router* de Egreso sólo tiene que hacer una consulta, como se indica en la figura 1.9, y podrá interpretar la etiqueta de la cima de un paquete recibido.

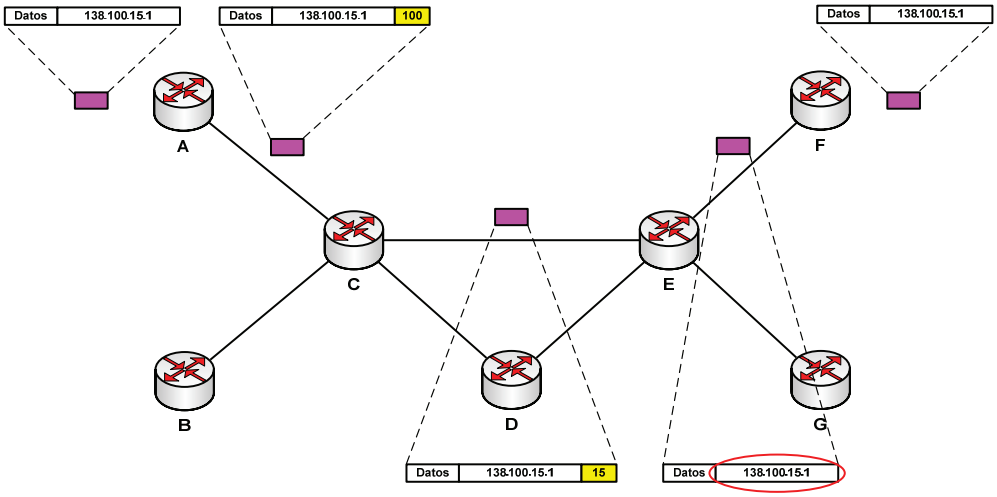

Figura 1.9 Una consulta realizada por extraer la etiqueta en el penúltimo salto[9]

1.1.5 FUNCIONAMIENTO DE MPLS[3][12]

Una red MPLS consiste de un conjunto de nodos denominados LSRs, cuyas funciones son la conmutación y el enrutamiento de paquetes, basados en la etiqueta colocada a cada paquete en su ingreso a la red.

La figura 1.10 indica los pasos de la operación de MPLS dentro de un dominio donde todos los *routers* tienen habilitado el funcionamiento MPLS.

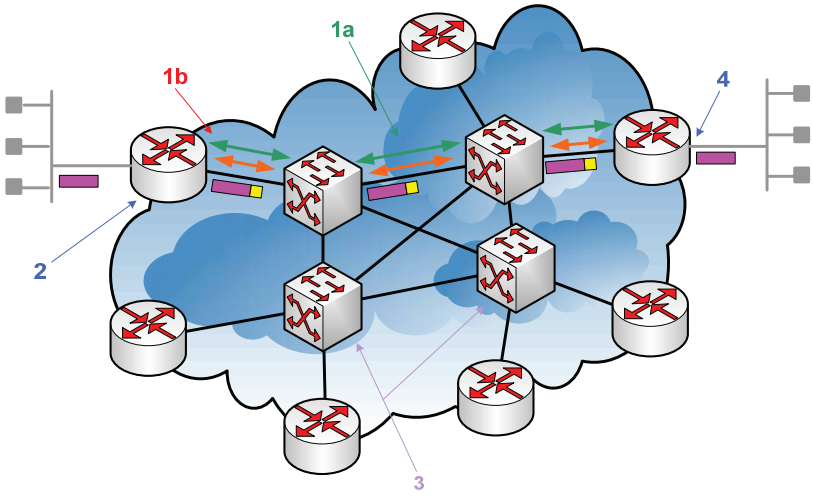

Figura 1.10 Funcionamiento de una red MPLS[12]

1a. Primeramente, se construye las tablas de enrutamiento mediante los protocolos internos como OSPF, IS-IS, *Routing Information Protocol* (RIP), entre otros, con el fin de intercambiar información de enrutamiento y alcance.

1b. Seguidamente, se crean los LSPs mediante las tablas de intercambios de etiquetas, usando un protocolo de distribución de etiquetas que determina la ruta y establece los valores de las etiquetas entre los LSRs adyacentes.

2. Cuando un paquete entra al dominio MPLS a través del LER de ingreso, es procesado para determinar los servicios de nivel de red que requiere, definiendo de esta manera la QoS que recibirá durante su transmisión. El LER asigna el paquete a una FEC particular, y por ende a un LSP en particular; le añade la etiqueta apropiada y lo envía al siguiente salto.

3. Dentro de la red MPLS, cada LSR recibe el paquete etiquetado, revisa su tabla de envío para determinar el siguiente salto, retira la etiqueta de entrada, añade la etiqueta de salida al paquete y lo envía al siguiente LSR a través del LSP. Los LSRs conmutan los paquetes de acuerdo a la etiqueta de entrada e ignoran por completo la cabecera IP.

4. Finalmente, el LER de egreso remueve la etiqueta, lee la cabecera del paquete IP y lo envía a su destino final.

En la figura 1.11 se puede apreciar un ejemplo de las tablas de envío que manejan los nodos MPLS y cómo van cambiando las etiquetas en el LSP.

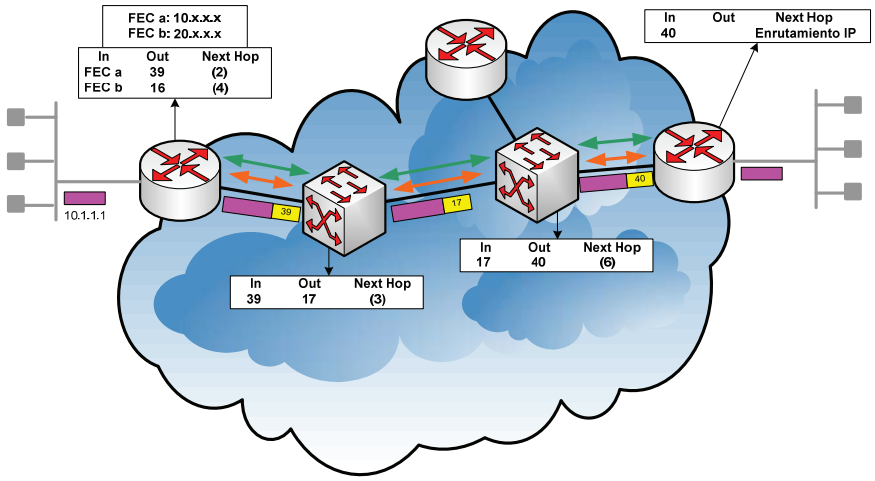

Figura 1.11 Asignación de etiquetas en el LSP

1.1.6 PROTOCOLOS DE DISTRIBUCIÓN DE ETIQUETAS[3][5][10]

Un protocolo de distribución de etiquetas es un conjunto de procedimientos, gracias a los cuales un LSR informa a otro de las asociaciones de etiquetas a FECs que ha realizado. Una desventaja de este método es la introducción de un nuevo protocolo dentro del sistema de red, lo cual aumenta la complejidad del mismo.

Cuando dos LSRs utilizan conjuntamente un protocolo de distribución de etiquetas para intercambiar información de asociaciones de etiquetas a FECs, se les denomina "LDP *peers*", respecto a la información de las asociaciones que intercambian.

MPLS no impone ningún protocolo específico para la distribución de etiquetas. De hecho, se están estandarizando distintos protocolos de distribución de etiquetas, entre los que se distinguen los protocolos nuevos definidos exclusivamente para la distribución de etiquetas y los que incorporan la etiqueta encima de protocolos existentes de encaminamiento. Estos protocolos son los siguientes:

- **Nuevos protocolos**
  - *Label Distribution Protocol* (LDP)
  - *Constraint-Based Routing* LDP (CR-LDP)
- **Protocolos existentes**
  - De enrutamiento con nuevas funciones:
    - *Border Gateway Protocol* (BGP)
    - *Protocol Independent Multicast* (PIM)
  - De señalización:
    - *Resource reSerVation Procotol-Traffic Engineering* (RSVP-TE)

Los nuevos protocolos son propios de MPLS, donde LDP sirve para señalización y gestión del espacio de etiquetas y CR-LDP es una extensión de LDP con funciones para soportar requerimientos de QoS y Clase de Servicio (CoS).

Los protocolos de enrutamiento como BGP permiten llevar información *piggybacked* sobre las etiquetas entre los contenidos propios del protocolo, mientras que PIM se utiliza para direcciones *multicast*. RSVP fue extendido para

soportar intercambio de etiquetas *piggybacked*, ingeniería de tráfico y reserva de recursos, por lo fue denominado como RSVP-TE.

1.1.6.1 *Label Distribution Protocol* (LDP)

LDP es una serie de procedimientos y mensajes mediante los cuales un LSR informa a otro de la asociación etiqueta y FEC, que será utilizada para el establecimiento de un LSP.

Dos LSRs que usan un protocolo de distribución de etiquetas para intercambiar la información de la etiqueta/FEC se les conoce como "puertos de distribución de etiquetas" respecto a la información que intercambian. Si dos LSRs son puertos de distribución de etiquetas, se dice que hay una "distribución de etiquetas adyacente" entre ellos y que han establecido una sesión LDP entre los mismos.

LDP permite a un LSR distribuir etiquetas a sus “LDP *peers*” usando el puerto *Transmission Control Protocol* (TCP) 646. En una sola sesión cada par o vecino es capaz de aprender sobre otros mapas de etiquetas; es decir, este protocolo es bidireccional.

LDP es un protocolo muy útil para los casos en los que se desee establecer un LSP a través de LSRs que no soporten *piggybacking* y como es bidireccional, podrá operar entre LSRs adyacentes o no adyacentes, como se muestra en la figura 1.12.

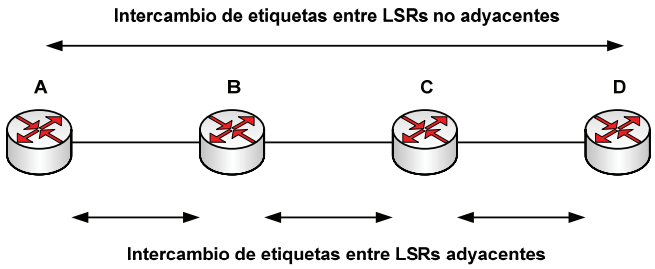

Figura 1.12 Operación de LDP entre LSRs adyacentes y no adyacentes[10]

1.1.6.1.1 Mensajes LDP[5]

LDP provee varios grupos de mensajes LDP, que son los siguientes:

Descubrimiento (*Discovery*).- Se usa para anunciar y mantener la presencia de un LSR en la red. Envía mensajes *HELLO* periódicamente por la red, a través de un puerto *User Datagram Protocol* (UDP) con la dirección *multicast* "todos los encaminadores de esta subred", para así aprender sobre los LSRs con los cuales tiene una conexión LDP directa.

Sesión (*Session*).- Este mensaje se utiliza para establecer, mantener y terminar sesiones LDP. Cuando un LSR descubre a otro por medio de mensajes *HELLO*, utiliza un procedimiento de iniciación LDP por medio de TCP.

Anuncio (*Advertisement*).- Mensajes transportados vía TCP para crear, modificar y eliminar asociaciones de etiqueta/FEC. Con el fin de realizar los diferentes anuncios, se usan los mensajes *label mapping* para anunciar asociaciones etiqueta/FEC, *label withdraw* para revertir el proceso de asociación y *label release* para cuando un LSR recibe información de los *label mappings* y requiere liberar la etiqueta debido a que no la necesita.

Notificación (*Notification*).- Mensaje transportado vía TCP para proveer información de asesoría e información de indicación de errores. Se tienen dos tipos de notificación que son notificación de error, usada para avisar de errores fatales, en cuyo caso se terminará la sesión y se descartarán todas las asociaciones de etiquetas aprendidas en dicha sesión; y, notificación de asesoría, usada para comunicar al LSR acerca de la sesión LDP o el estado de algún mensaje anterior.

1.1.6.1.2 Mecanismo LDP[3][5]

LDP establece las siguientes etapas:

- **Descubrimiento LDP:** Permite que un LSR descubra "LDP *peers*" potenciales. Existen dos tipos de este mecanismo que son descubrimiento básico, usado para descubrir LSRs vecinos que se encuentren conectados directamente al nivel de enlace; y, descubrimiento extendido, utilizado para sesiones LDP entre LSRs que no se encuentran conectados directamente.

- **Establecimiento de la sesión LDP:** Es un proceso que consta de dos pasos que son: establecimiento de la conexión TCP llevado a cabo por el LSR activo (identificador con el LSR más alto), e inicio de sesión donde luego de establecida la conexión TCP se negocian los parámetros de la sesión intercambiando mensajes de *Initialization*. Dos LSRs pueden enviar mensajes de inicialización, el LSR que recibe el mensaje contesta con un mensaje *KeepAlive*, si los parámetros son aceptados. Si los parámetros son inaceptables, el LSR envía un mensaje de notificación de error rechazando la sesión y cerrando la conexión.

La figura 1.13 muestra el intercambio de los diferentes mensajes en los mecanismos de LDP.

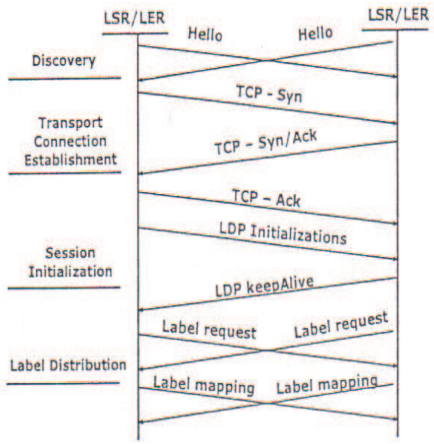

Figura 1.13 Intercambio de mensajes en el mecanismo LDP[3]

1.1.6.1.3 Formato del PDU de LDP[5]

El PDU de LDP consiste de una cabecera LDP seguida por uno o más mensajes LDP, los cuales no necesariamente podrían estar relacionados.

La cabecera LDP está formada por tres campos, como se indica en la figura 1.14.

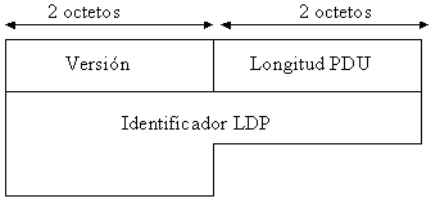

Figura 1.14 Formato de la cabecera del PDU[10]

Versión.- Es un campo de 16 bits que indica la versión del protocolo. La versión actual del protocolo LDP es uno.

Longitud PDU.- Es un campo de 16 bits que especifica la longitud total del PDU, excluyendo los campos de versión y de longitud de la cabecera.

Identificador LDP.- Campo de 48 bits. Este campo identifica el espacio de etiquetas del LSR. Los primeros cuatro octetos identifican el LSR y los dos últimos octetos identifican el espacio de etiquetas dentro del LSR.

Los mensajes LDP consisten de una cabecera seguida por parámetros obligatorios y opcionales, como muestra la figura 1.15.

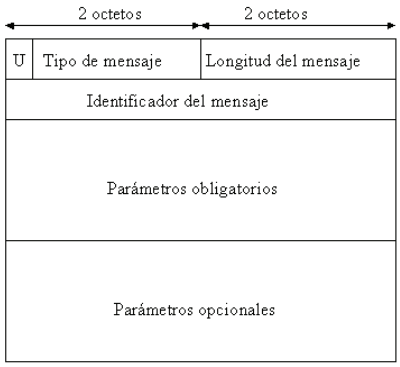

Figura 1.15 Formato del mensaje LDP[10]

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

Tipo de mensaje.- Es un campo de 15 bits que identifica el tipo de mensaje.

Longitud del mensaje.- Es un campo de 16 bits que especifica la longitud total en octetos de los campos identificador del mensaje, parámetros obligatorios y parámetros opcionales.

Identificador del mensaje.- Es un campo de 32 bits que se usa para identificar el mensaje.

Parámetros.- Campo de longitud variable, donde los parámetros son codificados usando un esquema *Type-Length-Value* (TLV). Existen parámetros obligatorios y opcionales. Los parámetros opcionales son usados para la detección de lazos.

1.1.6.1.4 Codificación TLV[5]

Los mensajes LDP usan un esquema de codificación denominado TLV, que se emplea para codificar la información transportada en los mensajes LDP. La figura 1.16 indica los campos que contiene esta codificación.

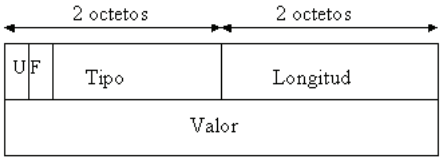

Figura 1.16 Formato de la codificación TLV[10]

Bit U.- Utilizado cuando un TLV desconocido es recibido. Si U=0, se retorna una notificación al creador del mensaje y todo el mensaje es ignorado. Si U=1, el TLV es ignorado y el resto del mensaje es procesado como si el TLV no existiera.

Bit F.- Es un bit TLV de desvío desconocido, aplicado solamente cuando U=1 y el mensaje LDP que contiene el TLV desconocido ha sido desviado. Si F=0, el TLV desconocido no es desviado con el resto del mensaje. Si F=1, el TLV es desviado con el resto del mensaje.

Tipo.- Campo de 14 bits que describe cómo el campo Valor será interpretado.

Longitud.- Campo de 16 bits que indica la longitud del campo Valor en octetos.

Valor.- Es un campo de longitud variable que codifica la información para ser interpretada como se especifica en el campo Tipo. Este campo puede contener por sí mismo uno o más TLVs.

1.1.6.2 *Constraint-Based Routing* LDP (CR-LDP)[5]

El protocolo CR-LDP fue creado para cubrir necesidades de crear LSPs de enrutamiento explícito a través de un dominio MPLS y asegurar que éstos puedan soportar CoS y requerimientos de ingeniería de tráfico. CR-LDP toma en cuenta parámetros como características de enlace (ancho de banda, retardo, etc.), número de saltos y calidad de servicio.

CR es un algoritmo de enrutamiento restringido que calcula los trayectos basándose en los recursos reservados, sin considerar la carga instantánea de los

enlaces; es decir, CR puede seleccionar la trayectoria más larga (en términos de costo), pero con menos carga de tráfico del que se tomaría con enrutamiento convencional, por lo que al mismo tiempo que CR incrementa la utilización de la red, agrega mayor complejidad a los cálculos de enrutamiento.

CR-LDP utiliza UDP para descubrir "LDP *peers*" y TCP para el control, administración y petición de etiquetas.

1.1.6.3 *Border Gateway Protocol* (BGP)[10]

El protocolo BGP se puede utilizar en MPLS para distribuir la información de asociación de etiquetas para cada ruta que se anuncie, gracias al *MultiProtocol Extensions* (MPE) de BGP versión 4.

La distribución de etiquetas se realiza mediante los mensajes de actualización (utilizando *piggybacking*), los cuales también se utilizan para distribuir la información de las rutas. La etiqueta se codifica en el campo *Network Layer Reachability Information* (NLRI); para indicar que el campo NLRI contiene una etiqueta, se utiliza el campo *Subsequent Address Family Identifier* (SAFI). Un *router* que soporta BGP no podrá utilizar BGP para la distribución de etiquetas hacia un igual a no ser que dicho igual le indique que puede procesar mensajes de actualización con el campo SAFI especificado.

Para retirar una ruta anunciada previamente un *router* BGP podrá:

- Anunciar una nueva ruta (y una etiqueta) con la misma NLRI que la ruta previa.
- Listando la NLRI de la ruta previa en el campo de retirada de rutas.

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

1.1.6.4 *Resource reSerVation Procotol-Traffic Engineering* (RSVP-TE)[5]

El protocolo RSVP-TE es una extensión del protocolo RSVP original, diseñado para ejecutar la distribución de etiquetas sobre MPLS; además, soporta la

creación de rutas explícitas con o sin reserva de recursos. Una de las características más importantes de este protocolo es que permite el re-enrutamiento de los túneles LSP, con el objetivo de dar una solución ante las caídas de red, congestión y “cuellos de botella”.

Los *routers* emplean RSVP-TE para enviar los requerimientos de QoS a todos los nodos a lo largo de la trayectoria del flujo y para establecer y mantener el estado que suministre el servicio requerido. Este protocolo lleva el requerimiento de reserva de recursos solicitado por cada *host* receptor a través de la red, transportando mensajes de requerimientos de reserva o mensajes de reserva.

Antes de que el protocolo RSVP–TE envíe los mensajes de reserva, el terminal transmisor debe enviar al receptor mensajes de trayectoria con la misma dirección IP origen y destino que la aplicación usa. Los mensajes de trayectoria irán almacenando en cada *router*, durante su trayectoria al receptor, la dirección IP del *router* anterior, de tal manera que cada uno de los *routers* que constituyen la trayectoria del flujo de datos contiene la dirección IP del *router* previo. De esta manera, el terminal receptor conoce el camino por donde la aplicación llegará.

El uso de RSVP-TE no significa que se requiera de una implementación completa de RSVP para correr en cada LER o LSR dentro de una red MPLS. Un LER o un LSR solo requieren las extensiones para ser capaces de soportar enrutamiento explícito.

1.1.7 APLICACIONES DE MPLS[12][15]

La tecnología MPLS tiene como principal ventaja las aplicaciones que puede soportar, como son[15]:

- **Redes de alto rendimiento:** Las decisiones de enrutamiento que han de tomar los *routers* MPLS son mucho más sencillas y rápidas que las que toma un *router* IP ordinario. La pila de etiquetas permite agregar flujos con mucha facilidad, por lo que el mecanismo es escalable.

- **Soporte multiprotocolo:** Los LSPs son válidos para múltiples protocolos, ya que el encaminamiento de los paquetes se realiza en base a la etiqueta MPLS estándar, no a la cabecera de la capa Red.
- **VPNs:** La posibilidad de crear y anidar LSPs da gran versatilidad a MPLS y hace muy sencilla la creación de VPNs.
- **Ingeniería de tráfico:** Se conoce con este nombre a la planificación de rutas en una red en base a previsiones y estimaciones a largo plazo con el fin de optimizar los recursos y reducir la congestión.
- **QoS:** Es posible asignar a un cliente o a un tipo de tráfico una FEC a la que se asocie un LSP que discurra por enlaces con bajo nivel de carga.

1.1.7.1 *Virtual Private Networks* (VPNs)[12]

Una VPN es una red privada de datos que se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de la VPN es enviar el tráfico mediante un túnel privado seguro, integrando aplicaciones multimedia de voz, datos y vídeo, a través de una red pública compartida como Internet o en el caso de MPLS, la red de un ISP.

En una VPN, los usuarios creen estar en el mismo segmento de red, situación que en realidad no siempre sucede, ya que por lo general se encuentran en redes distintas. Esto se logra gracias al uso de estructuras no conectivas como IP, que permiten crear una especie de túneles privados por los que no puede entrar nadie que no sea miembro de la IP VPN.

Los túneles IP en conexiones dedicadas se pueden establecer de dos maneras:

- En el nivel 3, mediante el protocolo IP *Security* (IPsec) del IETF.
- En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un ISP.

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte

por la red del proveedor. Se lo puede implementar en dispositivos especializados como *firewalls* o en los propios *routers* de acceso del ISP. Sin embargo, como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones de QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio y sólo es válido para paquetes IP nativos, ya que no admite otros protocolos.

En los túneles de nivel 2, se encapsulan paquetes de varios protocolos sobre los datagramas IP de la red del ISP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico.

Los túneles IP presentan muchas ventajas, pero están basados en un modelo topológico superpuesto sobre la topología física existente, lo que hace que presenten ciertas características que los hacen menos eficientes frente a una solución MPLS.

La arquitectura MPLS tiene un modelo topológico que no se superpone, sino que se acopla a la red del proveedor, superando los inconvenientes de los túneles IP. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común", en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs.

En la figura 1.17 se puede apreciar la diferencia entre el modelo “superpuesto” de los túneles IP y el modelo “acoplado” que usa la tecnología MPLS.

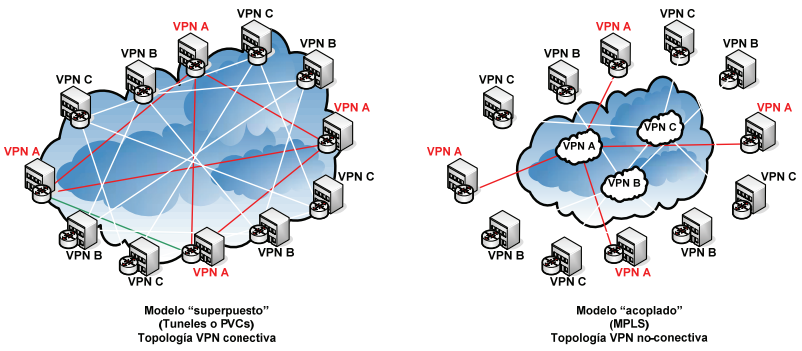

Figura 1.17 Diferencia entre túneles IP y MPLS[12]

1.1.7.2 Ingeniería de tráfico[12]

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los elementos de red, equilibrando de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados.

MPLS es considerado estratégicamente una solución para la ingeniería de tráfico debido a que potencialmente puede proveer más funcionalidad de manera integrada y con bajo coste. Además, ofrece aspectos automáticos de ingeniería de tráfico como la posibilidad de establecer un LSP explícito que permita emular un circuito conmutado en un modelo de enrutamiento.

La ingeniería de tráfico considera las deficiencias de los protocolos de enrutamiento como IGP, por lo que traslada los flujos de tráfico de rutas más congestionadas, seleccionadas por estos protocolos, a otras con menos congestión, aunque estén fuera de la ruta más corta (con menos saltos), sin la necesidad de añadir más capacidad a los enlaces. En la figura 1.18 se comparan dos tipos de caminos para el mismo par de nodos; el camino más corto entre A y B según la métrica normal IGP, es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los nodos correspondientes, haga aconsejable la utilización del camino alternativo con un salto más.

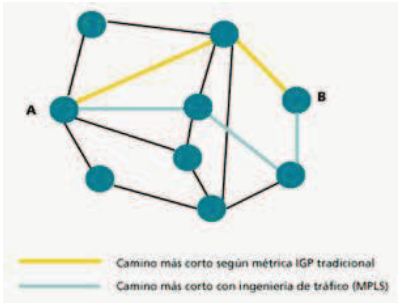

Figura 1.18 Elección de caminos mediante IGP e ingeniería de tráfico[12]

1.1.7.3 Calidad de Servicio (QoS)[15]

QoS es un mecanismo que satisface los requisitos exigidos por los usuarios para determinadas aplicaciones que circulan por la red. En caso de congestión, permite

garantizar que las aplicaciones más críticas como la transmisión de voz o videoconferencia, dispongan de mayor prioridad antes que aplicaciones tradicionales como WWW, correo electrónico o transferencia de ficheros, que son menos críticas.

Al establecer una red con QoS, los enlaces son controlados y el tráfico priorizado, de manera que se pueda distinguir entre diferentes tipos de tráfico y asignar recursos en función de ciertos parámetros como ancho de banda, retardo, *jitter* y pérdidas de paquetes.

El cumplimento de los servicios ofrecidos por las diferentes empresas portadoras, se lo realiza mediante los *Service Level Agreement* (SLAs), que son acuerdos establecidos entre el proveedor del servicio y el cliente, donde se describen las responsabilidades de prestación, recepción y las compensaciones que se apliquen en caso de no cumplirse con los niveles de servicio pactado.

1.1.7.3.1 Clase de Servicio (CoS)[12]

CoS es un término que se utiliza para diferenciar el tráfico de una red, es decir que gestiona diferentes clases de flujos de datos de forma eficaz. Las clases de servicio permiten asignar prioridades a distintos flujos de tráfico, de manera que los datos más importantes tengan preferencia sobre tráfico menos crítico respecto al tiempo.

MPLS es una tecnología que permite ofrecer CoS, ya que las etiquetas MPLS permiten propagar la CoS en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, debido a que el tráfico que fluye a través de un determinado LSP, se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en la etiqueta.

En redes MPLS, se tienen especificaciones para cada LSP. Por ejemplo, si se requiere un servicio de videoconferencia sobre una red MPLS, el LSP tendrá un mayor ancho de banda y se dirigirá por la ruta más corta, lo que permitirá disminuir el retardo y entregar una imagen nítida y en tiempo real; el camino de

esta petición de video será diferente al de una petición para transporte de datos, ya que el transporte de datos no requerirá de nitidez, ni tampoco de tiempo real.

1.2 MODELO DE REFERENCIA TCP/IP

1.2.1 INTRODUCCIÓN[16][17]

La red Internet comenzó siendo una red informática del *Advanced Research Projects Agency* (ARPA), patrocinada por el Departamento de Defensa de Estados Unidos (DoD) y denominada ARPANET; ésta conectaba redes de ordenadores de varias universidades y laboratorios de investigación, usando líneas telefónicas rentadas. Estos ordenadores procedían de una variedad de fabricantes y tenían diferencias tanto en hardware como en software, por lo que para posibilitar su comunicación fue necesario un conjunto de reglas formales para su interacción. A estas reglas se les denominó protocolos.

A medida que la red fue creciendo, se añadieron redes satelitales y de radio, lo que provocó que los protocolos existentes tuvieran problemas para interactuar con este tipo de redes, motivo por el cual el informático estadounidense Vinton Cerf desarrolló en 1973 los protocolos: *Internet Protocol* (IP) y *Transmission Control Protocol* (TCP), como parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por ARPA.

El proyecto tenía como objetivo crear una arquitectura que conectara múltiples redes que fueran capaces de sobrevivir a la pérdida del hardware de subred, mientras las máquinas de origen y destino estuvieran funcionando; esta arquitectura se popularizó como el modelo de referencia TCP/IP.

TCP/IP no es un único protocolo, es un conjunto de protocolos que cubren los distintos niveles del modelo OSI y toma su nombre en referencia a los dos protocolos más importantes que lo componen y que fueron los dos primeros en definirse.

1.2.2 DEFINICIÓN DE TCP/IP[18][19]

A diferencia de las tecnologías de *networking* propietarias, TCP/IP fue desarrollado como un estándar, lo que ayudó a su rápida evolución. Este modelo es un conjunto de protocolos que son la base de Internet y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PCs, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extendida (WAN).

En algunos aspectos, TCP/IP representa todas las reglas de comunicación para Internet y se basa en la noción de direccionamiento IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder enrutar paquetes.

1.2.3 ARQUITECTURA TCP/IP[18]

TCP/IP puede describirse por analogía con el modelo OSI, que describe los niveles o capas de la pila de protocolos, donde cada nivel soluciona una serie de problemas relacionados con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables. La figura 1.19 muestra la correspondencia entre las capas del modelo OSI y TCP/IP.

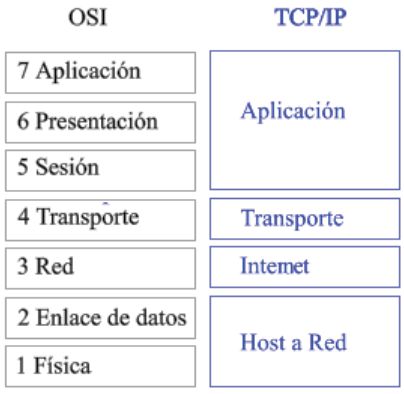

Figura 1.19 Correspondencia entre capas de los modelos OSI y TCP/IP[17]

1.2.3.1 Capa *Host* a Red

Esta capa de nivel inferior consta de una capa de interfaz de red responsable de aceptar los datagramas IP y transmitirlos hacia una red específica. Una interfaz de

red puede consistir en un dispositivo controlador o un complejo subsistema que utiliza un protocolo de enlace de datos propio.

La capa *Host* a Red no tiene un protocolo definido, pero trabaja con los protocolos de las tecnologías más comunes como *Ethernet* IEEE 802.3, *Token Bus* IEEE 802.4, *Token Ring* IEEE 802.5, Wi-Fi IEEE 802.11 y FDDI (*Fiber Distributed Data Interface*).

1.2.3.2 Capa Internet

La capa Internet provee de un servicio de entrega de paquetes de una máquina a otra, dejando que éstos viajen separadamente hasta su destino. La integridad de los datos no se verifica en este nivel, por lo que el mecanismo de verificación es implementado en capas superiores.

Esta capa define un formato de paquete y un protocolo denominado IP. Otros protocolos relacionados con esta capa que se encuentran encima de IP como *Internet Control Message Protocol* (ICMP) e *Internet Group Management Protocol* (IGMP) van encapsulados en IP, aunque realizan funciones del nivel de red e ilustran una incompatibilidad entre los modelos de TCP/IP y OSI. Todos los protocolos de enrutamiento como BGP, OSPF, y RSVP son realmente también parte del nivel de red, aunque ellos parecen pertenecer a niveles más altos.

1.2.3.3 Capa Transporte

La principal tarea de la capa Transporte es proporcionar la comunicación entre un programa de aplicación y otro; este tipo de comunicación se conoce frecuentemente como comunicación punto a punto. Además, regula el flujo de información y soluciona problemas como la fiabilidad y la seguridad de que los datos llegan en el orden correcto mediante el envío de acuses de recibo de retorno y retransmisión de paquetes perdidos.

Esta capa debe aceptar datos desde varios programas de aplicación, añadir información adicional a cada paquete y enviarlos a la capa del siguiente nivel. En

el nivel de Transporte, los protocolos que las aplicaciones normalmente usan son TCP y UDP.

1.2.3.4 Capa Aplicación

Este nivel es el que los programas más comunes utilizan para comunicarse a través de una red con otros programas. Los procesos que acontecen en este nivel son aplicaciones específicas que pasan los datos al nivel de aplicación en el formato que internamente use el programa, para ser codificados de acuerdo con un protocolo estándar.

Aquí se incluyen protocolos destinados a proporcionar servicios tales como correo electrónico, transferencia de ficheros, conexión remota, entre otros. Los protocolos y servicios más comunes en esta capa son HTTP (*Hypertext Transport Protocol*), FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transport Protocol*), POP (*Post Office Protocol*), DNS (*Domain Name System*), DHCP (*Dynamic Host Configuration Protocol*), TELNET (*Telecommunication Network*), TFTP (*Trivial File Transport Protocol*), LDAP (*Lightweight Directory Access Protocol*), SSH (*Secure Shell*), HTTPS (*Hypertext Transport Protocol Secure*), entre otros.

1.2.4 PROTOCOLOS TCP/IP

La figura 1.20 indica las tecnologías y los protocolos que maneja el modelo TCP/IP en cada una de sus capas.

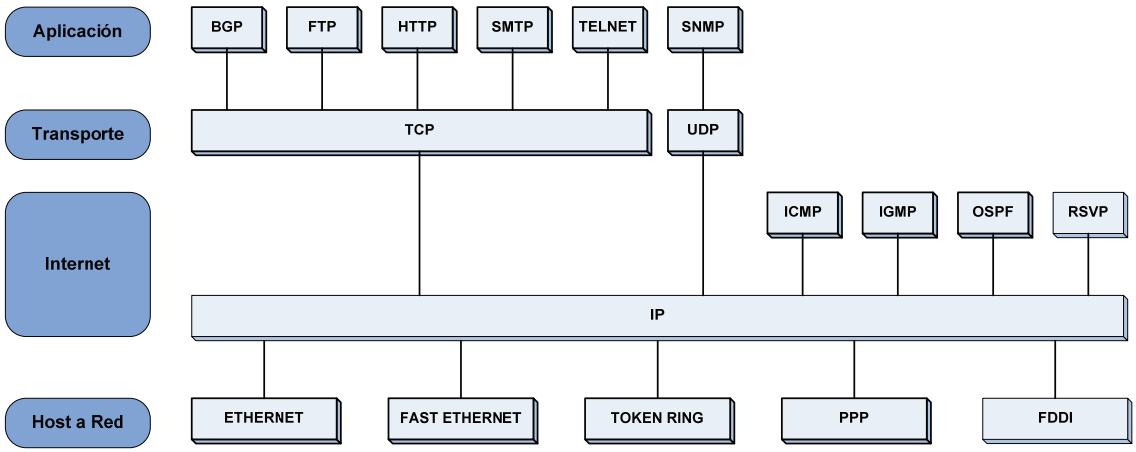

Figura 1.20 Tecnologías y protocolos del modelo TCP/IP

1.2.4.1 *Internet Protocol* (IP)[20][21]

IP es uno de los protocolos de Internet más importantes, ya que permite el desarrollo y transporte de datos en bloques conocidos como paquetes o datagramas. En particular, IP no necesita de ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes, sólo necesita hacer uso de las direcciones IP que contiene el datagrama. El protocolo IP está especificado en los RFCs 791, 950, 919 y 922, actualizados en el RFC 1349.

Este protocolo cubre tres aspectos importantes:

- Define la unidad básica para la transferencia de datos en una red, especificando el formato exacto de un datagrama IP.
- Realiza las funciones de ruteo.
- Define las reglas para que los *hosts* y *routers* procesen paquetes, los descarten o generen mensajes de error.

IP provee de un servicio de datagramas no fiable (mejor esfuerzo), ya que no posee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad a sus cabeceras y no a los datos que está transmitiendo.

1.2.4.1.1 Datagrama IP[21]

Los datos circulan en Internet en forma de datagramas, que son los datos encapsulados a los que se les agrega una cabecera con información necesaria para su transporte. Los *routers* analizan (y eventualmente modifican) los datos contenidos en un datagrama para que puedan transitar por la red.

Los datagramas IP están formados por “palabras” de 32 bits. Cada datagrama tiene una cabecera con un mínimo de cinco y un máximo de quince palabras. Los campos que componen el datagrama IP se muestran en la figura 1.21.

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

Figura 1.21 Formato del datagrama IP

Versión (Ver).- Campo de 4 bits que indica la versión del protocolo IP que se está utilizando para verificar la validez del datagrama. La versión actual que está en uso es la versión 4, aunque ya se está empleando la versión 6.

Longitud del encabezado (HLen).- Campo de 4 bits que indica la cantidad de palabras de 32 bits que componen la cabecera.

Tipo de servicio (ToS)[1]**.-** Campo de 8 bits cuya función es indicar la importancia del datagrama. Su estructura se muestra en la figura 1.22.

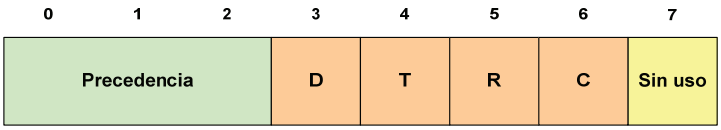

Figura 1.22 Estructura del campo ToS[1]

- **Precedencia:** Subcampo de 3 bits usado para asignar un nivel de prioridad a un datagrama. Aunque se dispone de 8 posibles niveles de combinación, los dos valores máximos están reservados para utilización interna de la red, lo que permite proporcionar un mecanismo para dividir el tráfico en hasta seis clases de servicio. Los bits 0-2 de la figura 1.22 definen las precedencias:
  - 111 Control de red
  - 110 Control de la red de interconexión
  - 101 Urgente
  - 100 Anulación de *flash*
  - 011 Flash
  - 010 Inmediato

- 001 Prioridad
- 000 Rutinario

- **Bits D, T, R y C:** La intención original de estos bits fue proporcionar un mecanismo para especificar el retardo, flujo de salida, fiabilidad y requisitos de coste de un datagrama respectivamente, pero su utilización nunca consiguió su objetivo debido a que el tráfico IP es no fiable, lento y costoso. Los significados de los valores que pueden tomar estos subcampos son:
  - **Bit D (*Delay*):** 0 normal, 1 bajo retardo
  - **Bit T (*Throughput*):** 0 normal, 1 alto
  - **Bit R (*Reliability*):** 0 normal, 1 alta
  - **Bit C (*Cost*):** 0 normal, 1 bajo

Longitud total.- Este campo de 16 bits indica el tamaño total del datagrama en bytes. El tamaño de este campo es de 2 bytes, por lo tanto el tamaño total del datagrama no puede exceder los 65536 bytes. Si se lo utiliza junto con el tamaño de la cabecera, este campo permite determinar el tamaño de los datos.

Identificación.- Campo de 16 bits que identifica al datagrama, permite implementar números de secuencia para reconocer los diferentes fragmentos de un mismo datagrama, ya que todos ellos comparten este mismo número.

Banderas (*Flags*).- Campo compuesto por tres bits que indican lo siguiente:

- El primer bit está reservado
- El segundo bit es denominado *Don´t fragment* (DF) e indica si se puede fragmentar el datagrama o no. Si el bit DF está en 0, entonces el datagrama puede desfragmentarse; caso contrario, si DF está en 1, no puede fragmentarse el datagrama. Si el datagrama tiene este bit en 1 y el *router* no puede enrutarlo sin fragmentarlo, el datagrama se rechaza con un mensaje de error.
- El tercer bit denominado *More Fragments* (MF) indica si el datagrama es un fragmento de datos. Si MF se encuentra en 0, esto indica que el fragmento es el último o que el datagrama no se ha fragmentado; caso contrario, significa que se tienen más fragmentos.

Margen del fragmento.- Campo de 13 bits que brinda la posición del comienzo del fragmento en el datagrama inicial. La unidad de medida para este campo es de 8 bytes (el primer fragmento tiene un valor igual a 0).

Tiempo de vida (TTL).- Este campo de 8 bits especifica el número máximo de *routers* por los que puede pasar un datagrama. Por lo tanto, este campo disminuye con cada paso por un *router* y cuando alcanza el valor crítico de 0, el *router* descarta el datagrama. Esto evita que la red se sobrecargue de datagramas perdidos.

Protocolo.- Campo de 8 bits que especifica, en notación decimal, qué protocolo de alto nivel se empleó para construir el mensaje transportado en el campo Datos del datagrama IP.

Suma de comprobación del encabezado (*Checksum*).- Este campo contiene un valor codificado de 16 bits, que permite controlar la integridad del encabezado para establecer si se ha modificado durante la transmisión. La suma de comprobación es la suma de todas las palabras de 16 bits de la cabecera, excluyendo este campo. Esto se realiza de tal modo que cuando se suman los campos del encabezado, incluyendo este campo, se obtenga un número con todos los bits en 1.

Dirección IP origen.- Este campo representa la dirección IP de 32 bits del equipo remitente y permite que el destinatario responda.

Dirección IP destino.- Campo que representa la dirección IP de 32 bits del destinatario del mensaje.

Opciones IP.- Existen hasta 40 bytes opcionales extra en la cabecera del datagrama IP que pueden llevar una o más opciones. Su uso es bastante raro.

1.2.4.1.2 IP versión 6[22]

IPv6 es el sucesor propuesto de IPv4 y es también conocido como protocolo de Internet de nueva generación. El número de versión de este protocolo es 6 frente

a la versión 4 utilizada hasta entonces, puesto que la versión 5 no pasó de la fase experimental.

Los cambios que se introdujeron en esta nueva versión son muchos y de gran importancia, aunque la transición desde la versión 4 no debería ser problemática, gracias a las características de compatibilidad que se han incluido en el protocolo. IPv6 se ha diseñado para solucionar todos los problemas que surgieron con la versión anterior, además de ofrecer soporte a las nuevas redes de alto rendimiento como ATM, *Gigabit Ethernet*, entre otras.

Una de las características más llamativas es el nuevo sistema de direcciones, en el cual se pasa de 32 a 128 bits, eliminando todas las restricciones del sistema actual. Otro de los aspectos mejorados es la seguridad, que en la versión anterior constituía uno de los mayores problemas. Además, el nuevo formato de la cabecera se ha organizado de una manera más efectiva, permitiendo que las opciones se sitúen en extensiones separadas de la cabecera principal.

1.2.4.2 *Transmission Control Protocol* (TCP)[23][24]

El protocolo TCP es un protocolo de comunicación orientado a conexión y fiable, actualmente documentado en el RFC 793. En la pila de protocolos TCP/IP, TCP es la capa intermedia entre las capas Internet y Aplicación. En el nivel de Aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo o van hacia él. Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo Protocolo en 6.

Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable, TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe libre de errores, sin pérdidas y con seguridad. Además, proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

Las principales características del protocolo TCP son:

- Coloca los datagramas nuevamente en orden cuando vienen del protocolo IP.
- Permite que los datos se formen en segmentos de longitud variada para "entregarlos" al protocolo IP.
- Capacidad para controlar la velocidad de los datos usando su capacidad para emitir mensajes de tamaño variable, llamados segmentos.
- Multiplexa los datos, es decir, permite que la información que viene de diferentes fuentes en la misma línea pueda circular simultáneamente.
- Por último, TCP permite comenzar y finalizar la comunicación amablemente.

1.2.4.2.1 Puertos TCP[24]

TCP usa el concepto de número de puerto para identificar a las aplicaciones emisoras y receptoras. Cada lado de la conexión TCP tiene asociado un número de puerto de 16 bits sin signo, por lo que existen 65536 puertos posibles, asignados por la aplicación emisora o receptora. Los puertos son clasificados en las categorías bien conocidos, registrados y dinámicos/privados.

Los puertos bien conocidos son asignados por la IANA, van del 0 al 1023 y son usados normalmente por el sistema o por procesos con privilegios. Las aplicaciones que usan este tipo de puertos son ejecutadas como servidores y se quedan a la escucha de conexiones.

Los puertos registrados son normalmente empleados por las aplicaciones de usuario de forma temporal cuando conectan con los servidores, pero también pueden representar servicios que hayan sido registrados por un tercero. El rango de puertos registrados va desde el 1024 al 49151.

Los puertos dinámicos/privados también pueden ser usados por las aplicaciones de usuario, pero este caso es menos común. Estos puertos no tienen significado fuera de la conexión TCP en la que fueron usados y su rango es desde el 49152 al 65535.

1.2.4.3 *User Datagram Protocol* (UDP)[25][26]

El protocolo UDP es un protocolo no orientado a conexión de la capa Transporte del modelo TCP/IP, documentado en el RFC 768 de la IETF.

UDP se basa en el intercambio de segmentos a través de la red sin haber establecido previamente una conexión, ya que el propio segmento incorpora suficiente información de direccionamiento en su cabecera. Este protocolo no tiene detección de errores, ACKs en la entrega o recepción, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros. Su uso principal es para protocolos en los que el intercambio de paquetes es mayor o no es rentable con respecto a la información transmitida, así como para la transmisión de audio y video en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

1.2.4.3.1 Puertos UDP[26]

UDP utiliza puertos para permitir la comunicación entre aplicaciones. El rango de valores válidos para los puertos va desde 0 hasta 65535. El puerto 0 está reservado, pero es un valor permitido como puerto origen si el proceso emisor no espera recibir mensajes como respuesta. Los puertos se clasifican en tres categorías:

- Los puertos 1 al 1023 se llaman puertos "bien conocidos".
- Los puertos 1024 al 49151 son puertos registrados.
- Los puertos 49152 al 65535 son puertos efímeros y son utilizados como puertos temporales, sobre todo por los clientes al comunicarse con los servidores.

1.3 CALIDAD DE SERVICIO (QoS) EN INTERNET

1.3.1 INTRODUCCIÓN

Internet fue desarrollada para proveer un servicio no confiable, utilizada principalmente para la transferencia de archivos, correo electrónico y acceso

remoto. Sin embargo, su abrumador crecimiento en los últimos años ha llevado a la proliferación de múltiples servicios y a la búsqueda de simplificar la operación y gestión de la misma. Hoy en día, se están desplegando aplicaciones tales como VoIP y videoconferencia, que tienen fuertes requerimientos de ancho de banda, de retardo, y tasa de paquetes perdidos extremadamente baja. Además, los diferentes agregados de tráfico que circulan por la red necesitan ser diferenciados, pues las distintas aplicaciones tienen distintas necesidades de recursos.

El procedimiento de asegurar los requerimientos y recursos de las aplicaciones, así como diferenciar los agregados de tráfico, se conoce como Calidad de Servicio (QoS). QoS significa disponibilidad de la red y eficiencia en la transmisión, lo que ayuda a mejorar el servicio a los usuarios y a reducir los costos de ofrecer dichos servicios, sin la necesidad de incrementar continuamente la capacidad de la red.

La implementación de QoS asegura una correcta entrega de la información necesaria o crítica, dando preferencia a aplicaciones críticas, donde se comparten simultáneamente los recursos de la red con otras aplicaciones no críticas. QoS hace la diferencia, al prometer un uso eficiente de los recursos ante la situación de congestión, seleccionando un tráfico específico de la red y priorizándolo según su importancia relativa.

1.3.2 DEFINICIÓN DE QoS[6]

En el año de 1984, la *International Telecommunication Union* (ITU) definió el término QoS en el documento E-800 como “el efecto colectivo del rendimiento de un servicio que determina el grado de satisfacción del usuario de dicho servicio”. Esta definición deja en claro que se trata de una percepción del usuario, quien establece los requerimientos mínimos para cualificar el grado de satisfacción del servicio.

En otras palabras, QoS podría definirse como el valor de un conjunto de parámetros de rendimiento que aseguran al usuario un servicio con niveles

aceptables de calidad. Como distintos tipos de servicio mantienen características particulares, cada uno tendría su propia QoS.

El término QoS engloba toda técnica que se refiera a ella y muchas veces es confundido con los términos Clase de Servicio (CoS) y Tipo de Servicio (ToS), que son dos técnicas utilizadas para su obtención. La CoS permite a los administradores de red solicitar prioridad para un tráfico, mientras que el ToS equivale a una ruta de uso compartido donde el ancho de banda es reservado con antelación para asignar el tráfico que necesite preferencia.

1.3.3 PARÁMETROS DE QoS[6][15][28]

Los parámetros que normalmente se utilizan hoy en día para definir la QoS en Internet son los siguientes:

- Ancho de banda disponible
- Tasa de paquetes perdidos
- Retardo
- *Jitter*

1.3.3.1 Ancho de banda disponible

El ancho de banda permite calcular la máxima capacidad de transferencia de datos entre dos extremos de la red. El límite lo impone la infraestructura física de los enlaces y es expresado en *Hertzios* (Hz) o en *Megahertzios* (MHz).

1.3.3.2 Tasa de paquetes perdidos

La tasa de paquetes perdidos corresponde al número de paquetes perdidos desde el comienzo de la recepción. Se calcula como el número de paquetes esperados menos el número de paquetes recibidos, contabilizando paquetes duplicados o retrasados, por lo que la tasa de paquetes perdidos puede resultar negativa.

1.3.3.3 Retardo

El retardo es el tiempo de retraso en la llegada de los paquetes hasta su destino. Este retraso puede producirse debido a la prioridad de ciertos flujos y a los picos de tráfico.

1.3.3.4 Jitter

El *jitter* es la fluctuación que se puede producir en el retardo de ida y vuelta medio. Una de la causas del *jitter* es la distorsión de los tiempos de llegada de los paquetes recibidos, comparados con los tiempos de los paquetes transmitidos originalmente. El aumento de esta fluctuación provoca que en el destino se entregue una señal distorsionada.

Se puede reducir el *jitter* añadiendo un retardo adicional en el lado del receptor. Por ejemplo, con un retardo de 70 ± 20 ms se puede asegurar un *jitter* de 0 si el *buffer* del receptor añade un retardo de 40 ms (90 ± 0 ms), como se indica en la figura 1.23. Para el retardo adicional, el receptor ha de tener un *buffer* suficientemente grande. En algunas aplicaciones no es posible añadir mucho retardo pues esto reduce la interactividad como en la videoconferencia y la telefonía por Internet.

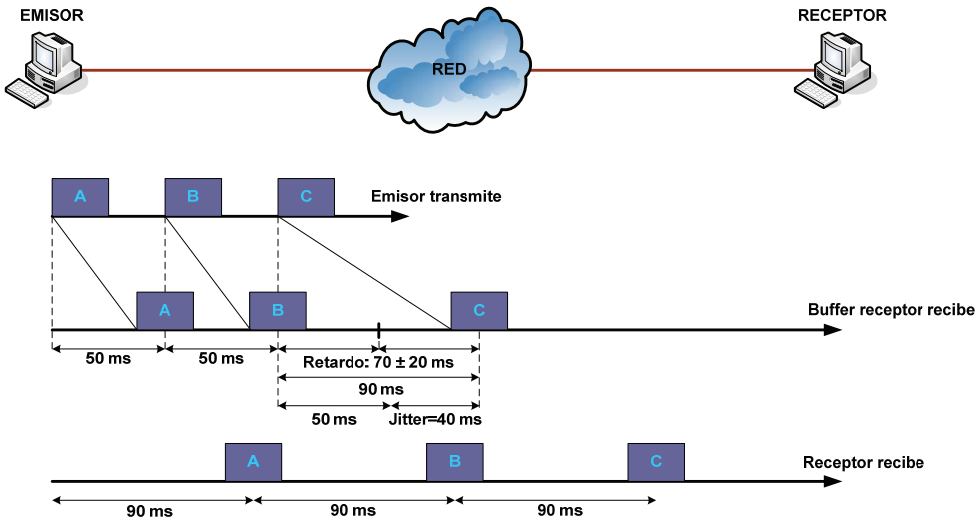

Figura 1.23 *Jitter* en la transmisión de paquetes[15]

1.3.4 CLASIFICACIÓN DE QoS[6]

La QoS se la puede clasificar de muchas formas, pero especialmente por lo siguiente:

- Según la sensibilidad del tráfico
- Según las garantías
- Según el lugar de aplicación

1.3.4.1 Según la sensibilidad del tráfico

Los diferentes flujos de tráfico que circulan por las redes tienen distintos requerimientos de ancho de banda, tasa de paquetes perdidos, retardo y *jitter*, por lo que según estos parámetros, la QoS puede clasificarse como:

- **QoS muy sensible al retardo:** Para esta clase de tráfico es necesario garantizar la cantidad y disponibilidad del ancho de banda y un valor de retado mínimo que asegure su correcta transmisión.
- **QoS algo sensible al retardo:** Para este tipo de tráfico se debe garantizar un cierto nivel de ancho de banda menor que el anterior.
- **QoS muy sensible a pérdidas:** Esta clasificación abarca el tráfico tradicional. Si se garantiza un nivel de pérdidas de valor cero, entonces los paquetes nunca se descartarían y a su vez, los *buffers* de almacenamiento no se desbordarían.
- **QoS nada sensible:** La filosofía de este tráfico es usar cualquier oportunidad de transmisión, asumiendo que la capacidad del *buffer* es suficiente para llevar a cabo dicha transmisión con la prioridad de tráfico más baja. El algoritmo que corresponde a este tipo de QoS es el de “mejor esfuerzo”.

1.3.4.2 Según las garantías

Esta clasificación tiene muy en cuenta la reserva de recursos que la red necesita para proporcionar los servicios, así se tiene:

- **QoS garantizada:** Esta QoS produce una reserva absoluta de los recursos de la red para un tráfico determinado.
- **QoS no garantizada:** Es una QoS sin garantías, el tráfico correspondiente a este tipo de QoS es el que se tiene en los servicios de "mejor esfuerzo".
- **QoS diferenciada:** Es el punto medio entre los dos tipos de QoS anteriores, donde se realiza una diferenciación del tráfico.

1.3.4.3 Según el lugar de aplicación

La QoS es posible aplicarla en los bordes o en los extremos de la red, por tal motivo se tiene:

- **QoS extremo a extremo:** Esta clase de servicio es la aplicación de las políticas de QoS entre los extremos de una red. Comúnmente se la conoce como QoS absoluta. Una de las ventajas de utilizar esta QoS es que las aplicaciones podrían seleccionar dinámicamente el nivel de QoS.
- **QoS borde a borde:** Es la aplicación de políticas de servicio entre dos puntos cualquiera de la red, lo que trae consigo varias ventajas, una de ellas es que no requiere que los administradores de red toquen ninguno de los extremos. Otra ventaja es que el número de dispositivos que deben ser manejados para la obtención de QoS es menor. Este tipo de QoS se la conoce como QoS relativa.

1.3.5 ARQUITECTURAS DE QoS[6]

Durante los últimos años han surgido varias arquitecturas para establecer QoS en equipamientos de redes, donde cada red puede tomar ventaja de distintos aspectos en implementaciones de QoS para obtener una mayor eficiencia. Las arquitecturas desarrolladas proveen las siguientes características:

- Lineamientos para distribuir recursos que soporten el aseguramiento de recursos y diferenciación de servicios.
- Nuevos modelos de servicios, además del de "mejor esfuerzo".
- Lenguaje para describir el aseguramiento de recursos y los requerimientos de los mismos.

- Mecanismos para diferenciar los agregados de tráfico.

La IETF ha propuesto diversas tecnologías que cumplen estas características, de las cuales se tiene dos arquitecturas claramente diferenciadas y comúnmente utilizadas que son:

- Servicios Integrados (IntServ)
- Servicios Diferenciados (DiffServ)

1.3.5.1 Arquitectura de Servicios Integrados (IntServ)[6][31][33]

IntServ fue la primera arquitectura de QoS desarrollada por la IETF a principios de los años 90. En el diseño se consideró que las aplicaciones de tiempo real serían las más importantes y sensibles de las aplicaciones que necesitan QoS.

Esta arquitectura definida en el RFC 2210, cuyo objetivo es disponer de una sola red IP que transporte tráfico de “mejor esfuerzo” y multimedia de tiempo real, permite reservar los recursos de ancho de banda y tamaño de cola precisos para proveer a las aplicaciones de un nivel garantizado de servicio, negociando parámetros de red, de extremo a extremo.

La reserva de recursos es realizada por la aplicación, la misma que solicita el nivel de servicio necesario para ella antes de comenzar a operar, con el fin de trabajar apropiadamente. Para realizar la solicitud, primeramente se caracteriza la fuente del flujo y sus requerimientos, luego la red utiliza un algoritmo de ruteo para elegir la ruta que cumpla con dichos requerimientos y por último, un protocolo de reservación establece el estado de reserva a lo largo de la ruta, para lo cual cada nodo debe chequear si hay recursos disponibles antes de aceptar la reserva. Estas reservaciones se mantienen en pie hasta que la aplicación termina o hasta que el ancho de banda requerido por ésta sobrepase el límite reservado para dicha aplicación.

1.3.5.1.1 Niveles de servicio[6]

IntServ proporciona tres niveles de servicio a elegir por los usuarios y son los siguientes:

- **Mejor esfuerzo:** Es el nivel de servicio tradicional que no brinda ninguna garantía.
- **Carga controlada:** Nivel de servicio definido en el RFC 2211 que exige a los medios de la red un comportamiento semejante al del “mejor esfuerzo” en situaciones de bajo nivel de carga, con lo que se logra mantener muy bajos la tasa de paquetes perdidos y el retardo. Además, no se requiere realizar ningún control del *jitter*.
- **Carga garantizada:** Nivel definido en el RFC 2212 que asegura a las aplicaciones que no se producirán pérdidas por congestión mientras el tráfico se halle dentro de los parámetros acordados y asegura un tiempo máximo garantizado de transmisión de extremo a extremo.

1.3.5.1.2 Resource reSerVation Protocol (RSVP)[27][33]

La arquitectura IntServ se basa en el protocolo RSVP para señalizar y reservar la QoS deseada para cada flujo en la red. Debido a que la información de estados para cada reserva necesita ser mantenida por cada enrutador a lo largo de la ruta, la escalabilidad para cientos de miles de flujos a través de una red central, típicos de una red óptica, se convierte en un problema.

RSVP está descrito en el RFC 2205 y es un protocolo de capa Transporte designado para reservar recursos a través de una red integrada de servicios de Internet. RSVP reserva los canales o rutas en redes internet para la transmisión por *unicast* y *multicast* con escalabilidad y robustez.

RSVP puede ser utilizado tanto por *hosts* como por *routers* para pedir o entregar niveles específicos de QoS para los flujos de datos de las aplicaciones. RSVP define cómo las aplicaciones deben hacer las reservas y cómo liberar los recursos reservados una vez que han terminado. Las operaciones RSVP generalmente dan como resultado una reserva de recursos en cada nodo a lo largo de un camino.

A pesar de las características que proporciona RSVP, la arquitectura IntServ está limitada a redes locales o de pequeño tamaño por su escalabilidad, pues se requiere una reserva explícita para cada flujo de datos y en Internet éstos pueden ser varios miles, cada uno con una entrada en una tabla de admisión. Por esto,

IntServ parece tener futuro principalmente en redes corporativas, donde desaparecen los problemas de escalabilidad y hay demanda de telefonía IP y videoconferencia en las intranets. Sin embargo, para Internet se hizo patente que se requería otra arquitectura que fuese más simple, escalable y que pudiera proveer un servicio mejor al de “mejor esfuerzo”, por lo que es allí donde surge la arquitectura de Servicios Diferenciados.

1.3.5.2 Arquitectura de Servicios Diferenciados (DiffServ)[15][29][30]

DiffServ surge como una alternativa a IntServ para satisfacer requisitos como proporcionar altas prestaciones, escalabilidad, permitir el crecimiento sostenido del tamaño de las redes y su ancho de banda, entre otros. Su filosofía se basa en situar el procesado complejo y la gestión de los recursos en los límites de la red, con un apropiado SLA que se asume está en su lugar en los bordes del dominio, al mismo tiempo que mantiene el reenvío de paquetes en el núcleo de la red de la manera más sencilla posible. En los nodos del núcleo de la red no se mantiene el estado de las conexiones, sino que el tratamiento se basa únicamente en un campo de los paquetes, que designan la clase de calidad que deben recibir.

Esta arquitectura definida en el RFC 2475 propone un tratamiento diferenciado en los nodos para un conjunto reducido de flujos o clases, de forma que todos los paquetes que pertenezcan a una misma clase recibirán un mismo tratamiento por parte de la red. Así, cuanto mayor sea la prioridad o el ancho de banda asignado a la clase, mejor trato recibirá. Los nodos del borde identifican a qué clase pertenece un paquete y se monitoriza si un flujo cumple con el SLA. Los nodos interiores retransmiten los paquetes sólo basados en la clase de los mismos.

La ventaja de DiffServ frente a otras arquitecturas consiste en la posibilidad de utilizar la actual infraestructura de red sin la necesidad de introducir grandes cambios, lo que posibilita un despliegue gradual. También hay que señalar que DiffServ tiene sus inconvenientes. En primer lugar no es capaz de garantizar de forma determinista una cierta calidad de servicio, garantizando sólo un mejor tratamiento a ciertos flujos por parte de la red. El otro problema es el fenómeno de *starvation*. Este fenómeno se produce cuando una clase de prioridad inferior es

servida a una velocidad muy inferior a sus necesidades debido a que siempre hay un pequeño tráfico de prioridad superior esperando ser servido.

1.3.5.2.1 Campo DiffServ[1][30][33]

Cada paquete IPv4 tenía en su cabecera un campo llamado ToS y en la versión 6, el campo equivalente es Clase de tráfico.

La primera tarea del grupo de DiffServ fue re-especificar este campo de 1 byte. El campo redefinido fue denominado como DS (DiffServ) para ambas versiones, formado por los subcampos *DiffServ CodePoint* (DSCP) de 6 bits que indica el tratamiento que debe recibir el paquete en los *routers* y *Currently Unused* (CU) de 2 bits, utilizado actualmente para control de congestión. El octeto DS con sus subcampos se indica en la figura 1.24.

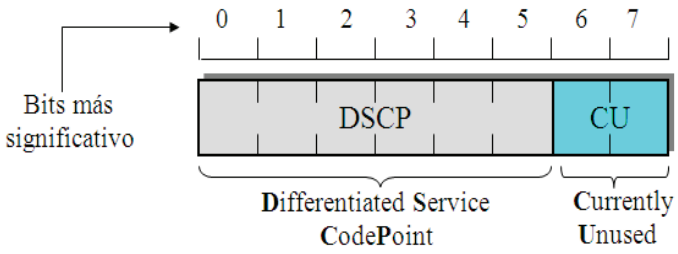

Figura 1.24 Campo DS de DiffServ[33]

El subcampo DSCP permite hasta 64 diferentes valores binarios que representan 64 categorías de tráfico diferentes, que hasta el momento se han dividido en tres grupos, como se indica en la tabla 1.1.

Categorías	Valores	Uso
xxxyy0	32	Estándar
xxxx11	16	Local/Experimental
xxxx01	16	Reservado

Tabla 1.1 Categorías del subcampo DSCP[1]

1.3.5.2.2 Per-Hop Behaviors (PHB)[6][29][30]

En DiffServ, el tratamiento de retransmisión de un paquete es llamado PHB, donde cada PHB es representado por uno de los 32 valores DSCP de uso estándar en la cabecera del paquete. Los paquetes que tienen el mismo DSCP, reciben el mismo trato en cada nodo y son conocidos como *Behavior Aggregate* (BA).

Cuando un paquete entra en un nodo, la lógica de ruteo selecciona su puerto de salida y el valor DSCP es usado para conducir el paquete a una cola específica o tratamiento específico en ese puerto. En otras palabras, un PHB se refiere a la planificación, el encolamiento y la política de un nodo con cualquier paquete dado perteneciente a un BA.

Los recursos se distribuyen a los PHBs, lo que da lugar a que un PHB se describa en términos absolutos o relativos, según los recursos se distribuyan con un mínimo garantizado en el primer caso o en forma proporcional en el segundo. Los PHBs se describen preferentemente como distribución de ancho de banda, prioridad de descarte, entre otros.

Existen cuatro estándares disponibles de PHBs que son:

- ***Default* PHB:** Definido en el RFC 2474, tiene un valor de DSCP igual a 000000 y el servicio esperado es exactamente igual al servicio de “mejor esfuerzo” tradicional. Además, si un paquete llega a un nodo y el valor DSCP no se mapea a algún otro PHB, el paquete será mapeado al *Default* PHB.
- ***Class-Selector* PHB:** Definido en el RFC 2474, tiene siete valores DSCP que funcionan desde el 001000 al 111000 y son especificados para seleccionar hasta siete comportamientos, cada uno de los cuales tiene una mayor probabilidad de envío a tiempo que su predecesor.
- ***Assured Forwarding* PHB (AF):** Definido en el RFC 2597 y “asegura” que el tráfico conforme al perfil contratado para un flujo sea entregado sin pérdidas con probabilidad muy alta; se permite exceder el perfil con la comprensión de que el tráfico en exceso no será entregado con una

probabilidad tan alta y se garantiza la secuencialidad dentro de cada flujo, independientemente de que los paquetes sean conformes o no. Este PHB permite ofrecer distintos niveles de "garantía de entrega" o de calidad relativa para paquetes IP. Para esto se definen N clases AF tal que a cada clase AF se le reservan recursos, de forma que los retardos y/o pérdidas de una clase sean siempre inferiores a los de una clase de menor prioridad. Dentro de cada clase, los paquetes se pueden clasificar a su vez en M categorías de preferencia de descarte. En caso de congestión, la preferencia de descarte determina la importancia relativa del paquete dentro de la clase. Actualmente N=4 y M=3 son definidos para uso general. En la tabla 1.2 se indica los valores DSCP que toman cada clase AF.

% de descarte	Clase 1	Clase 2	Clase 3	Clase 4
Bajo	AF11=001010	AF21=010010	AF31=011010	AF41=100010
Medio	AF12=001100	AF22=010100	AF32=011100	AF42=100100
Alto	AF13=001110	AF23=010110	AF33=011110	AF43=100110

Tabla 1.2 Valores DSCP correspondientes a AF[1]

- ***Expedited Forwarding* PHB (EF):** Definido en el RFC 2598, tiene un valor de DSCP igual a 101110 que permite ofrecer un servicio punta a punta de bajas pérdidas, baja latencia, bajo *jitter* y un ancho de banda asegurado. También recibe por ello el nombre de "Servicio Premium". EF aparece en los puntos finales como una "línea virtual alquilada", caracterizada por no ofrecer garantías cuantitativas y cuyo objetivo es que el flujo de tráfico vea siempre o casi siempre, la cola vacía. Aplicaciones como la VoIP, vídeo y programas online requieren este servicio robusto. Sin embargo, para una eficiencia óptima, EF debe ser reservado para únicamente las aplicaciones más críticas, puesto que en situaciones de congestión de tráfico, no es factible tratar todo o gran parte del tráfico con alta prioridad.

1.3.5.2.3 Componentes de DiffServ[29][33]

La arquitectura DiffServ está formada por varios componentes, como se indica en la figura 1.25.

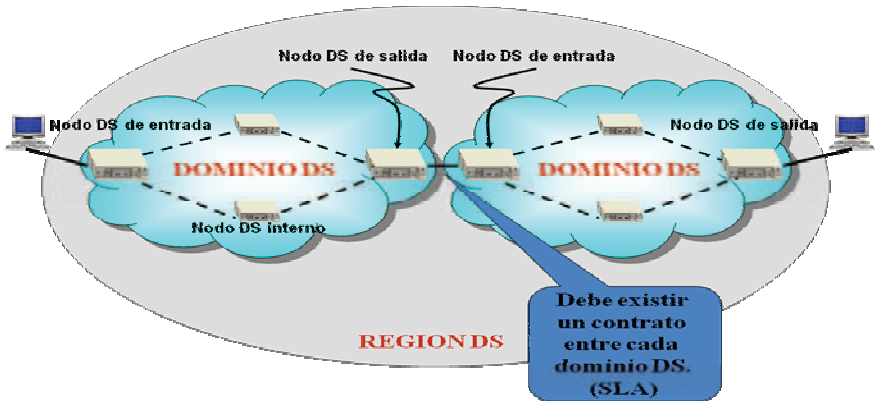

Figura 1.25 Componentes de la arquitectura DiffServ[33]

Dominio DS.- Un dominio DS es un conjunto de nodos que soportan DiffServ y operan con una política de provisionamiento de servicios común, con un conjunto de PHBs implementados en cada nodo.

Nodos DS externos.- Estos nodos interconectan el dominio DS con otros dominios que pueden o no soportar DiffServ. Los nodos externos clasifican y posiblemente condicionan el tráfico entrante para asegurarse que los paquetes que transitan el dominio estén apropiadamente marcados para seleccionar un PHB de los grupos PHBs que son soportados dentro del dominio. Pueden ser nodos DS de entrada o nodos DS de salida.

Nodos DS internos.- Estos nodos tienen limitadas funciones de acondicionamiento y se conectan a otros nodos internos o nodos externos dentro del mismo dominio DS. La selección de un PHB sólo se realiza analizando el subcampo DSCP.

Región DS.- Es un conjunto de uno o más dominios DS contiguos. Los dominios DS en una región DS pueden soportar distintos grupos PHBs internamente. Sin embargo, para permitir servicios que se expandan a través de los dominios, los dominios DS contiguos deben cada uno establecer un SLA entre ellos para

especificar cómo el tránsito del tráfico de un dominio DS a otro es condicionado en la frontera entre los dos dominios DS.

1.3.5.2.4 Funciones de DiffServ[6][29][30]

Los nodos DS externos son los responsables de mapear los paquetes entrantes en alguna de las clases de retransmisión soportadas por la red y de asegurarse que cumplan el SLA. La primera función se conoce como clasificación de tráfico y la segunda como acondicionamiento de tráfico.

El módulo de clasificación de tráfico contiene un clasificador y un marcador de paquetes. El paquete saliente de este módulo se entrega al módulo de acondicionamiento.

- **Clasificador:** El clasificador divide el tráfico entrante en varios grupos basado en un descriptor de tráfico. Existen dos tipos de clasificadores que son *Behavior Aggregate* (BA) y *Multi-field* (MF). El clasificador BA identifica paquetes basado sólo en los valores DSCP de los mismos; se usa cuando los paquetes han sido marcados antes del ingreso a la red del proveedor, por ejemplo en el *host* del cliente, el primer *router* o por la red de otro proveedor. El clasificador MF selecciona paquetes basado en el valor de una combinación de uno o más campos de la cabecera como dirección origen, dirección destino, campo DS, protocolo, puertos origen o destino, entre otros; además, el clasificador debe autentificar la información que usa para clasificar el paquete.
- **Marcador:** Está relacionado con la clasificación de paquetes. Permite marcar un paquete basado en la clasificación realizada. Este marcador se puede usar para asociar el paquete con un grupo local de QoS.

En los nodos DS externos se tiene el perfil del tráfico para cada clase y para cada cliente. Los perfiles de tráfico especifican las propiedades temporales de una corriente de tráfico seleccionada por el clasificador. Éstos proveen de reglas para determinar si un paquete está dentro o fuera del perfil.

El módulo de acondicionamiento mide el flujo de tráfico y lo compara con el perfil del cliente, luego decide de acuerdo a una regla predefinida si el paquete se considera como dentro del perfil o fuera de éste. Si el paquete está adentro, se envía a la red; si no lo está, se toma alguna acción predefinida, como remarcar el paquete, descartarlo o almacenarlo temporalmente. Con esto, los nodos externos no sólo mapean los paquetes en una clase, sino que también aseguran el cumplimiento del SLA y previenen la congestión. Este módulo está compuesto por medidor, marcador, conformador y despachador. Cuando los paquetes salen del acondicionador de tráfico de un nodo DS externo, el campo DS de cada paquete debe setearse a un valor apropiado.

- **Medidor:** Mide las propiedades temporales de la corriente de paquetes seleccionada por el clasificador en base a un perfil de tráfico. Pasa información de estado a otras funciones de condicionamiento para tomar cierta acción para cada paquete tanto dentro como fuera del perfil.
- **Marcador:** Setea el campo DS con un código particular, agregando el paquete marcado a un BA particular. Se puede marcar todos los paquetes que son dirigidos a él con un código particular o puede estar configurado para marcar un paquete a un código de un grupo de códigos usados para seleccionar un PHB en un grupo PHB. Cuando el marcador cambia el código en un paquete, se dice haber “remarcado” el paquete.
- **Conformador:** Retarda uno o todos los paquetes de una corriente de tráfico de manera de que la corriente cumpla con el perfil de tráfico estipulado. Usualmente tiene un *buffer* de tamaño finito y los paquetes pueden ser descartados sino hay suficiente espacio de *buffer* para almacenar a los paquetes retrasados.
- **Despachador:** Descarta algunos o todos los paquetes en una corriente de tráfico de manera de que la corriente cumpla con el perfil de tráfico estipulado. Este proceso es conocido como “política”. Un despachador puede ser implementado como un caso especial de un conformador, si se pone el tamaño del *buffer* del conformador igual a cero o a muy pocos paquetes.

La figura 1.26 indica las funciones de la arquitectura DiffServ que se realizan sobre el tráfico entrante a los nodos DS.

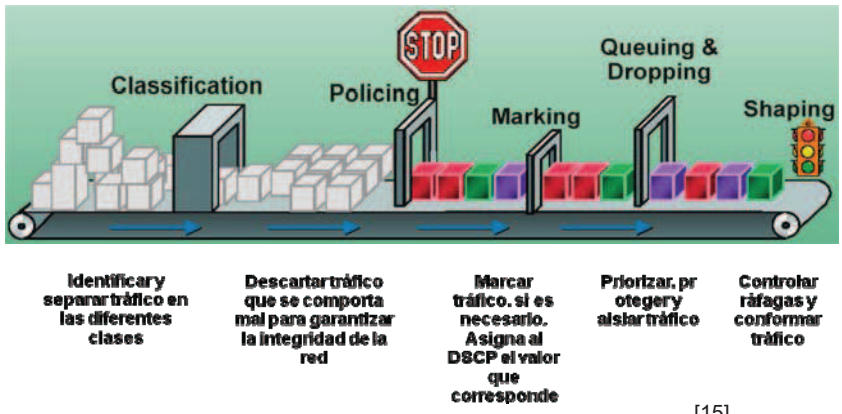

Figura 1.26 Funciones de la arquitectura DiffServ[15]

1.3.5.2.5 Localización de las funciones de DiffServ[6]

Tanto los clasificadores como los acondicionadores de tráfico usualmente están ubicados en los nodos DS de entrada y de salida de tráfico entre dominios. Sin embargo, pueden estar en otros lugares.

- **Dentro de un dominio origen:** Definido como el dominio que contiene el nodo que origina el tráfico que recibe un servicio particular. El marcado y acondicionamiento de tráfico puede ser realizado por el *host* origen o por algún nodo intermedio antes que deje el dominio origen. Esto se conoce como pre-marcado. El pre-marcado permite clasificar el tráfico basándose en políticas locales al cliente. También simplifica el proceso de clasificación, pues mientras más cerca se está del origen, el tráfico está menos mezclado y las reglas pueden ser mucho más sencillas.
- **En el borde de un dominio DS:** Entre dos dominios DS, el mapeo del valor de DSCP a un PHB puede ser distinto, por lo que se hace necesario remarcar los paquetes en el borde de los dominios. El SLA especifica cuál dominio realiza el marcado del DSCP correspondiente. Sin embargo, el nodo de entrada debe acondicionar el tráfico. Si el dominio que envía los paquetes no tiene capacidad de DiffServ, el nodo de ingreso del receptor debe realizar la clasificación.

- **En el interior de nodos DS:** Se pueden encontrar excepcionalmente en puntos de gran congestión y no se debe afectar a otros servicios.

1.3.6 PROCEDIMIENTOS DE QoS[1][2][6][31][32]

Existen varios procedimientos con los cuales se puede proveer de calidad de servicio a una red. Algunos de ellos son el de contar con una estrategia de manejo de los paquetes en caso de congestión o evitar que la red alcance este estado, descartando paquetes a medida que éstos ingresan a la red. Estos procedimientos son denominados control de congestión y evasión de congestión.

1.3.6.1 Control de congestión

La congestión en un interfaz de salida se produce cuando no puede enviar paquetes al medio físico tan rápidamente como le llegan, procedentes de las interfaces de entrada de los *routers*.

El término “control de congestión” se usa para nombrar los distintos tipos de estrategias de encolamiento que se utilizan para manejar situaciones donde la demanda de ancho de banda solicitada por las aplicaciones excede el ancho de banda total de la red. Las características de control de congestión permiten controlar la congestión determinando el orden en el que los paquetes son enviados a través de una interfaz, basándose en prioridades asignadas a los paquetes. El control de congestión involucra la creación de colas, asignación de paquetes a dichas colas basándose en la clasificación del paquete y la planificación de los paquetes en la cola para su transmisión.

El procedimiento de control de congestión con calidad de servicio está constituido por cinco tipos de encolamiento:

- *First-In, First-Out* (FIFO)
- *Weighted Fair Queueing* (WFQ): Este tipo de encolamiento define tres tipos que son WFQ basado en flujos (WFQ), WFQ VIP Distribuido (DWFQ) y WFQ basado en clases (CBWFQ)
- *Custom Queueing* (CQ)

- *Priority Queueing* (PQ)
- *Low Latency Queueing* (LLQ)

1.3.6.1.1 First-In, First-Out (FIFO)

Es el tipo más simple de encolamiento, se basa en el concepto de que el primer paquete en entrar a la interfaz es el primero en salir, como se indica en la figura 1.27. La ventaja clave de FIFO es que requiere la menor cantidad de recursos del *router*. Sin embargo, su naturaleza simplista es también su desventaja principal, ya que como los paquetes salen por la interfaz en su orden de llegada, no es posible asignar prioridades al tráfico, ni evitar que una aplicación o usuario utilicen en exceso el ancho de banda disponible.

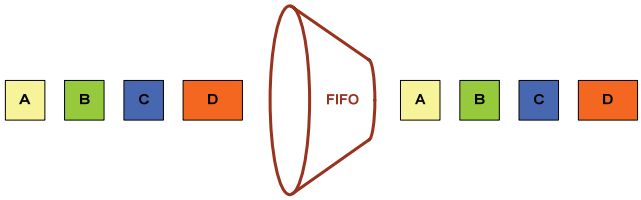

Figura 1.27 Tipo de encolamiento FIFO[2]

FIFO es adecuado para interfaces de alta velocidad, pero no para las de baja velocidad, ya que es capaz de manejar cantidades limitadas de ráfagas de datos; si llegan más paquetes cuando la cola está llena, éstos son descartados.

1.3.6.1.2 WFQ basado en flujos (WFQ)

En situaciones en las que se desea proveer un tiempo de respuesta razonable a todos los usuarios de la red sin agregar demasiado ancho de banda, la solución es WFQ. WFQ es un algoritmo de encolamiento basado en flujos, que realiza dos cosas simultáneamente, programar el tráfico interactivo al frente de la cola para reducir el tiempo de respuesta y compartir equitativamente el ancho de banda remanente entre flujos de gran ancho de banda.

WFQ asegura que las colas no mueran de inanición por falta de ancho de banda y que el tráfico tenga un servicio predecible. Los flujos de tráfico de bajo volumen reciben un servicio preferencial, transmitiendo toda su carga en el momento

oportuno. Los flujos de tráfico de alto volumen comparten entre ellos la capacidad remanente proporcionalmente.

WFQ está diseñado para minimizar los esfuerzos de configuración y adaptarse automáticamente a las condiciones de cambio del tráfico en las redes. De hecho, WFQ realiza un buen trabajo en la mayoría de las aplicaciones que han sido implementadas con el modo de encolamiento por defecto en interfaces seriales configuradas para correr a velocidades de 2048 Kbps o menores. En la figura 1.28 se muestra gráficamente el esquema utilizado por WFQ.

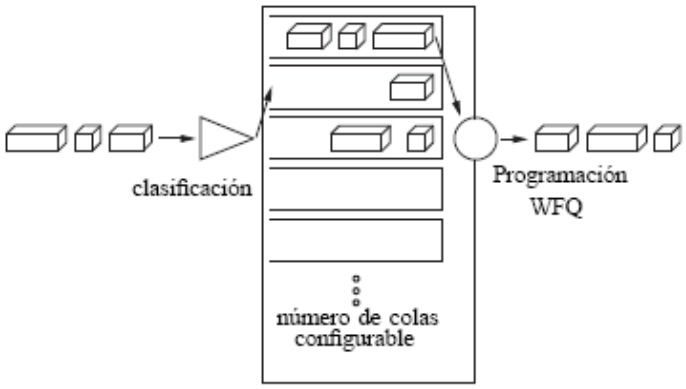

Figura 1.28 Esquema gráfico del encolamiento WFQ[6]

1.3.6.1.3 WFQ basado en clases (CBWFQ)

WFQ tiene algunas limitaciones de escalamiento, ya que la implementación del algoritmo se ve afectada a medida que el tráfico por enlace aumenta y colapsa debido a la cantidad numerosa de flujos que se debe analizar. CBWFQ fue desarrollado para evitar estas limitaciones, permitiendo la creación de clases definidas por el usuario, que permiten un mayor control sobre las colas de tráfico y asignación del ancho de banda.

Cada clase posee una cola separada y todos los paquetes que cumplen el criterio definido para una clase en particular son asignados a dicha cola. Una vez que se establecen los criterios para las clases, es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados. Si una clase no utiliza su porción de ancho de banda, otras pueden hacerlo. Se pueden configurar específicamente el ancho de banda o la profundidad de la cola para cada clase. El peso asignado

a la cola de la clase es determinado mediante el ancho de banda asignado a dicha clase. En la figura 1.29 se muestra gráficamente el esquema utilizado por CBWFQ.

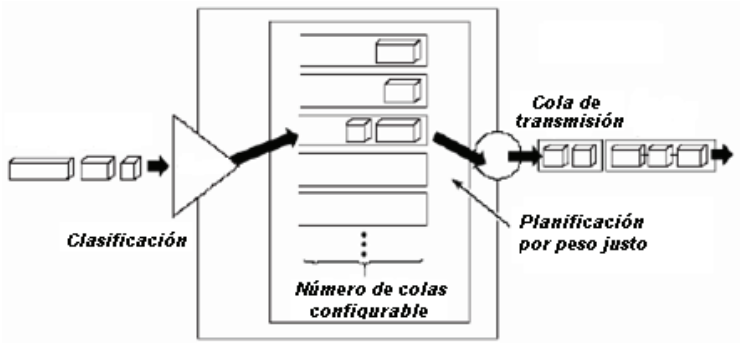

Figura 1.29 Esquema gráfico del encolamiento CBWFQ[6]

1.3.6.1.4 Custom Queueing (CQ)

En CQ, el ancho de banda es asignado proporcionalmente para cada clase de tráfico diferente. CQ permite especificar el número de bytes o paquetes que serán sacados de la cola, lo que es útil especialmente en interfaces lentas. Se pueden crear hasta 16 colas para categorizar el tráfico, donde cada cola es atendida al estilo *round-robin*. Se utiliza CQ para proveer a tráficos particulares de un ancho de banda garantizado en un punto de posible congestión, asegurando para este tráfico una porción fija del ancho de banda y permitiendo al resto del tráfico utilizar los recursos disponibles. La gestión de colas CQ permite especificar qué porcentaje de ancho de banda se dedica a cada tipo de tráfico. En la figura 1.30 se muestra gráficamente el esquema utilizado por CQ.

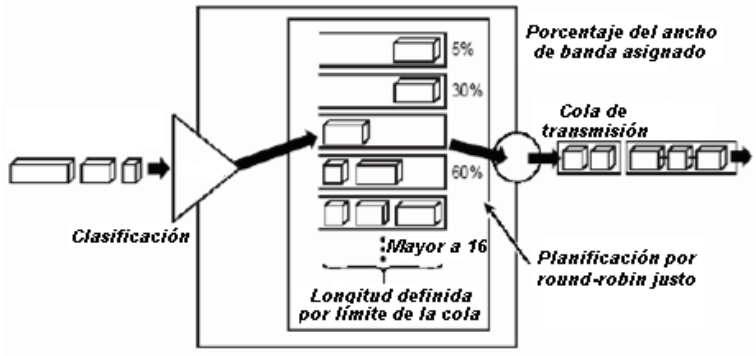

Figura 1.30 Esquema gráfico del encolamiento CQ[6]

1.3.6.1.5 Priority Queueing (PQ)

PQ consiste en un conjunto de cuatro colas, clasificadas desde alta hasta baja prioridad. Cada paquete es asignado a una de estas colas, las cuales son servidas en estricto orden de prioridad. Las colas de mayor prioridad son siempre atendidas primero, luego la siguiente de menor prioridad y así. Si una cola de menor prioridad está siendo atendida, y un paquete ingresa a una cola de mayor prioridad, ésta es atendida inmediatamente. PQ se ajusta a condiciones donde existe un tráfico importante, pero puede causar el fenómeno de *starvation*. En la figura 1.31 se muestra gráficamente el esquema usado por PQ.

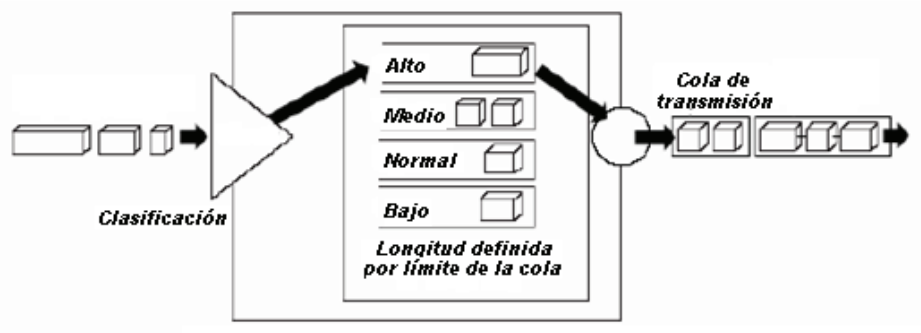

Figura 1.31 Esquema gráfico del encolamiento PQ[6]

1.3.6.1.6 Low Latency Queueing (LLQ)

LLQ es una mezcla entre los métodos PQ y CBWFQ y es actualmente el método de encolamiento recomendado para VoIP y telefonía IP, por lo que también trabajará apropiadamente con tráfico de videoconferencia. LLQ consta de colas de prioridad personalizadas, basadas en clases de tráfico, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas. Si existe tráfico en la cola de prioridad, ésta es atendida antes que las otras colas de prioridad personalizadas. Si la cola de prioridad no está encolando paquetes, se procede a atender las otras colas según su prioridad. Debido a este comportamiento es necesario configurar un ancho de banda límite reservado para la cola de prioridad, evitando la inanición del resto de las colas.

1.3.6.2 Evasión de congestión

Las técnicas de evasión de congestión monitorean la carga de tráfico en la red en un esfuerzo por anticipar y evitar la congestión en los "cuellos de botella" comunes. La evasión de congestión se logra mediante el descarte de paquetes.

Los mecanismos de evasión de congestión se basan en la manera que los protocolos operan, con el fin de no llegar a la congestión de la red. Entre los mecanismos de evasión de congestión más usados está *Random Early Detection* (RED) y *Weighted Random Early Detection* (WRED), los cuales son útiles para redes con tráfico de alta velocidad. Si no se configura ninguno de los dos, el *router* usa el mecanismo de descarte de paquetes por defecto llamado *tail drop*.

1.3.6.2.1 Tail drop

Tail drop trata todo el tráfico de igual forma y no hace diferencias entre clases de servicio. En una situación de congestión las colas se llenan; cuando la cola de salida está llena y este mecanismo entra en acción, los paquetes que llegan son descartados hasta que la congestión es eliminada y la cola no está muy llena.

1.3.6.2.2 Random Early Detection (RED)

Con este mecanismo, la eliminación de paquetes en la cola se realiza de forma aleatoria y antes de que se produzca la congestión del interfaz. De esta forma se fuerza a que conexiones TCP aleatorias reduzcan su tasa de envío de datos, evitando que la congestión se produzca.

1.3.6.2.3 Weighted Random Early Detection (WRED)

WRED es la implementación del mecanismo para evitar la congestión conocido como RED. WRED evita la congestión asegurándose que la cola no se llene, calculando constantemente la longitud media de la cola y comparándola con dos umbrales o límites. Si el tamaño de la cola se encuentra por debajo del umbral mínimo no se descarta ningún paquete, si es mayor que el máximo entonces todos los paquetes nuevos que lleguen serán descartados y si el tamaño se

encuentra entre los dos umbrales, entonces los paquetes se descartan de acuerdo a un cálculo de probabilidad obtenido del tamaño mínimo de la cola; es decir, a medida que el tamaño medio de la cola se va acercando al umbral máximo, se va descartando un número cada vez mayor de paquetes. La probabilidad de descarte de paquetes será mayor en conexiones que utilicen un mayor ancho de banda.

WRED es útil porque evita un problema conocido como sincronización global, que se refiere a una pérdida total del flujo de tráfico en la red, producida por el descarte de paquetes desde varias conexiones al mismo tiempo. Si un dispositivo que maneja varias conexiones dentro de la red comienza a descartar paquetes de forma sistemática, el flujo total de tráfico en la red caerá de forma significativa. Esta situación es indeseable puesto que provoca que todas las líneas reduzcan sus tasas de transmisión y que no se pueda utilizar toda la capacidad de la red. WRED evita esta situación escogiendo aleatoriamente las conexiones a las cuales descarta paquetes, en lugar de realizar un descarte sistemático en todas las conexiones. La figura 1.32 muestra gráficamente el esquema utilizado por WRED.

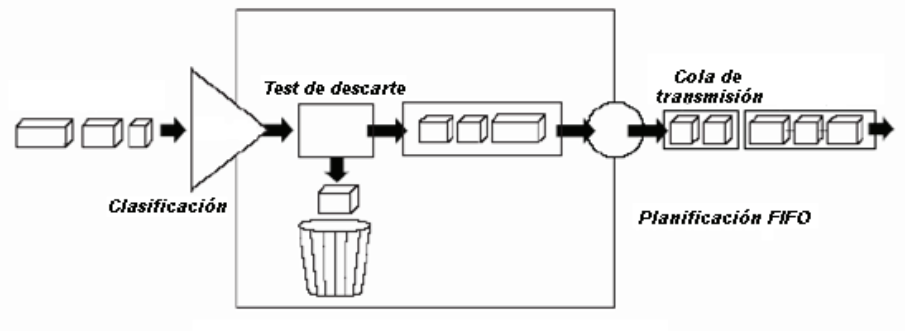

Figura 1.32 Esquema gráfico del mecanismo WRED[6]

REFERENCIAS CAPÍTULO 1

LIBROS Y MANUALES

[1] SACKETT, George. Manual de routers Cisco. 1era edición. Mc Graw Hill. Madrid. 2002

[2] KEAGY, Scott. Integración de redes de voz y datos. 2da edición. Pearson Educación S.A. Madrid. 2001

[3] HIDALGO, Pablo. Folleto de redes de área extendida. EPN. Marzo 2007

PROYECTOS DE TITULACIÓN

[4] PADILLA, René; URQUIZA, Luis. “Rediseño de la red WAN de Petrocomercial con calidad de servicio”. EPN. Enero 2008

[5] CHÁVEZ, Diego; MONTERO, Silvana. “Diseño para la migración de la red de SETEL hacia un carrier que utiliza tecnología MPLS, para proveer servicios de VoIP en todo el Distrito Metropolitano de Quito”. EPN. Marzo 2008

[6] DÍAZ, Carlos. “Reingeniería de la red de campus de la Escuela Politécnica Nacional considerando los criterios de calidad de servicio”. EPN. Marzo 2005

ARTÍCULOS E INTERNET

[7] ROSEN, E. “Multiprotocol Label Switching Architecture”. IETF RFC 3031. 2001

[8] SIENRA, Luis Gabriel. “Ofreciendo Calidad de Servicio mediante MPLS: Fundamentos y aplicación a las redes de cable”.
http://www.cinit.org.mx/articulo.php?idArticulo=14

[9] GARCIA, Jorge. “Arquitectura de Multi Protocol Label Switching (MPLS)”
http://panoramix.fi.upm.es/~jgarcia/Curso_MPLS/capitulo4.html

[10] GARCIA, Jorge. “Protocolos de distribución de etiquetas”
http://panoramix.fi.upm.es/~jgarcia/Curso_MPLS/capitulo5.html

[11] ANÓNIMO. “MPLS”
http://es.wikipedia.org/wiki/MPLS

[12] ANGULO, Jenny; HERNANDEZ, Jorge; MORENO, Deibis. “MPLS”
http://www.monografias.com/trabajos/informacion-mpls/informacion mpls.shtmly

[13] DREILINGER, Tímea. “DiffServ and MPLS”
http://saturn.acad.bg/bis/pdfs/04_doklad.pdf

[14] IPINFUSION. “Quality of service and MPLS methodologies”
http://www.ipinfusion.com/pdf/IP_InfusionQoS_MPLS2.pdf

[15] ANÓNIMO. “QoS”
http://www2.ing.puc.cl/~iee3542/amplif_4.ppt

[16] ANÓNIMO. “Arpanet”
http://es.wikipedia.org/wiki/arpanet

[17] ANÓNIMO. “El modelo TCP/IP”
http://neo.lcc.uma.es/evirtual/cdd/tutorial/modelos/Mtcp.html

[18] ANÓNIMO. “Familia de protocolos de internet”
http://es.wikipedia.org/wiki/TCP/IP

[19] CHÁVEZ, Julio. “Protocolos de red: protocolo TCP/IP”
http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

[20] ANÓNIMO. “Protocolo de internet”
http://es.wikipedia.org/wiki/Protocolo_de_Internet

[21] NORTON, Juan. “El protocolo IP"
http://www.monografias.com/trabajos7/protoip/protoip.shtml

[22] ANÓNIMO. “IPv6”
http://es.wikipedia.org/wiki/IPv6

[23] KIOSKEA, “Protocolo TCP”
http://es.kioskea.net/contents/internet/tcp.php3

[24] ANÓNIMO. “Transmission Control Protocol”
http://es.wikipedia.org/wiki/TCP

[25] KIOSKEA. “Protocolo UDP”
http://es.kioskea.net/contents/internet/udp.php3

[26] ANÓNIMO. “User Datagram Protocol”
http://es.wikipedia.org/wiki/User_Datagram_Protocol

[27] ANÓNIMO. “Protocolo de reserva de recursos”
http://es.wikipedia.org/wiki/Protocolo_de_reserva_de_recursos

[28] IBARRA, Edwin. “MPLS (MultiProtocol Label Switching) y Calidad de Servicio en las redes IP”
http://www.tecnologicoamper.com/descargas/seminario01CC.pdf

[29] ANÓNIMO. “Calidad de servicio: Servicios Diferenciados” http://www.info-ab.uclm.es/asignaturas/42650/PDFs/practica5.pdf

[30] DELFINO, Adrián; RIVERO, Sebastián. “Diffserv: Servicios Diferenciados” http://iie.fing.edu.uy/ense/asign/perfredes/trabajos/diffserv/Trabao%20Final.pdf

[31] ÁLVAREZ, Sebastián; GONZÁLEZ, Agustín. “Estudio y configuración de calidad de servicio para protocolos IPv4 e IPv6 en una red de fibra óptica WDM” http://www.scielo.cl/pdf/rfacing/v13n3/art15.pdf

[32] DENZER, Patricio. “Administración de ancho de banda utilizando un router Cisco 3600” http://profesores.el.utfsm.cl/2006/senacitel/DenzerLopezGonzalezSubmitted.pdf

[33] DÍAZ, Daniel. “Nuevas soluciones en la internet: IntServ, DiffServ y MPLS” http://www.redes.unb.br/Topicos_Redes_Comunicacao/IntServ_DiffServ.pdf

CAPÍTULO 2

ANÁLISIS DE TRÁFICO EN UN PROVEEDOR DE SERVICIOS DE INTERNET (ISP)

2.1 INTRODUCCIÓN

La búsqueda de información y de servicios conlleva a que el uso de la red Internet se convierta en una necesidad antes que en un lujo, siendo la tasa de crecimiento del tráfico de Internet en torno al 100% anual[1]. Esta necesidad creciente de conectividad con Internet está imponiendo fuertes exigencias a las empresas dedicadas a ofrecer este servicio, denominadas como Proveedores de Servicios de Internet (ISPs).

El principal objetivo de un ISP es proporcionar a los usuarios el acceso a Internet a través de diferentes medios, que inicialmente eran el uso de ordenadores personales dotados de módems, utilizando como medio de transmisión las líneas de cobre usadas por la telefonía. Sin embargo, la creciente demanda de aplicaciones con capacidades superiores y la invención de nuevas y mejores tecnologías exigieron una diversificación de los modos de acceso a Internet, debido principalmente a la velocidad de conexión para aprovechar todos los recursos que ofrecía Internet.

Además, los diferentes agregados de tráfico que manejan los clientes individuales y corporativos, tienen diversos requerimientos de recursos que la red del proveedor debe proporcionar para cumplir con los parámetros comprometidos dentro de los Acuerdos de Nivel de Servicio (SLAs) contratados con los clientes.

Al realizar un análisis del tráfico que cursa por la red de un proveedor, se puede determinar los requerimientos tanto del tráfico generado por los clientes como del tráfico usado para la administración de la red; esto permitirá aprovechar de manera eficiente la capacidad existente y los servicios que ofrece Internet,

[1] De acuerdo a declaraciones de John Chambers, *Chief Executive Officer* (CEO) de Cisco, acerca de la estimación del crecimiento del tráfico de Internet en los próximos años.

detectando a tiempo posibles “cuellos de botella” y evitando periodos de congestión, que consumen recursos y disminuyen la eficiencia de la misma.

2.2 PROVEEDOR DE SERVICIOS DE INTERNET (ISP)

2.2.1 CONCEPTO DE UN ISP[6][9]

Un ISP es una empresa dedicada a comercializar el servicio de conexión a Internet a usuarios o a las distintas redes que tengan mediante las líneas telefónicas o cualquier otra red de acceso disponible, así como dar mantenimiento necesario para el adecuado funcionamiento de dicho servicio. Además, ofrecen servicios relacionados como alojamiento web, registro de dominios, entre otros.

2.2.2 TIPOS DE ISPs

Los ISPs han sido clasificados de acuerdo a varios criterios, pero principalmente por su cobertura geográfica y su nivel de conectividad con las principales conexiones troncales de Internet (*backbone*).

2.2.2.1 ISPs según su cobertura geográfica[7]

Los ISPs cubren una determinada área geográfica dependiendo de las características de su infraestructura, por ello se tiene tres tipos de ISPs:

ISPs locales.- Son proveedores pequeños cuya cobertura se limita al área de una ciudad o gran parte de la misma. Generalmente poseen una oficina central encargada de la administración y pocas oficinas locales dependiendo de su número de usuarios, constituyendo puntos de presencia de los ISPs de mayor cobertura, ya que para acceder a Internet deben conectarse a alguno de ellos.

ISPs regionales.- Estos ISPs cubren una determinada región, por lo que su estructura es más compleja y robusta que la de un ISP local. Pueden poseer varias oficinas centrales, regionales y locales, conectarse a un ISP nacional, internacional o tener acceso directo al *backbone* de Internet. Las oficinas centrales están adecuadamente distribuidas e interconectadas entre sí y poseen

equipos de redundancia para aumentar la disponibilidad del servicio. Las oficinas locales proveen la conexión a los clientes y enrutan el tráfico hacia las oficinas regionales.

ISPs nacionales o internacionales.- Son proveedores que cubren el área de un país, en el caso de los ISPs nacionales y el área de varios países, en el caso de los ISPs internacionales. Cuentan con su propia infraestructura y generalmente están conectados directamente al *backbone* principal de Internet. Entre sus clientes se pueden encontrar a grandes corporaciones y proveedores de tamaño menor, aunque también pueden ofrecer servicios de interconexión. Son empresas de gran importancia y se los puede clasificar de la siguiente manera:

- **ISPs integrados:** Aparecen cuando los ISPs regionales crecen llegando a ser redes de gran velocidad que conectan varias oficinas centrales.
- **ISPs de acceso *outsourced*:** Este tipo de ISP utiliza un grupo de proveedores locales alquilados para dar acceso local a clientes; de esta forma reducen sus costos, dan un mejor servicio y pueden extenderse hacia nuevas áreas.
- **ISPs multimodo:** Son empresas telefónicas que entregan mayor cantidad de servicios por medio de su propia infraestructura logrando gran cobertura.

2.2.2.2 ISPs según su nivel de conectividad con el *backbone* de Internet[2][10]

Los ISPs son designados de acuerdo a una jerarquía basada en su nivel de conectividad con el *backbone* de Internet. Cada nivel inferior obtiene conectividad al *backbone* a través de una conexión con un nivel más alto, por lo que se tienen los siguientes tres niveles de ISPs:

ISPs de nivel 1.- En el extremo más alto de la jerarquía se encuentran los ISPs de nivel 1. Estos ISPs conocidos como troncales Internet tienen cobertura internacional o nacional y están directamente conectados con el *backbone* de Internet. Los usuarios de estos ISPs son nueve compañías que son AOL, AT&T, Global Crossing, Level3, Verizon Business, NTT Communications, Qwest, SAVIS y SprintLink. Sus ventajas principales son la confiabilidad y velocidad. Además,

debido a que los usuarios tienen una sola conexión a Internet, son pocas las posibilidades de fallas o “cuellos de botella”.

ISPs de nivel 2.- Un ISP de nivel 2 normalmente tiene una cobertura regional o nacional y se conecta a Internet a través de los ISPs de nivel 1. Estos ISPs generalmente se enfocan en negocios y ofrecen más servicios que los ISPs de nivel 1 y nivel 3 como DNS, servidores de correo electrónico, servidores web, comercio electrónico, comercio empresarial y VoIP. La principal desventaja de este nivel comparado con el nivel 1 es que el acceso a Internet es más lento debido a que tiene más de una conexión al *backbone* de Internet, lo que conlleva a una menor confiabilidad.

ISPs de nivel 3.- Por debajo de los ISPs de nivel 2 están los ISPs de nivel más bajo o nivel 3, que se conectan a través de uno o más ISPs de nivel 2. Estos ISPs se concentran en el comercio minorista y mercados de un área específica. Su necesidad principal es la conectividad y soporte. Los ISPs de nivel 3 ofrecen servicio de conexión a Internet como parte de una red y de contratos de servicios de computadoras a sus usuarios. Poseen un reducido ancho de banda y menor confiabilidad que los ISPs de nivel 1 y nivel 2, aunque son una buena elección para pequeñas y medianas empresas.

2.2.3 MODELO JERÁRQUICO DE TRES CAPAS[11]

En la actualidad, muchos ISPs han optado por diseñar sus redes en base al modelo jerárquico de tres capas, gracias a las características de escalabilidad, redundancia, rendimiento, seguridad, administración y mantenimiento que ofrece.

Este modelo divide la red en tres capas, donde cada una de ellas posee funciones específicas que definen su rol dentro de toda la red. Las tres capas del modelo jerárquico son:

- Capa *core*
- Capa distribución
- Capa acceso

2.2.3.1 Capa *core*

La capa *core* es el núcleo de la red, su única función es conmutar y llevar grandes cantidades de tráfico tan rápido como sea posible de manera confiable y veloz, por lo que la latencia y la velocidad son factores importantes. El tráfico que transporta es común a la mayoría de los usuarios, por lo que en caso de falla todos se ven afectados, haciendo que la tolerancia a fallas sea importante.

2.2.3.2 Capa distribución

Esta capa es el medio de comunicación entre la capa *core* y la capa acceso. Se encarga de proporcionar una conectividad basada en una determinada política, dado que determina cuándo y cómo los paquetes pueden acceder a los servicios principales de la red, así como de establecer la manera más rápida de responder a los requerimientos de la red.

La capa distribución permite implementar políticas de red como ruteo, filtrado de paquetes, colas de espera, seguridad y políticas de red, redistribución entre protocolos de ruteo, enrutamiento entre VLANs, entre otras.

2.2.3.3 Capa acceso

La capa acceso se encuentra en el borde de la red del proveedor y es el punto a través del cual los usuarios finales pueden ingresar a la red. En esta capa se pueden encontrar múltiples grupos de usuarios con sus correspondientes recursos y entre sus funciones está el enrutamiento, control de acceso, políticas de control de tráfico y QoS, entre otras.

Esta capa ofrece acceso remoto a la red del proveedor a través de tecnologías de área extendida o líneas alquiladas.

2.2.4 MEDIOS DE TRANSMISIÓN PARA ACCEDER A INTERNET[1][6]

Se tienen cuatro medios de transmisión utilizados para que el cliente pueda acceder a la red del proveedor y son los siguientes:

- Par trenzado
- Cable coaxial
- Fibra óptica
- Radio

2.2.4.1 Acceso mediante par trenzado

El acceso por par trenzado es el más económico, más antiguo y más ampliamente utilizado. Este medio cuenta con una amplia red desplegada sobre pares de cobre trenzados donde su principal propósito era la telefonía pública. La forma trenzada del cable disminuye la interferencia electromagnética entre pares adyacentes de un cable. La figura 2.1 muestra el interior de un cable de par trenzado.

Figura 2.1 Cable de par trenzado[12]

2.2.4.2 Acceso mediante cable coaxial

El cable coaxial fue utilizado para la red troncal de telecomunicaciones, pero con el tiempo ha sido reemplazado por la fibra óptica. Este medio de transmisión es más caro y menos flexible que el par trenzado, aunque la tecnología es sumamente conocida, pues se ha usado por muchos años en varios tipos de comunicaciones. La figura 2.2 muestra el interior de un cable coaxial.

Figura 2.2 Cable coaxial[13]

2.2.4.3 Acceso mediante fibra óptica

La fibra óptica es el medio de transmisión que permite un mayor ancho de banda y la inmunidad a interferencias electromagnéticas como principales ventajas. Este medio es ideal para enlaces de alta velocidad, compitiendo sólo con los radioenlaces de alta capacidad en aquellos puntos en donde se requiere un acceso rápido y económico. La figura 2.3 muestra el interior de una fibra óptica.

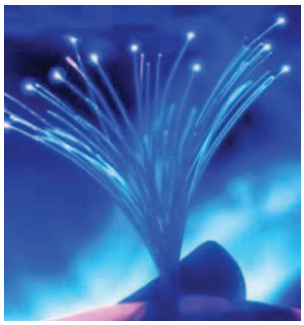

Figura 2.3 Fibra óptica[14]

Este medio está constituido por un núcleo de plástico o vidrio sobre el que se monta una cubierta de plástico o vidrio y se la cubre con una chaqueta protectora. La información se transmite mediante pulsos de luz en lugar de señales eléctricas, como ocurre con el par trenzado y el cable coaxial.

A pesar de sus grandes ventajas, presenta dificultades como los altos costos de instalación, los equipos que utiliza, la necesidad del uso de transductores óptico/eléctrico y las licencias de obra.

Se tienen dos tipos de fibra óptica:

- **Multimodo:** Múltiples rayos son transmitidos al interior de la fibra, donde cada rayo tiene diferente modo de propagación. El diámetro del núcleo de una fibra multimodo es mayor y presenta peores condiciones de transmisión que la fibra óptica monomodo.
- **Monomodo:** Fibra en la cual el diámetro del núcleo se reduce significativamente, a tal punto que actúa como una guía de onda y un solo rayo de luz se propaga en línea recta en el interior de la fibra. Tiene mejores características de transmisión que la fibra multimodo, son costosas pero pueden utilizarse para mayores distancias.

2.2.4.4 Acceso mediante radio

Las tecnologías inalámbricas mediante radio fueron utilizadas a mediados de los años 90 y entre sus principales ventajas están su fácil generación, posibilidad de viajar grandes distancias, penetración fácil en los edificios y menor costo que las basadas en un soporte físico. Sin embargo, su capacidad es reducida por cada cliente debido al limitado espectro electromagnético. La figura 2.4 muestra cómo acceden los clientes al ISP mediante los enlaces de radio.

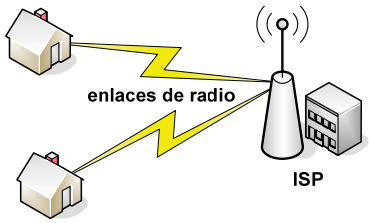

Figura 2.4 Acceso mediante enlaces de radio

2.2.5 FORMAS DE ACCESO A LA RED DEL PROVEEDOR

Los clientes acceden a los servicios de los ISPs mediante una red de acceso, que es el conjunto de tecnologías clasificadas según el soporte físico utilizado. Entre las tecnologías más utilizadas por los proveedores se tiene:

- Acceso conmutado o *dial-up*
- Acceso *Digital Subscriber Line* (DSL)
- Acceso por cable
- Acceso *clear channel*
- Acceso satelital
- Acceso *hot spots*
- Acceso *Broadband over Power Lines* (BPL)

2.2.5.1 Acceso conmutado o *dial-up*[2][15]

Una conexión *dial-up* es una forma económica pero lenta de acceso a Internet. Esta conexión se realiza mediante un módem interno o externo que se conecta a la *Public Switched Telephone Number* (PSTN) cuando el cliente lo requiera. La computadora accede a través de un número telefónico que provee el ISP y el

módem convierte la señal analógica en señal digital para recibir datos, mientras que el proceso inverso permite enviarlos. La figura 2.5 muestra el acceso a través de una conexión conmutada.

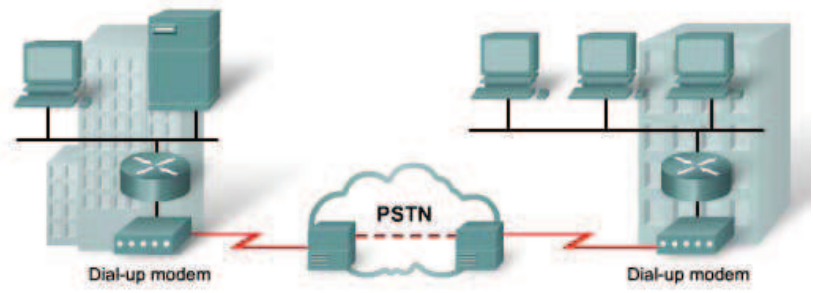

Figura 2.5 Acceso conmutado o *dial-up*[2]

Al utilizar la línea telefónica, la calidad de conexión no es siempre buena y está sujeta a pérdida de datos y limitaciones de todo tipo. Por ejemplo, durante la conexión a Internet no es posible usar la misma línea telefónica para una conversación.

Las conexiones *dial-up* poseen velocidades que van desde los 2400 bps hasta los 56 Kbps y son utilizadas en zonas rurales o en áreas muy remotas, donde las conexiones de banda ancha son imposibles por falta de infraestructura.

Actualmente, los ISPs ofrecen a sus clientes un servicio un poco diferente al de *dial-up*, al cual se puede acceder por medio de tarjetas prepago que cubren el valor correspondiente al servicio, mientras que el uso de la línea telefónica es cancelado por separado.

2.2.5.2 Acceso *Digital Subscriber Line* (DSL)[16]

Este tipo de acceso utiliza la línea telefónica a mayor velocidad y al mismo tiempo permite a los usuarios utilizar el teléfono para una conversación. Además, no es necesario esperar el marcado telefónico y la conexión al ISP.

El acceso DSL tiene varios tipos de tecnologías que son referidas como xDSL, con un rango aproximado entre 128 Kbps y 8 Mbps. Tiene tres categorías principales que son *Asymmetric* DSL (ADSL), *Symmetric* DSL (SDSL) y *Very High* DSL (VDSL).

2.2.5.2.1 Asymmetric Digital Subscriber Line (ADSL)[6][17]

ADSL es un tipo de línea DSL que consiste en una transmisión de datos digital a través del par simétrico de cobre que lleva la línea telefónica, consiguiendo velocidades descendentes de 1,5 Mbps en distancias de 5 o 6 Km, aunque si la distancia se reduce a 3 Km se puede llegar hasta los 9 Mbps, y velocidades ascendentes de 16 a 640 Kbps sobre los mismos tramos.

Este tipo de acceso a Internet es de banda ancha, lo que implica capacidad para transmitir más datos en un mismo tiempo. Con ADSL, el envío y recepción de los datos se establece desde el ordenador del usuario a través de un módem ADSL, encargado de modular las señales de datos usando el espectro de frecuencias entre 0 y 4 KHz de un canal telefónico y el rango comprendido entre 4 KHz y 2,2 MHz, como se indica en la figura 2.6. Al operar sobre una banda de frecuencias fuera de las vocales, el servicio telefónico normal se mantiene inalterado en caso de falla.

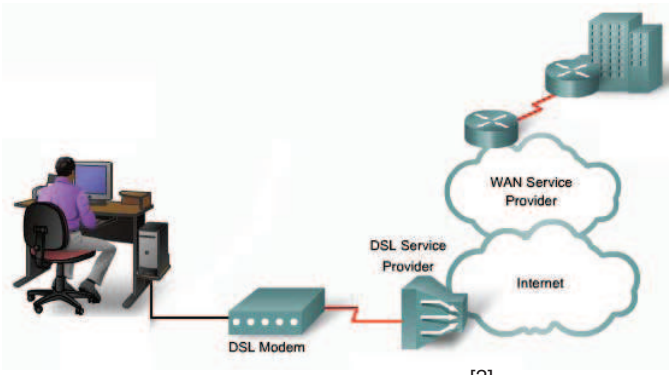

Figura 2.6 Acceso ADSL[2]

Con el fin de evitar distorsiones en las señales transmitidas, es necesaria la instalación de un filtro llamado *splitter*, que se encarga de separar la señal telefónica convencional de las señales moduladas de la conexión mediante ADSL. En una línea ADSL, se establecen tres canales de comunicación:

- Dos canales de alta velocidad, uno de recepción y otro de envío de datos.
- Un tercer canal para la comunicación normal de voz.

ADSL ofrece la ventaja de ser un servicio permanente para cada usuario, por lo que la calidad del servicio es constante, mientras que con otros módems la línea

se comparte entre todos los usuarios, degradándose la calidad de servicio conforme se van conectando o el tráfico va aumentando.

2.2.5.2.2 Symmetric Digital Subscriber Line (SDSL)[18]

La tecnología SDSL es una variante de DSL con velocidades de 400, 800, 1200 y 2048 Kbps. SDSL funciona enviando pulsos digitales en el área de alta frecuencia de las líneas telefónicas y no puede operar simultáneamente con las conexiones de voz en la misma línea, requiriendo de un módem especial SDSL para operar.

SDSL proporciona igual ancho de banda para capacidad de subida de datos, bajada de datos y transferencias directas. Su costo es relativamente más caro que la conexión ADSL, pero a su vez es más veloz.

2.2.5.2.3 Very high Digital Subscriber Line (VDSL)[6]

VDSL, también llamada como VADSL y BDSL, permite velocidades mayores que cualquier otra técnica sobre distancias muy cortas, encontrándose todavía en fase de definición. Alcanza una velocidad descendente de 52 Mbps sobre distancias de 300 metros y de sólo 13 Mbps si se alarga hasta los 1500 metros, siendo su velocidad ascendente de 1,5 y 2,3 Mbps respectivamente.

2.2.5.3 Acceso por cable[2][19]

En este acceso a Internet, la información es enviada por fibra óptica y llega al usuario con cable coaxial, donde se utiliza un dispositivo denominado cable módem para conectar la computadora al proveedor, con una velocidad que va desde los 512 Kbps hasta los 20 Mbps.

El cable módem permite una conexión permanente a Internet, es fácil de instalar y es el encargado de trasladar las señales digitales, en frecuencias de banda ancha, usadas para transmitir sobre la red de televisión por cable. La oficina de televisión por cable local, denominada como cable *headend*, contiene el sistema computacional y las bases de datos necesarias para proveer el acceso a Internet. El componente más importante localizado en el *headend* es el *Cable Modem*

Termination System (CMTS), encargado de enviar y recibir las señales digitales sobre la red de cable, así como de proveer el servicio a los usuarios. La figura 2.7 muestra la forma en la que los clientes acceden al servicio de Internet por cable.

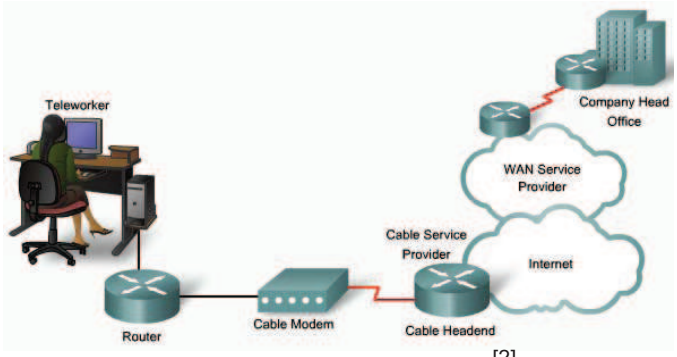

Figura 2.7 Acceso por cable[2]

Dependiendo de la infraestructura instalada por el proveedor de servicios, este tipo de conexión se puede ofrecer en alguna de las siguientes modalidades:

- **Modalidad de retorno telefónico:** Consistente en que el usuario recibirá la señal de Internet a través del cable coaxial, pero si desea enviar algún dato tendrá que hacerlo por medio de una línea telefónica. Por lo tanto, es necesario activar las dos conexiones para contar con acceso completo a Internet.
- **Modalidad de doble vía:** Ésta es la modalidad ideal, consistente en que toda la información que se envía y recibe viaja a través del cable coaxial.

Además, se puede hacer uso de la televisión al mismo tiempo que se está conectando a Internet, ya que lo único que se necesita es instalar un *splitter* para hacer una derivación hacia el cable módem.

2.2.5.3.1 Tipos de módems utilizados[6]

El cable módem puede ser de dos tipos:

- **Módems coaxiales de fibra óptica *Hybrid Fiber Coaxial* (HFC):** Son dispositivos bidireccionales que operan por cable HFC. Los módems HFC por lo general ofrecen velocidades de carga en el rango de 3 a 30 Mbps y velocidades de descarga entre 128 Kbps y 10 Mbps, aunque actualmente los usuarios pueden esperar velocidades de alrededor de los 4 Mbps.

- **Módems unidireccionales:** Son más antiguos que los anteriores y operan por cables coaxiales de televisión tradicionales. Los módems unidireccionales de cable coaxial permiten velocidades de carga de hasta 2 Mbps y requieren de un módem convencional de marcación para completar la conexión.

2.2.5.4 Acceso *clear channel*[6]

El acceso *clear channel* es una conexión dedicada, directa y de mejor calidad entre el ISP y el cliente. Son circuitos cuya característica principal es que su velocidad tanto de transmisión como de recepción es la misma y están instalados sobre redes *Time Division Multiplexing* (TDM), lo que garantiza que no existirán niveles de compartición en la última milla, así como tampoco en el lado del proveedor.

Este acceso permite una conexión ilimitada y permanente a Internet, con velocidades de 64, 128 y 256 Kbps.

2.2.5.5 Acceso satelital[6][16]

Este tipo de conexión permite acceder a Internet a través de un satélite que orbita la tierra, sin imponer límites de distancia entre el proveedor y el cliente, brindando velocidades de 492 a 512 Kbps. El acceso satelital es ideal para empresas grandes, medianas o pequeñas que actualmente se ven imposibilitadas de tener un acceso a Internet 24 horas, debido a que no hay ningún proveedor en la zona o que las conexiones existentes son de muy mala calidad.

Las conexiones satelitales necesitan para acceder al servicio de Internet de un módem ADSL, una antena VSAT y un proveedor de Internet satelital, como se indica en la figura 2.8. Sin embargo, la instalación puede ser difícil. La activación del servicio puede ser más cara y complicada que otros tipos de servicios de alta velocidad, debido al costo de los dispositivos y a la necesidad de una línea de visión despejada hasta el satélite del proveedor. Además, por la gran distancia, la señal debe viajar desde la superficie de la tierra hasta el satélite y luego volver otra vez, haciendo lento el servicio, especialmente en la velocidad de respuesta.

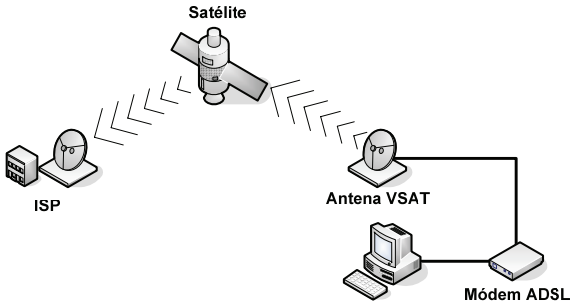

Figura 2.8 Acceso satelital

2.2.5.6 Acceso *hot spots*[6]

Un *hot spot* es una zona de cobertura que ofrece servicios de Internet inalámbrico de corto alcance. Los *hot spots* se encuentran en lugares públicos como aeropuertos, bibliotecas, centros de convenciones, cafeterías, hoteles, etc. Para acceder a este servicio es necesario que el computador, dispositivo PDA o teléfono móvil incluya en su hardware una tarjeta de acceso inalámbrico 802.11g o más reciente. La figura 2.9 muestra cómo los dispositivos acceden a los *hot spots*.

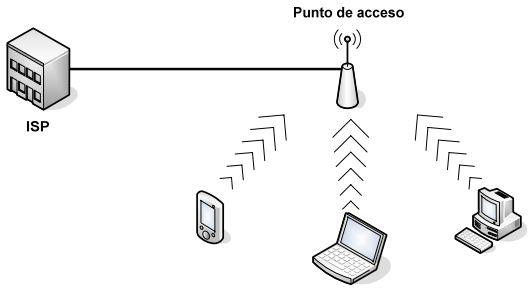

Figura 2.9 Acceso *hot spots*

Las desventajas de este servicio es que es susceptible a interferencias causadas por otros aparatos que utilizan la misma frecuencia y a condiciones físicas de la sala, o en el caso de exteriores, de los elementos físicos.

2.2.5.7 Acceso *Broadband over Power Lines* (BPL)[20]

Actualmente, se han desarrollado tecnologías que utilizan las líneas de energía eléctrica convencionales para transmitir señales de radio para propósitos de comunicación, denominadas como *Power Line Communications* (PLC). Esta tecnología 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 por banda ancha, conocido como *Broadband over Power Lines* (BPL).

BPL utiliza los cables de electricidad existentes en un edificio para acceder a Internet, por medio de un módem especial enchufado en cualquier toma de energía, como se indica en la figura 2.10.

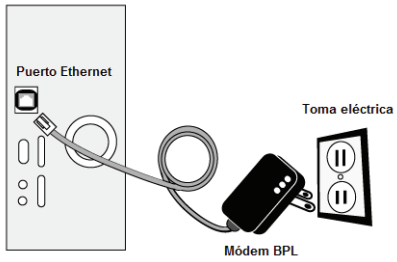

Figura 2.10 Acceso BPL

Los módems BPL transmiten en la gama de frecuencias de 1,6 a 30 MHz. La velocidad asimétrica en el módem va generalmente desde 256 Kbps hasta 2,7 Mbps. En el repetidor, situado en el cuarto de medidores de un edificio, la velocidad es hasta 45 Mbps y se puede conectar con 256 módems. En las estaciones de voltaje medio, la velocidad desde los *headend* hacia Internet es de hasta 134 Mbps. Para conectarse con Internet, las empresas de electricidad pueden utilizar un *backbone* de fibra óptica o enlaces inalámbricos.

A primera vista, la tecnología BPL parece ofrecer ventajas con respecto a las conexiones regulares de banda ancha, debido a la amplia infraestructura disponible, permitiendo que usuarios en lugares remotos tengan acceso a Internet con una inversión de equipo relativamente pequeña para la compañía eléctrica.

Sin embargo, la carencia actual de estándares por parte del *Institute of Electrical and Electronics Engineers* (IEEE) hace que el suministro del servicio esté lejos de ser un proceso estandarizado y repetible, y que el ancho de banda que un sistema BPL puede proporcionar, comparado con sistemas de cable e inalámbricos, esté en duda. Además, el sistema tiene un número de problemas complejos, siendo el primero que las líneas de energía intrínsecamente constituyen ambientes muy ruidosos; cada vez que un dispositivo se enciende o apaga, introduce voltajes transitorios en la línea. Los dispositivos ahorradores de

energía introducen a menudo armónicos ruidosos en la línea. El sistema se debe diseñar para ocuparse de las interrupciones naturales de las señales y trabajar con ellas.

2.2.6 TIPOS DE CLIENTES[7]

Los ISPs distinguen dos tipos principales de clientes: corporativos y residenciales. Dependiendo del tipo de cliente, se puede determinar la mejor forma de acceder a Internet a través del proveedor.

2.2.6.1 Clientes corporativos

Los clientes corporativos son entidades empresariales, agencias del gobierno, organizaciones, universidades, bancos, e incluso ISPs más pequeños, que requieren conectar su red a Internet a través de un ISP. La conectividad hacia el cliente corporativo precisa de tres elementos principales:

- Equipo Terminal de Abonado (CPE)
- Circuito de transmisión
- *Router* PoP

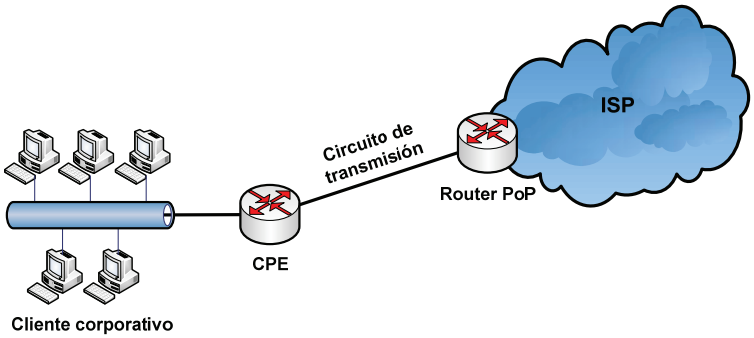

Figura 2.11 Elementos de un cliente corporativo

2.2.6.1.1 Equipo Terminal de Abonado (CPE)

Este equipo se encuentra generalmente en el lado del abonado, puede ser propio o arrendado y se encarga de interconectar la red local del cliente. Realiza funciones específicas como la seguridad a través de *firewalls* y el filtrado de tráfico.

2.2.6.1.2 Circuito de transmisión

Consiste en un circuito dedicado que puede ser uno de los circuitos conmutados *Frame Relay*, ATM, MPLS; puede ser arrendado desde el *carrier*.

2.2.6.1.3 Router Punto de Presencia (PoP)

Este *router* es el límite lógico de la zona de administración del ISP. Se encarga de funciones de control de ruteo y administración de acceso a la red del cliente. El *router* PoP tiene instalado los filtros de ruta y realiza control del tráfico entrante y saliente de la red, monitoreo y confiabilidad. Los clientes corporativos pueden conectarse al proveedor por medio de tres formas:

- **Cliente *single-homed*:** Cuando el cliente se conecta directamente a un solo ISP por medio de un puerto de acceso dedicado.
- **Cliente multiconectado:** Cuando el cliente se conecta al ISP por más de una conexión, aumentando la robustez y confiabilidad del enlace.
- **Cliente *multi-homed*:** Cuando el cliente recibe conectividad de tiempo completo procedente de varios ISPs, mejorando la fiabilidad de la conectividad externa.

2.2.6.2 Clientes residenciales

Son usuarios aislados como el computador de un hogar o de una oficina pequeña. En la mayoría de casos, se conectan al ISP a través de un acceso *dial-up*. Generalmente este tipo de clientes utilizan correo electrónico y páginas web.

2.2.7 ACUERDO DE NIVEL DE SERVICIO (SLA)[5]

Un SLA es un protocolo plasmado normalmente en un documento de carácter legal, por el que una compañía que presta un servicio a otra se compromete a prestar el mismo, bajo determinadas condiciones y con prestaciones mínimas de mutuo acuerdo. Entre las determinadas condiciones de un SLA están el nivel operativo de funcionamiento, limitaciones de responsabilidad y penalizaciones por

caída de servicio, disponibilidad temporal, métodos de medida, tarifas de los servicios, entre otras.

Este acuerdo debe considerar diferentes tópicos que representan una serie de parámetros mínimos que describen los niveles de servicio, entre los que se puede mencionar:

- Alcance del SLA
- Disponibilidad
- Conexión al punto de presencia
- Parámetros comprometidos
- Servicios de valor agregado
- Condicionamiento de tráfico

2.2.7.1 Alcance del SLA

El proveedor puede dar mantenimiento sólo a su *backbone* o incluir los CPEs, lo que se define como el alcance del SLA. El proveedor se hace responsable de las entidades de hardware o software que puede controlar; si incluye los equipos de acceso, se convertiría en un SLA de extremo a extremo.

2.2.7.2 Disponibilidad

Los servicios que se ofrecen deben contemplar el factor de disponibilidad de los mismos. La no disponibilidad de un servicio puede afectar a una entidad, a sus funcionarios o a los usuarios de los servicios que provee la entidad. Es decir, la disponibilidad se define en porcentaje como el tiempo en el cual el servicio está disponible en un lapso sobre un determinado tiempo de medición, generalmente mensual.

2.2.7.3 Conexión al punto de presencia

Aparte de la disponibilidad de la conexión, deben definirse niveles de servicio entre el proveedor y el cliente que reflejen de manera clara la calidad y desempeño de la solución de última milla que se contrate. Además, debe

considerarse la capacidad de reacción ante fallas que puedan presentarse en el servicio de conectividad. Dependiendo del tipo de tecnología que utilice el proveedor para su última milla, ésta debe especificar de manera concisa sus parámetros de desempeño.

2.2.7.4 Parámetros comprometidos

Algunos servicios requieren ciertos niveles de calidad de servicio que, actualmente, los ISPs están poniendo a disposición de sus clientes. Los proveedores garantizan el valor de uno o varios de los parámetros que definen la calidad de servicio que ofrece la red en sus SLAs y el cliente solicita el nivel de servicio que desea. Sin embargo, si no hay un acuerdo previo entre ambas partes, el servicio ofrecido es el de "mejor esfuerzo". Entre los parámetros comprometidos más importantes están el ancho de banda, retardo, *jitter* y tasa de paquetes perdidos.

Los ISPs utilizan el término ancho de banda para referirse a la tasa de transferencia de datos, que es la cantidad de datos que se pueden llevar de un punto a otro en un período dado. La tasa de transferencia es medida en bits por segundo (bps), mientras que el ancho de banda es medido en *Hertzios* (Hz), pero comercialmente se utiliza el término ancho de banda en bits por segundo (bps).

2.2.7.5 Servicios de valor agregado

Este servicio es responsabilidad contractual del proveedor con cada usuario, donde describe, expone y precisa en detalle los componentes y aspectos que lo destacan como un buen proveedor de dichos servicios, cualquiera que haya sido contratado u ofrecido como facilidades o servicios complementarios a la conectividad.

2.2.7.6 Condicionamiento de tráfico

Los SLAs deben adjuntar funciones de control de los requisitos de tráfico, denominados como Acuerdo de Condicionamiento de Tráfico (TCA). Este acuerdo

contiene reglas para clasificar el tráfico, reglas de condicionamiento de acuerdo a los perfiles de tráfico dentro de un SLA y reglas implícitas de los requisitos del servicio.

2.3 ANÁLISIS DE TRÁFICO EN UN ISP

Las muestras de tráfico a utilizarse en el análisis serán obtenidas de la empresa Telconet S.A., empresa portadora dedicada a ofrecer servicios de Internet y transmisión de datos a clientes corporativos y residenciales, con sede en la ciudad de Quito. A fin de realizar el posterior análisis, se procederá a efectuar una breve descripción de la red de Telconet S.A.

2.3.1 BREVE DESCRIPCIÓN DE LA RED DE TELCONET S.A.[85]

Actualmente, Telconet S.A. está en proceso de migración desde su red *Gigabit Ethernet* con tecnología IP a la tecnología MPLS. La mayoría de clientes utilizan la tecnología IP, mientras que son pocos los clientes que están conectados bajo MPLS.

La red de Telconet S.A. con tecnología IP/MPLS está diseñada bajo el modelo jerárquico de tres capas. La capa *core* está formada por dos nodos que concentran la mayor cantidad de tráfico, interconectados con fibra óptica monomodo. Los equipos de estos nodos trabajan como LSRs y son denominados como:

- CAT6500G (Gosseal)
- CAT6500M (Muros)

Adicionalmente, la capa *core* tiene otros equipos que distribuyen el tráfico a grandes velocidades y trabajan como LSRs y LERs a la vez, para permitir el paso entre las tecnologías IP y MPLS. Estos nodos enrutan el tráfico entrante a la red MPLS, usando un protocolo de señalización de etiquetas y distribución de tráfico saliente. Estos equipos son denominados como:

- PE1UIOG

- PE2UIOG
- PE1UIOM
- PE2UIOM

Los nodos PE indicados anteriormente forman también parte de la capa distribución, debido a las funciones que realizan como la implementación de políticas de ruteo y de red, filtrado de paquetes, seguridad, enrutamiento entre VLANs, entre otras.

La capa distribución implementa otros nodos para formar segmentos de red más pequeños denominados anillos, con enlaces redundantes para casos de fallas, cuya principal función es administrar los anillos que dependan de ellos. Los nodos de esta capa son denominados como:

- SW1AGUIOG
- SW2AGUIOG
- SW1AGUIOM
- SW2AGUIOM

Todos los enlaces entre los nodos de la capas *core* y distribución son de 1 Gbps de capacidad.

La capa acceso permite la interconexión de los clientes con la red de Telconet S.A., utilizando como medios de transmisión de última milla fibra óptica y enlaces de microondas. Los 48 nodos de esta capa conforman los anillos que son administrados por los nodos de la capa distribución, con un máximo de siete nodos por anillo. Además, esta capa tiene implementado un CPE para interconectar la red del cliente con la red de Telconet S.A.; estos equipos son entregados por la empresa en modalidad de alquiler y permiten manejar los protocolos de capa enlace y capa red para realizar las VPNs. Los CPEs no manejan tecnología MPLS.

La figura 2.12 muestra la red de Telconet S.A. descrita para las capas *core*, distribución y acceso del modelo jerárquico. El análisis de tráfico será realizado sobre las capas *core* y distribución, donde se encuentra concentrado la mayor cantidad de tráfico.

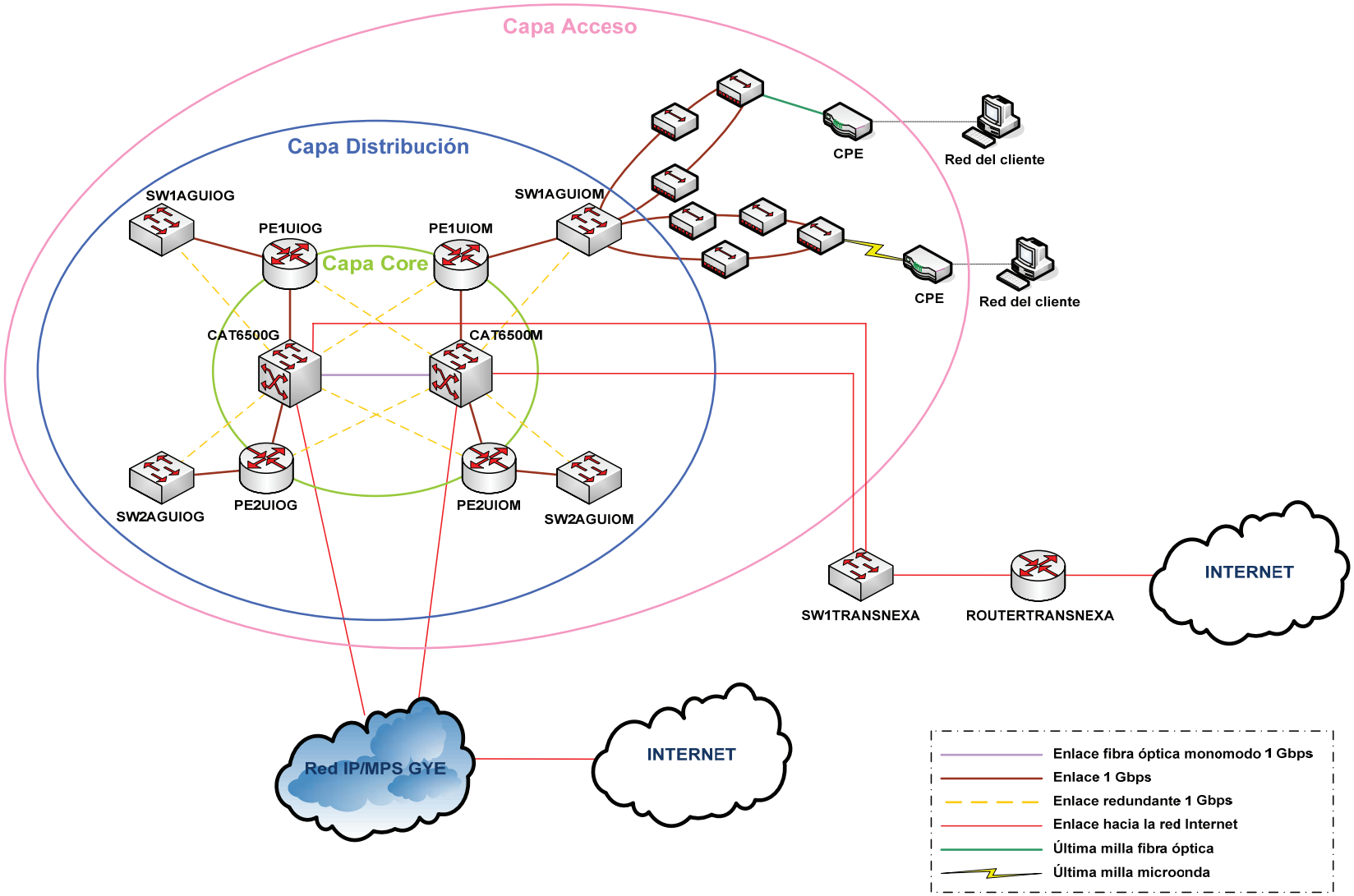

Figura 2.12 Red IP/MPLS de Telconet S.A. de acuerdo al modelo jerárquico

2.3.2 CARACTERÍSTICAS DE LA HERRAMIENTA UTILIZADA PARA EL MONITOREO DE LOS EQUIPOS[21][22]

Telconet S.A. hace uso de la herramienta CACTI para monitorear el tráfico y la carga de CPU en los equipos de su red. Esta herramienta polea información de los equipos y almacena los datos obtenidos en una base de datos de MySQL, para luego presentarlos en forma de gráficos.

CACTI aprovecha el poder de almacenamiento y la funcionalidad de graficar que posee la Round *Robin Database tool* (RRDtool), que es una herramienta que trabaja con una base de datos que maneja planificación *round-robin*. Esta técnica consiste en que la base de datos trabaja como si fuera un círculo, sobreescribiendo los datos almacenados hasta alcanzar la capacidad de la base, que depende de la cantidad de información como historial que se quiera conservar.

Esta herramienta tiene una interfaz de usuario fácil de usar, que resulta conveniente para instalaciones del tamaño de una LAN, así como también para redes complejas con cientos de dispositivos.

Las principales características de CACTI se indican a continuación:

- **Obtención de los datos:** Un concepto ligado a la RRDtool es el de *Simple Network Management Protocol* (SNMP). Este protocolo es usado para realizar consultas a dispositivos acerca del valor de los contadores que ellos tienen. El valor obtenido de esos contadores es el que se almacena en la RRD.
- **Fuente de datos:** Para manejar la recopilación de datos, CACTI sigue la ruta a cualquier *script* o comando junto con cualquier dato que el usuario necesite ingresar, los reúne y carga en la base de datos de MySQL, así como los archivos de la planificación *round-robin* que debe actualizar. Una fuente de datos también puede ser creada, haciendo uso de *scripts* y definiendo cualquier información adicional que la fuente requiera. Luego de que una fuente de datos es creada, es automáticamente mantenida cada cinco minutos.

- **Gráficos:** Una vez que una o más fuentes de datos son definidas, una gráfica de RRDtool puede ser creada usando los datos obtenidos. CACTI permite crear prácticamente cualquier gráfica como por ejemplo el uso de conexión a Internet, datos como temperatura, velocidad, voltaje, etc. Además, existen varias formas de mostrar las gráficas como la lista de vistas estándar, vista preliminar y vista en árbol, la cual permite colocar gráficos en un árbol jerárquico para propósitos organizacionales.
- **Manejo de usuarios:** CACTI cuenta con la funcionalidad de manejo de usuarios embebida, para así hacer posible agregar un usuario y darle permisos a ciertas áreas de la herramienta. Esto permite tener usuarios que puedan cambiar parámetros de un gráfico, mientras que otros sólo pueden ver los gráficos. Así mismo, cada usuario mantiene su propia configuración de vista de gráficos.
- **Plantillas:** CACTI puede escalar a un gran número de fuentes de datos y gráficos a través de plantillas. Esto permite la creación de una única plantilla de gráficos o fuente de datos, la cual define cualquier gráfico o fuente de datos asociada con esta plantilla. Las plantillas de *hosts* permiten definir las capacidades de un *host*, así CACTI puede utilizar esta información a la hora de agregar un nuevo *host*.

2.3.3 ANÁLISIS DEL USO DE LA CAPACIDAD EN LOS ENLACES

Mediante la herramienta CACTI y los criterios que proporciona, se obtuvieron muestras de forma mensual del tráfico que circula por los enlaces de la red MPLS de Telconet S.A.

La tabla 2.1 indica los valores de tráfico promedio de entrada (*Inbound Average*) y de salida (*Outbound Average*) del mes de Enero del 2009, obtenidos de las gráficas del **ANEXO 1 MEDICIÓN DE LA CAPACIDAD EN LOS ENLACES**.

Al observar los valores obtenidos en la tabla 2.1 durante el monitoreo del tráfico en los enlaces, se puede notar que son sumamente bajos, no representando el tráfico real que circularía por la red MPLS, debido a que el número de clientes conectados bajo esta tecnología actualmente es del 2%.

Enlace	*Inbound Average*	*Outbound Average*
CAT6500G y PE1UIOG	4,61 Mbps	5,71 Mbps
CAT6500G y PE2UIOG	14,03 Mbps	3,78 Mbps
CAT6500G y PE1UIOM	12,55 Kbps	12,66 Kbps
CAT6500G y PE2UIOM	4,11 Mbps	5,36 Mbps
CAT6500G y CAT6500M	5,16 Kbps	4,19 Kbps
CAT6500G y SW1AGUIOG	14,54 Kbps	423,68 Kbps
CAT6500G y SW2AGUIOG	1,43 Kbps	409,95 Kbps
CAT6500M y PE1UIOM	4,33 Kbps	3,16 Mbps
CAT6500M y PE2UIOM	2,21 Kbps	18,25 Kbps
CAT6500M y PE1UIOG	419,09	3,51 Kbps
CAT6500M y PE2UIOG	417,26	3,51 Kbps
CAT6500M y SW1AGUIOM	3,15 Mbps	368,72 Kbps
CAT6500M y SW2AGUIOM	1,89 Kbps	393,41 Kbps
PE1UIOG y SW1AGUIOG	155,80 Kbps	15,13 Kbps
PE2UIOG y SW2AGUIOG	21,13 Kbps	172,99
PE1UIOM y SW1AGUIOM	23 Kbps	3,14 Mbps
PE2UIOM y SW2AGUIOM	21,02 Kbps	172,50

Tabla 2.1 Tráfico promedio mensual de entrada y salida en los enlaces

De acuerdo al estudio de tráfico realizado por el departamento de Proyectos de Telconet S.A. previo al proceso de migración, los nodos de la capa *core* soportarían el tráfico presentado en la tabla 2.2.

Nodo	Tráfico MPLS (Mbps)
CAT6500G	195,62
PE1UIOG	89,38
PE2UIOG	74,82
CAT6500M	232,53
PE1UIOM	108,6
PE2UIOM	88,59

Tabla 2.2 Estudio de tráfico de la red MPLS de Telconet S.A.[86]

El tráfico indicado es el tráfico total por cada nodo, el cual se reparte entre las diferentes interfaces de cada equipo, lo que llevaría a concluir que los enlaces de 1 Gbps de la red MPLS de Telconet S.A. no estarán saturados luego de migrar los clientes desde la red con tecnología IP.

2.3.4 ANÁLISIS DEL USO DE CPU DE LOS EQUIPOS

Se considera que un equipo está siendo usado de forma normal cuando su porcentaje de rendimiento de CPU no supera el 75%, caso contrario, debe evaluarse su funcionamiento para tomar medidas al respecto[4].

El **ANEXO 2 MEDICIÓN DEL USO DE CPU DE LOS EQUIPOS** muestra las gráficas del rendimiento de CPU de los nodos de la red MPLS de Telconet S.A. Analizando estas gráficas, se concluye que ningún equipo tiene un rendimiento mayor del 14%, que es el rendimiento máximo en el nodo SW2AGUIOM, debido al escaso número de clientes conectados con MPLS en la actualidad.

El porcentaje indicado está dentro del porcentaje de uso normal de CPU del equipo explicado anteriormente, por lo que no es necesario hacer ninguna mejora ó tomar medidas al respecto.

2.3.5 CARACTERÍSTICAS DEL EQUIPO UTILIZADO PARA EL MONITOREO DE LAS APLICACIONES[23]

Telconet S.A. tiene instalado dos equipos analizadores de tráfico modelo PTS 8210 de la compañía Sandvine.

El *Policy Traffic Switch* (PTS) es un equipo de alto rendimiento en tiempo real basado en la inspección profunda de paquetes (DPI), que es una tecnología de filtrado de paquetes que analiza los datos y/o parte de la cabecera de un paquete. Este equipo cuando un paquete pasa por un punto de inspección, lo analiza en busca de un protocolo de no cumplimiento, virus, *spams*, intrusiones o criterios previamente definidos, para decidir si el paquete puede pasar, o si tiene que ser enviado a un destino diferente, o con el fin de recoger información estadística.

Entre las principales características que ofrece la compañía Sandvine en sus equipos están:

- **Administración inteligente de tráfico:** El tráfico *peer-to-peer* (P2P) consume una buena parte del ancho de banda en la actualidad, por lo que es necesario la optimización de sesiones externas P2P que utilizan ancho de banda ascendente, optimización de las descargas P2P de los clientes mediante rutas de red preferidas y la modelación adaptable de tráfico.
- **Administración de políticas:** Estos equipos ofrecen una gran capacidad para aplicar administración de políticas de tráfico por tipo de servicio, agente de políticas de clientes para definición y administración de políticas simple y centralizada, y opciones de identificación de clientes mediante integración del protocolo *Dynamic Host Configuration Protocol* (DHCP), *Radius* u OSS.
- **Integridad de red:** Brindan protección a la red contra ataques como gusanos, ataques de negación de servicio (DoS), troyanos en correo no deseado y ataques de servidores de nombres de dominio (DNS).
- **Creación de servicios para clientes:** Las redes actuales de servicios mínimos no están adaptadas para abordar aplicaciones multimedia sensibles al *jitter* y a los retardos, por lo que los equipos PTS pueden introducir nuevos servicios priorizados para juegos, voz sobre IP y otras aplicaciones multimedia, mediante el establecimiento de los bits del campo ToS del paquete IP para identificar el tráfico priorizado.
- **Administración de soporte operacional:** La QoS cumple un papel importante en el tráfico de los clientes a medida que las aplicaciones de Internet se convierten en una pieza clave de sus estilos de vida. Esta característica administra el tráfico total o por cliente de las aplicaciones, alertando acerca de tendencias de calidad de aplicaciones, de manera que se puedan resolver los problemas antes de que los clientes se vean afectados.
- **Compatibilidad con protocolos:** Permite reconocer tráfico P2P, búsqueda en la web, grupos de noticias, mensajería instantánea, correo electrónico, base de datos, protocolos de transmisión, tunelización que incluye VPNs,

voz sobre IP, conectividad remota, administración de red, protocolos de acceso a archivos, protocolos de almacenamiento de red y protocolos de juegos.

- **Demografía de redes:** Entrega de informes de aplicaciones avanzadas con visiones completas de toda la red, de la región y del cliente; informes para comprender mejor el comportamiento del cliente y análisis con valor agregado, que incluyen detalles de llamadas de voz sobre IP e informes de calidad de experiencia.

2.3.5.1 Resumen técnico del PTS 8210

Las principales características técnicas que presenta el PTS 8210 son:

- Interfaces *Gigabit Ethernet* monomodo/multimodo de fibra óptica y 10/100/1000 de cobre
- Entrada de 100 a 240 V AC o de 42 a 60 V DC
- Temperatura de funcionamiento entre 0°C y 40°C
- Humedad del 5% al 85% sin condensación
- Montaje en soporte de 48 cm, 1 Unidad de *Rack* (RU)

2.3.5.2 Conexión de los PTS 8210 en la red[87]

Los equipos PTS 8210 están instalados en la salida hacia Internet de la red de Telconet S.A. de Quito, por lo que el tráfico de las aplicaciones que están monitoreando son tanto de los clientes conectados con tecnología MPLS como con tecnología IP. La figura 2.13 indica la conexión de los equipos en la red.

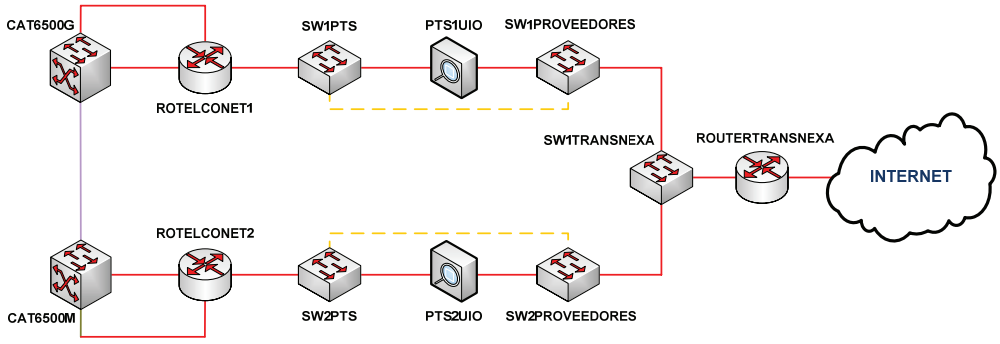

Figura 2.13 Conexión de los PTS en la red

Los nodos ROTELCONET1 y ROTELCONET2 son equipos instalados con dos enlaces a los nodos de la capa *core* para permitir el enrutamiento entre los clientes con tecnología MPLS y los clientes con tecnología IP, es decir, estos equipos están configurados con MPLS y sin MPLS.

El nodo ROUTERTRANSNEXA es un equipo de marca Cisco 7513, utilizado para la interconexión con el proveedor internacional de Internet, Transnexa, que a su vez tiene una conexión con el cable panamericano NAP de las Américas. Este *router* recibe todas las peticiones de usuarios para ingresar a Internet; es decir, es la puerta de enlace hacia el proveedor internacional.

Cada equipo PTS monitorea por separado los equipos de la capa *core* CAT6500G y CAT6500M, los cuales de acuerdo a estudios de tráfico proporcionados por el departamento de Proyectos de la empresa, cada uno de ellos soporta un tráfico aproximado de 200 Mbps.

2.3.6 ANÁLISIS DEL TRÁFICO DE LAS APLICACIONES

Como se mencionó anteriormente, cada equipo PTS monitorea un tráfico aproximado de 200 Mbps, por lo que el análisis se lo realizará en sólo uno de los equipos, en el PTS1UIO instalado en Telconet S.A.

Utilizando el equipo indicado, se realizó el monitoreo del tráfico semanal de las aplicaciones de todos los clientes de la empresa. El **ANEXO 3.1 TRÁFICO DIARIO DE LAS APLICACIONES POR CATEGORÍA** presenta las gráficas del tráfico transmitido y recibido de las aplicaciones dividido en cinco grandes categorías que se explican a continuación:

- **Navegación vía web:** Agrupa los diferentes protocolos y aplicaciones utilizados para visualizar e interactuar con textos, imágenes, vídeos y cualquier otro tipo de información, localizada en la página web de un sitio web en la *World Wide Web* (WWW)[24].
- ***Peer-to-peer* (P2P):** Engloba las aplicaciones utilizadas para compartir archivos en cualquier formato digital, en una red que no tiene clientes ni servidores fijos[25].

- **Tunelización:** Categoría que concentra los protocolos utilizados para encapsular un protocolo de red sobre otro protocolo, creando un túnel dentro de una red de computadoras, con el fin de encaminar paquetes de datos sobre nodos intermedios que son incapaces de ver su contenido[26].
- **Protocolos *streaming*:** Son los protocolos utilizados para escuchar música o ver vídeos directamente de una página web sin necesidad de descargarlos al ordenador previamente[27].
- **Voz sobre IP (VoIP):** Asocia los protocolos utilizados para permitir la transmisión de la voz sobre el protocolo IP.

El **ANEXO 4.1 CÁLCULO DEL TRÁFICO RECIBIDO POR CATEGORÍA** muestra el cálculo del tráfico recibido promediado por día y por semana de forma categorizada, obtenido de las gráficas del Anexo 3.1. A continuación se indica los resultados obtenidos del cálculo del tráfico recibido.

Horario	Navegación vía web	P2P	Tunelización	Protocolos streaming
02/02/09	77,96	71,52	3,25	1,67
03/02/09	82,33	79,39	3,89	2,70
04/02/09	159,58	19,39	8,27	4,05
05/02/09	159,42	19,79	8,27	4,05
06/02/09	155,61	21,54	9,14	3,66
Media semanal	**126,98 Mbps**	**42,33 Mbps**	**6,56 Mbps**	**3,23 Mbps**
Tráfico total recibido	179,10 Mbps			

Tabla 2.3 Tráfico recibido promediado por categoría

Los resultados mostrados en la tabla 2.3 se indican en la figura 2.14.

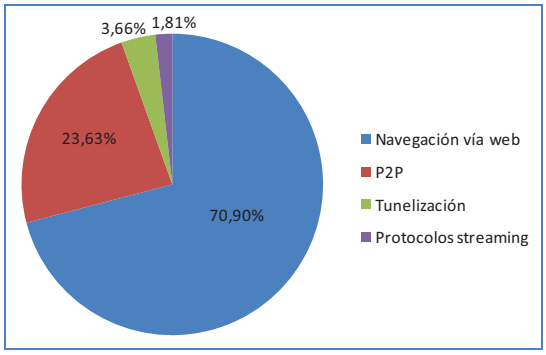

Figura 2.14 Tráfico semanal recibido por categoría

De acuerdo a los resultados mostrados en la figura 2.14, el tráfico de navegación vía web corresponde al 70,9% de la totalidad del tráfico recibido durante la semana de monitoreo. Este tráfico es utilizado para el acceso a las páginas web, lo que conlleva a concluir que tanto clientes corporativos como residenciales utilizan mayormente el servicio de acceso a Internet, ya sea para consulta de información, correo electrónico, entretenimiento, etc.

El **ANEXO 4.2 CÁLCULO DEL TRÁFICO TRANSMITIDO POR CATEGORÍA** muestra el cálculo del tráfico transmitido promediado por día y por semana de forma categorizada, obtenido de las gráficas del Anexo 3.1. En la tabla 2.4 se indican los resultados obtenidos del cálculo del tráfico transmitido.

Horario	Navegación vía web	P2P	Tunelización	Protocolos *streaming*	VoIP
02/02/09	0,96	4,42	0,25	0,09	0,21
03/02/09	1,00	2,51	0,38	0,39	0,17
04/02/09	2,05	6,02	1,34	0,10	0,27
05/02/09	1,52	7,57	0,52	0,13	0,26
06/02/09	1,86	11,77	0,71	0,08	0,11
Media semanal	**1,48 Mbps**	**6,46 Mbps**	**0,64 Mbps**	**0,16 Mbps**	**0,20 Mbps**
Tráfico total transmitido	8,94 Mbps				

Tabla 2.4 Tráfico transmitido promediado por categoría

Los resultados mostrados en la tabla 2.4 se indican en la figura 2.15.

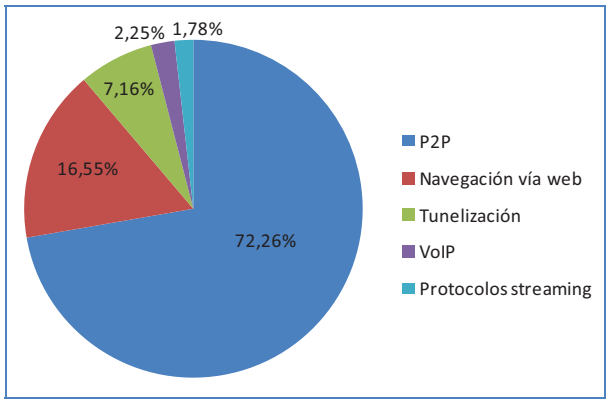

Figura 2.15 Tráfico semanal transmitido por categoría

De acuerdo a los resultados mostrados en la figura 2.15, el tráfico *peer-to-peer* (P2P) equivale al 72,26% de la totalidad del tráfico transmitido durante la semana de monitoreo. El tráfico P2P corresponde al tráfico utilizado para la compartición de archivos de cualquier naturaleza; es decir, que tanto clientes corporativos como residenciales transmiten archivos a la red Internet con el fin de compartir información y obtener privilegios para acceder de manera más rápida a una mayor cantidad de información.

El tráfico para la transmisión de la VoIP es significativo, representado un 2,25% del tráfico transmitido. Este tráfico es considerado de tiempo real y debe recibir excelentes prestaciones en cuanto a parámetros de QoS se refiere, a pesar de que su porcentaje no es alto en comparación con el resto de tráfico transmitido a través de la red.

La suma del tráfico recibido por categoría y del tráfico transmitido por categoría durante la semana de monitoreo dan un total de 188,04 Mbps, valor aproximado al tráfico de 200 Mbps que de acuerdo al departamento de Proyectos de Telconet S.A. monitorea cada equipo PTS 8210.

El **ANEXO 3.2 TRÁFICO DIARIO DE LAS APLICACIONES POR PROTOCOLO** indica las gráficas del tráfico transmitido y recibido de los protocolos de las categorías mencionadas anteriormente. Adicionalmente, Telconet S.A. monitorea el tráfico transmitido y recibido por las aplicaciones de los juegos en Internet.

El **ANEXO 4.3 CÁLCULO DEL TRÁFICO RECIBIDO POR PROTOCOLO** muestra el cálculo del tráfico recibido promediado por día y por semana de los protocolos que representan la mayor cantidad de tráfico en cada categoría, obtenido de las gráficas del Anexo 3.2. En la tabla 2.5 se indican los resultados obtenidos del cálculo del tráfico recibido.

Tráfico		02/02/09	03/02/09	04/02/09	05/02/09	06/02/09	Media semanal
Navegación vía web	HTTP	85,87	89,53	168,24	139,32	140,75	**124,74 Mbps**
P2P	*Ares* UDP	5,88	5,93	7,84	10,90	11,15	**8,34 Mbps**
	BitTorrent	3,75	3,89	11,94	7,23	8,62	**7,09 Mbps**
	eDondkey	2,00	3,18	4,40	4,82	7,09	**4,30 Mbps**
	Ares	2,36	1,44	3,58	3,18	4,30	**2,97 Mbps**
	Gnutella	1,37	0,58	1,59	0,87	0,34	**0,95 Mbps**
	RapidShare	1,16	1,59	2,35	1,87	3,08	**2,01 Mbps**
Tunelización	SSL	3,09	2,04	4,18	3,64	5,16	**3,62 Mbps**
	IPsec	0,39	0,46	1,24	3,20	0,95	**1,25 Mbps**
	SSH	0,16	0,09	0,27	0,18	0,11	**0,16 Mbps**
	GRE	0,07	0,07	0,12	0,09	0,18	**0,10 Mbps**
Protocolos *streaming*	*YouTube*	0,66	0,33	1,46	0,79	0,88	**0,82 Mbps**
	Flash Vídeo	0,66	0,76	1,22	0,84	1,80	**1,06 Mbps**
	RTSP	0,34	0,28	0,51	0,80	0,71	**0,53 Mbps**
	QQLive	0,32	0,12	0,38	0,38	0,52	**0,34 Mbps**
VoIP	*Skype*	0,27	0,35	0,59	0,56	0,53	**0,46 Mbps**
	UniqueFone	0,11	0,12	0,22	0,20	0,18	**0,17 Mbps**
	SIP RTP	0,05	0,03	0,08	0,09	0,07	**0,06 Mbps**
	SIP	0,04	0,04	0,04	0,05	0,06	**0,04 Mbps**
	H.323 Data	0,01	0,01	0,00	0,00	0,03	**0,01 Mbps**
	Skype In/Out	0,01	0,01	0,02	0,03	0,02	**0,02 Mbps**
	MSN *Media Data*	0,00	0,00	0,00	0,00	0,01	**0,00 Mbps**
Juegos	Xbox *Live*	0,01	0,01	0,02	0,01	0,01	**0,01 Mbps**
	World of Warcraft	0,01	0,00	0,09	0,07	0,09	**0,05 Mbps**
	Yahoo games	0,00	0,00	0,00	0,00	0,00	**0,00 Mbps**
	Blizzard Battle.net	0,00	0,00	0,00	0,00	0,01	**0,00 Mbps**
	PlayStation2 Unclassified	0,00	0,00	0,00	0,00	0,00	**0,00 Mbps**
	PlayStation2 Control	0,00	0,00	0,00	0,00	0,00	**0,00 Mbps**

Tabla 2.5 Tráfico recibido promediado por protocolo

Gráficamente, los resultados mostrados en la tabla 2.5 se pueden apreciar en la figura 2.16.

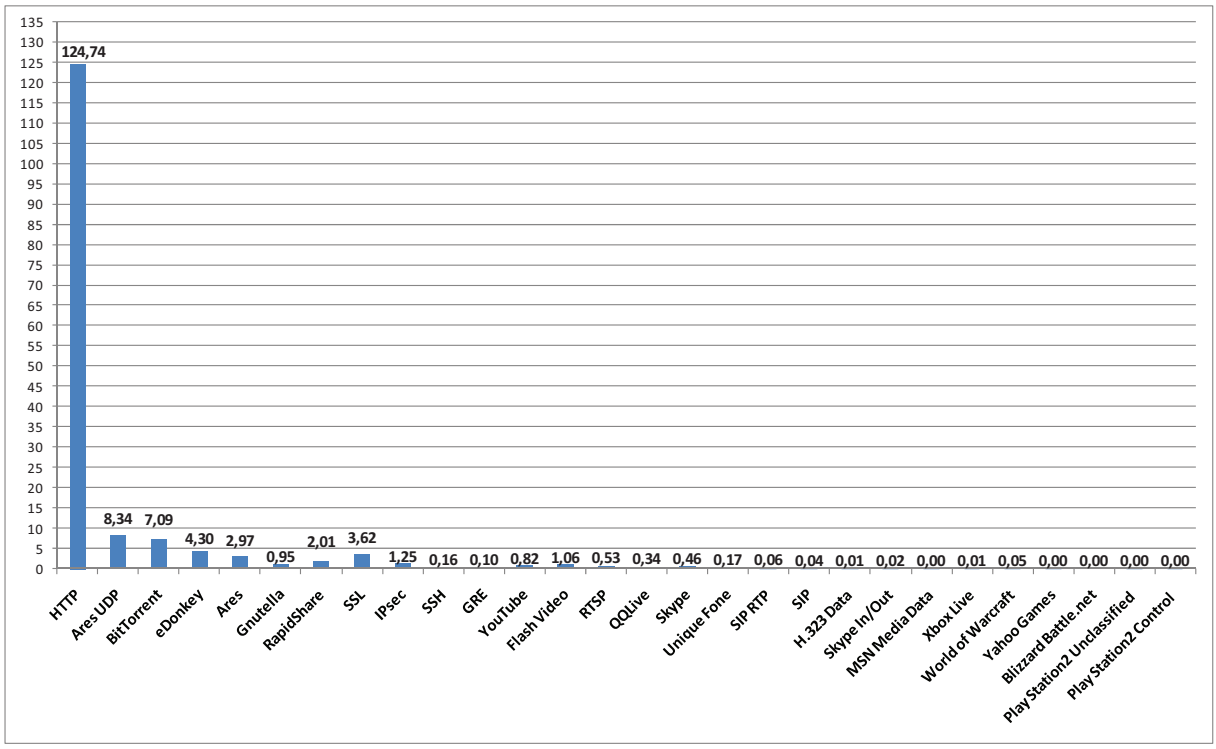

Figura 2.16 Tráfico semanal recibido por protocolo

De acuerdo a los resultados mostrados en la figura 2.16, el protocolo *Hyper-Text Transfer Protocol* (HTTP), utilizado para la navegación web, es el protocolo mayormente usado por el tráfico de entrada a la red, con un porcentaje del 69,65% respecto al tráfico total recibido; el porcentaje del 29,1% corresponde a los protocolos del tráfico P2P, tunelización, *streaming* y VoIP indicados en la figura 2.16, mientras que el 1,25% pertenece al resto de protocolos del tráfico de navegación vía web como *Facebook*, HTTP *Proxy* y *Nintendo Wii Web Browsing*, indicados en las gráficas del anexo 3.2.

El **ANEXO 4.4 CÁLCULO DEL TRÁFICO TRANSMITIDO POR PROTOCOLO** muestra el cálculo del tráfico transmitido promediado por día y por semana de los protocolos que representan la mayor cantidad de tráfico en cada categoría, obtenido de las gráficas del Anexo 3.2. En la tabla 2.6 se indican los resultados obtenidos del cálculo del tráfico transmitido.

Tráfico		02/02/09	03/02/09	04/02/09	05/02/09	06/02/09	Media semanal
Navegación vía web	HTTP	0,74	0,79	1,27	1,20	1,32	**1,06 Mbps**
	Facebook	0,04	0,02	0,06	0,05	0,05	**0,04 Mbps**
P2P	*eDonkey Encripted*	1,46	0,68	2,95	4,58	5,05	**2,94 Mbps**
	Ares UDP	0,90	0,78	1,15	1,23	1,43	**1,10 Mbps**
	BitTorrent	1,04	0,55	0,77	0,59	0,76	**0,74 Mbps**
	eDonkey	0,37	0,09	0,76	0,66	1,05	**0,59 Mbps**
	Ares	0,17	0,34	0,26	0,35	0,44	**0,31 Mbps**
Tunelización	SSL	0,08	0,24	0,15	0,37	0,30	**0,23 Mbps**
	IPsec	0,13	0,08	0,36	0,15	0,53	**0,25 Mbps**
	SSH	0,01	0,04	0,03	0,01	0,06	**0,03 Mbps**
	GRE	0,02	0,03	0,00	0,01	0,01	**0,01 Mbps**
Protocolos *streaming*	*YouTube*	0,03	0,03	0,05	0,04	0,06	**0,04 Mbps**
	Flash Vídeo	0,02	0,01	0,03	0,02	0,05	**0,02 Mbps**
	QQLive	0,03	0,01	0,03	0,01	0,02	**0,02 Mbps**
	Symantec Live Update	0,01	0,01	0,02	0,02	0,02	**0,01 Mbps**
VoIP	*Skype*	0,07	0,05	0,12	0,14	0,10	**0,09 Mbps**
	UniqueFone	0,00	0,00	0,00	0,00	0,01	**0,00 Mbps**
	SIP RTP	0,04	0,02	0,07	0,08	0,05	**0,05 Mbps**
	SIP	0,01	0,00	0,01	0,01	0,02	**0,01 Mbps**
	H.323 Data	0,00	0,00	0,00	0,00	0,00	**0,00 Mbps**
	Skype In/Out	0,01	0,01	0,02	0,02	0,02	**0,01 Mbps**
	MSN Media Data	0,00	0,00	0,00	0,00	0,00	**0,00 Mbps**
Juegos	*World of Warcraft*	0,00	0,00	0,01	0,01	0,01	**0,01 Mbps**
	Yahoo games	0,00	0,00	0,00	0,00	0,00	**0,00 Mbps**
	Battlefield 2	0,00	0,00	0,00	0,00	0,00	**0,00 Mbps**

Tabla 2.6 Tráfico transmitido promediado por protocolo

Gráficamente, los resultados mostrados en la tabla 2.6 se pueden apreciar en la figura 2.17.

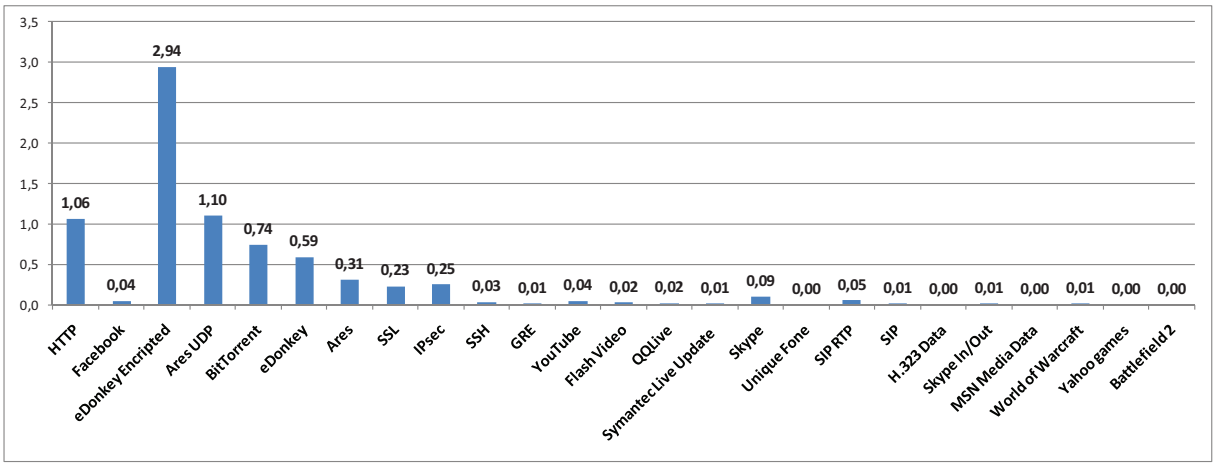

Figura 2.17 Tráfico semanal transmitido por protocolo

De acuerdo a los resultados mostrados en la figura 2.17, las aplicaciones *eDonkey Encripted* y *Ares* UDP del tráfico P2P, y el protocolo HTTP del tráfico de navegación vía web, son los protocolos mayormente usados por el tráfico de salida de la red; los porcentajes son del 32,86%, 12,30% y 11,86% respectivamente en relación al tráfico total transmitido.

2.4 DESCRIPCIÓN DEL TRÁFICO Y REQUERIMIENTOS DE QoS

El tráfico de las aplicaciones debe ser definido para determinar el tipo de información que circula por la red de un ISP y el impacto que pueda llegar a tener sobre la misma. Al describir el tráfico, se puede determinar cuánto ancho de banda se consume en los enlaces, manejar prioridades de tráfico, prevenir periodos de congestión y ataques o implementar políticas de QoS.

Las aplicaciones analizadas anteriormente y otros agregados de tráfico a ser descritos, pueden clasificarse de la siguiente forma:

- Servicios web
- Correo electrónico
- Infraestructura de red
- Terminales
- Seguridad
- *Streaming*

- VoIP
- Bases de datos
- Transferencia de archivos
- P2P

2.4.1 SERVICIOS WEB[6]

Un servicio web es un conjunto de protocolos y estándares que se utilizan para intercambiar datos entre distintas aplicaciones de software, desarrolladas en lenguajes de programación diferentes y ejecutadas sobre cualquier plataforma. Los servicios web son equivalentes a cualquier aplicación que corra en un equipo local, pero la información necesaria para alguna tarea es enviada al servidor y el resultado se devuelve al usuario, ambos en la forma de contenido web.

Se requiere de un navegador web para acceder a este servicio, extraer documentos o páginas web y visualizarlos. Los documentos pueden contener información en formato de texto plano, imágenes, sonidos, animaciones, etc. El usuario puede seguir los hiperenlaces de una página a otros documentos y enviar información al servidor.

2.4.1.1 *HyperText Transfer Protocol* (HTTP)[28][29]

HTTP es un sencillo protocolo cliente/servidor, usado en cada transacción web para articular los intercambios de información entre los clientes web y los servidores HTTP, como se indica en la figura 2.18. Define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web para comunicarse.

Figura 2.18 Funcionamiento del protocolo HTTP[3]

HTTP no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado, por lo que usan los cookies, que son información que un servidor puede almacenar en el cliente.

2.4.1.2 HTTP *Secure* (HTTPS)[30]

HTTPS es el protocolo usado para transacciones seguras en la web. Un mensaje seguro del HTTP es una línea de petición o de estado, seguida por otros encabezados y un cierto contenido. El contenido puede ser información irrelevante, un mensaje seguro del HTTP, o un mensaje del HTTP.

2.4.1.3 *HyperText Transfer Protocol* (HTTP)-*Proxy*[31]

Un HTTP-*Proxy* actúa como un servicio interactivo entre los clientes HTTP (*web browsers*) y los servidores HTTP de los sitios web. Estos proxies almacenan las páginas web para proveer de una respuesta más rápida, y pueden estar bien situados para brindar servicios de metadatos, es decir, incluir cabeceras HTTP con información referente a servicios relacionados.

2.4.1.4 *Facebook*[32]

Facebook es un sitio web de redes sociales, abierto a cualquier persona que tenga una cuenta de correo electrónico. Los usuarios pueden participar en una o más redes sociales, en relación con su situación académica, su lugar de trabajo o región geográfica. Este sitio web ha recibido mucha atención en los medios de comunicación al convertirse en una plataforma sobre la que terceros pueden desarrollar aplicaciones y hacer negocios a partir de la red social. A pesar de ello, existe la preocupación acerca de su posible modelo de negocio, dado que los resultados en publicidad se han revelado como muy pobres.

2.4.1.5 *Nintendo Wii web browsing*[33]

Actualmente, algunos navegadores web incorporan características que les permite convertirse en plataformas para la consola *Nintendo Wii*. Estos

navegadores se manejan utilizando el mando de consola, de forma igual que cualquier videojuego o el sensor de movimiento del mando para desplazarse por las páginas.

2.4.1.6 Requerimientos de QoS[34]

El tráfico de los protocolos de los servicios web no demanda fuertes exigencias en los requerimientos de QoS. En general, usan el ancho de banda restante de los enlaces, con valores de velocidades de transmisión entre 19,2 Kbps y 2 Mbps, retardos entre 0,5 y 60 segundos y son insensibles al *jitter* y a la tasa de paquetes perdidos.

2.4.2 CORREO ELECTRÓNICO[35]

El correo electrónico es un servicio de red que permite a los usuarios enviar y recibir mensajes rápidamente mediante sistemas de comunicación electrónicos. Por medio de los mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales.

Para enviar y recibir correo electrónico hay que estar registrado en alguna empresa, tener una dirección de correo personal única y duradera, un nombre de usuario y una contraseña. Hay varios tipos de proveedores de correo, que se diferencian sobre todo por la calidad del servicio que ofrecen, por lo que se tiene los correos gratuitos y los de pago.

Los correos gratuitos son los más usados, incluyen algo de publicidad y se puede acceder a través de un programa de correo configurado para descargar el correo de forma automática. Una desventaja de estos correos es que cada dirección muestra el nombre del proveedor, lo que da un aspecto menos profesional, por lo que es muy común que las empresas compren un dominio propio.

Los correos de pago consisten en comprar un nombre de dominio e instalar un ordenador-servidor de correo con los programas apropiados. En este tipo de correo no hay que pagar cuotas por el correo, pero sí por el dominio y por los gastos de mantener un ordenador encendido todo el día.

Este servicio utiliza algunos protocolos para transferencia o acceso a los correos electrónicos, como se indica en la figura 2.19.

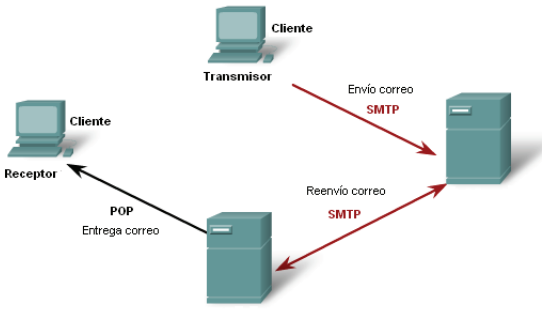

Figura 2.19 Proceso de entrega de correo electrónico[3]

2.4.2.1 *Simple Mail Transfer Protocol* (SMTP)[36]

SMTP es un protocolo de red basado en texto, utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos. Este protocolo se basa en el modelo cliente/servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres ASCII.

2.4.2.2 *Post Office Protocol* 3 (POP3)[37]

POP3 es utilizado por los clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Este protocolo permite a los usuarios con conexiones intermitentes ó muy lentas, descargar su correo mientras tienen conexión y revisarlo posteriormente, incluso desconectados.

Al igual que otros viejos protocolos de Internet, POP3 utilizaba un mecanismo de firmado sin cifrado. En la actualidad, POP3 cuenta con diversos métodos de autenticación que ofrecen una diversa gama de niveles de protección contra los accesos ilegales al buzón de correo de los usuarios.

2.4.2.3 *Internet Message Access Protocol* 4 (IMAP4)[38]

IMAP es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor desde cualquier equipo que tenga una conexión a Internet. Este protocolo es utilizado frecuentemente en redes grandes.

Este protocolo tiene varias ventajas sobre POP3 como visualizar los mensajes de manera remota sin descargarlos, permitir accesos simultáneos a múltiples clientes, vigilar el estado del mensaje y proporcionar mecanismos para que los clientes pidan al servidor que busque mensajes de acuerdo a cierta variedad de criterios.

2.4.2.4 Requerimientos de QoS[34]

El correo electrónico ocupa un ancho de banda alto o bajo, dependiendo del contenido que transmite, mientras que los valores de retardo, *jitter* y tasa de paquetes perdidos que soporta pueden ser altos, respecto a los valores indicados en los requerimientos de QoS del tráfico de los servicios web.

2.4.3 INFRAESTRUCTURA DE RED

La infraestructura de una red comprende las aplicaciones y protocolos utilizados para mantener una red operativa, eficiente, segura, monitoreada y administrada[39].

2.4.3.1 *Domain Name Service* (DNS)[40]

El DNS es un sistema de nombres que permite traducir nombres de dominio a direcciones IP y viceversa, aunque también se puede asociar distintos tipos de información a cada nombre. A pesar de que Internet sólo funciona en base a direcciones IP, el DNS permite que las personas usen nombres de dominio que son bastante más simples de recordar.

El sistema de nombres de dominios es un sistema distribuido, jerárquico, replicado y tolerante a fallas. El punto central se basa en un árbol que define la jerarquía entre los dominios y los subdominios. En un nombre de dominio, la jerarquía se lee de derecha a izquierda. A la etiqueta ubicada más a la derecha se la llama dominio de nivel superior y cada una de las etiquetas a la izquierda especifica un subdominio. Los subdominios exponen el nombre del *host* y especifican la manera de crear una ruta lógica a la información requerida.

2.4.3.2 *Dynamic Host Configuration Protocol* (DHCP)[41]

DHCP es un protocolo de red que asigna direcciones IP dinámicas a los equipos que solicitan y tienen habilitado este servicio. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP que va asignando a los clientes conforme éstas van quedando libres, conociendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Sin DHCP, cada dirección IP debe configurarse manualmente en cada computadora y si la computadora se mueve a otra subred, se debe configurar otra dirección IP diferente. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si la computadora es conectada en un lugar diferente.

2.4.3.3 *Internet Control Message Protocol* (ICMP)[42]

ICMP es un subprotocolo de control y notificación de errores del protocolo IP. No es utilizado directamente por las aplicaciones de usuario en la red; las únicas excepciones son las herramientas *ping* y *traceroute*, que envían mensajes de petición y reciben mensajes de respuesta para determinar si un *host* está disponible, el tiempo que le toma a los paquetes en ir y regresar a ese *host* y la cantidad de *hosts* por los que cruza.

Los mensajes ICMP son construidos en el nivel de capa de red. IP encapsula el mensaje ICMP apropiado con una nueva cabecera IP y transmite el datagrama resultante de manera habitual. Estos mensajes son comúnmente generados en respuesta a errores o para diagnóstico y ruteo, como se muestra en la figura 2.20.

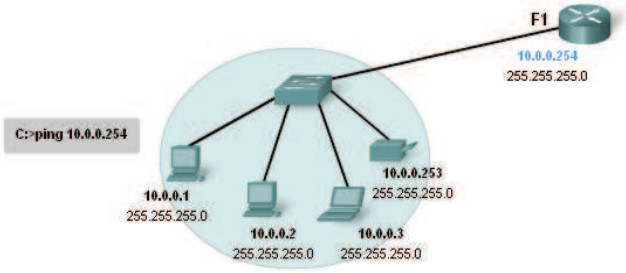

Figura 2.20 Diagnóstico usando el protocolo ICMP[3]

2.4.3.4 *Simple Network Management Protocol* (SNMP)[43]

SNMP es un protocolo de la capa de aplicación del modelo de referencia TCP/IP que facilita el intercambio de información de administración entre dispositivos de red. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas y planear su crecimiento.

Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Ambas versiones tienen un número de características en común, pero SNMPv2 ofrece mejoras significativas como operaciones adicionales. SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad. Sin embargo, no ha sido mayoritariamente aceptado en la industria.

El protocolo SNMP permite obtener los datos a administrar del sistema Agente, que es el dispositivo donde se encuentran, para entregarlos al sistema Administrador (NMS), que es un software que permite administrar. Estos elementos se indican en la figura 2.21.

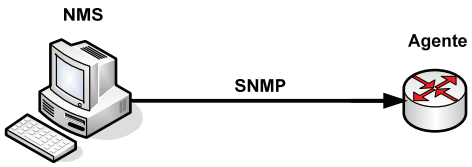

Figura 2.21 Elementos de un sistema administrador

2.4.3.5 Requerimientos de QoS[44]

El tráfico de los protocolos indicados para la infraestructura de una red no requiere gran ancho de banda y es tolerante al *jitter*. Sin embargo, es muy importante que tenga un bajo retardo y una tasa media de paquetes perdidos, debido a que los refrescos en el monitoreo de la red deben ser rápidos para tomar acciones correctivas inmediatas en caso de fallas.

2.4.3.6 Protocolos de enrutamiento

Los protocolos de enrutamiento son utilizados por los *routers* para compartir información de enrutamiento con otros *routers* y conocer sobre cambios en la

topología de la red. Existen varios protocolos de enrutamiento para IP, pero los más utilizados por los ISPs en la actualidad son OSPF, BGP y EIGRP.

2.4.3.6.1 Open Shortest Path First (OSPF)[45]

OSPF es un protocolo de enrutamiento jerárquico utilizado en la parte interna de las redes y que calcula la ruta más corta a cada red de destino mediante el algoritmo de Dijkstra. Su métrica de enrutamiento es el costo de los enlaces, parámetro que se calcula en función del ancho de banda. Además, permite el balanceado de carga entre nodos donde exista más de un camino.

El algoritmo de Dijkstra consiste en ir explorando todos los caminos más cortos que parten de un vértice origen y que llevan a todos los demás vértices que componen un grafo[2]; cuando se obtiene el camino más corto desde el vértice origen al resto de vértices, el algoritmo se detiene.

El protocolo OSPF es probablemente el más utilizado en grandes redes y puede operar con seguridad usando MD5 para autentificar a sus puntos antes de establecer nuevas rutas y aceptar avisos.

2.4.3.6.2 Border Gateway Protocol (BGP)[45]

BGP es un protocolo muy complejo que se usa en la interconexión de redes conectadas por un *backbone* de Internet. Este protocolo usa parámetros como ancho de banda, precio de la conexión, saturación de la red, denegación de paso de paquetes, etc. para enviar un paquete por una ruta o por otra. Un *router* BGP da a conocer sus direcciones IP a los *routers* BGP y esta información se difunde por los *routers* BGP cercanos y no tan cercanos.

BGP es el principal protocolo de publicación de rutas utilizado por las compañías más importantes de ISP en Internet.

---

[2] Un grafo es un conjunto de objetos llamados vértices o nodos unidos por enlaces llamados aristas o arcos, que permiten estudiar las interrelaciones entre unidades que interactúan unas con otras.

2.4.3.6.3 Enhanced Interior Gateway Routing Protocol (EIGRP)[46]

EIGRP es un protocolo de encaminamiento híbrido, propiedad de Cisco Systems. Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Aunque no garantiza la mejor ruta es bastante usado, ya que es algo más fácil de configurar que OSPF.

Los *routers* EIGRP mantienen información de ruta y topología a disposición en la RAM, para que puedan reaccionar rápidamente ante los cambios. Al igual que OSPF, EIGRP guarda esta información en varias tablas y bases de datos. Las rutas reciben un estado y se pueden rotular para proporcionar información adicional de utilidad.

2.4.3.6.4 Requerimientos de QoS[34][44]

El tráfico de los protocolos de enrutamiento no exige una QoS eficiente, ya que no existen valores mínimos o máximos en los parámetros para medir su QoS. Sin embargo, este tráfico permite mantener operativa la red, lo que conlleva a que reciba una QoS mejor a la de “mejor esfuerzo”, de manera que se pueda resolver de forma eficaz los problemas que puedan presentarse en la operación del *backbone* de un ISP.

2.4.4 TERMINALES[47][48]

Los terminales son programas informáticos que actúan como una interfaz de usuario para comunicarlo con el sistema operativo, mediante una ventana que espera órdenes escritas por el usuario en el teclado, las interpreta y entrega al sistema operativo para su ejecución; la respuesta del sistema operativo se muestra al usuario en la misma ventana.

Existen emuladores de terminales que simulan el funcionamiento de un terminal de un ordenador central a través de una red de telecomunicaciones entre dicho ordenador central y el ordenador que ejecuta el emulador de terminal, como es el caso de TELNET y SSH.

2.4.4.1 *TELecommunication NETwork* (TELNET)[49]

TELNET es el nombre de un protocolo que sirve para acceder mediante una red a otra máquina o servidor, para manejarla remotamente como si se estuviera frente a ella. Para que la conexión funcione, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. Los programas cliente se pueden conectar al mismo tiempo al equipo, como se muestra en la figura 2.22, donde uno muy utilizado y popular es el Putty.

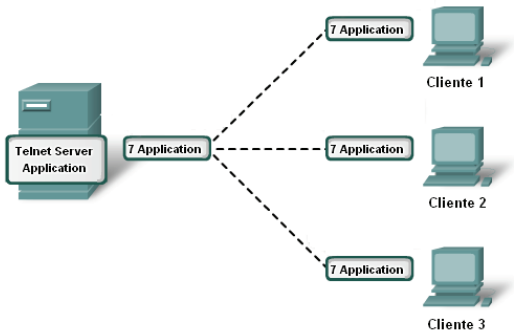

Figura 2.22 Clientes conectándose vía TELNET[3]

Este protocolo es muy seguro y sólo sirve para acceder en modo terminal, pero es una herramienta muy útil para arreglar fallos a distancia. También se usa para consultar datos a distancia, como datos personales en máquinas accesibles por red, información bibliográfica, etc.

2.4.4.2 Secured Shell (SSH)[50]

SSH es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y permitiendo a los usuarios conectarse a un *host* remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o TELNET, SSH encripta la sesión de conexión, haciendo muy difícil que alguien pueda obtener las contraseñas.

2.4.4.3 *Virtual Network Computing* (VNC)[51]

VNC es un programa de software libre basado en una estructura cliente/servidor, que permite tomar el control del ordenador-servidor remotamente a través de un ordenador-cliente. También es llamado software de escritorio remoto. VNC

permite que el sistema operativo en cada computadora sea distinto, de manera que es posible compartir la pantalla de una máquina de cualquier sistema operativo, conectando desde cualquier otro ordenador o dispositivo que disponga de un cliente VNC portado.

2.4.4.4 Requerimientos de QoS[44]

El tráfico de los emuladores de terminales no necesita un gran ancho de banda y es tolerante al *jitter*. Sin embargo, es importante que tenga un bajo retardo y una tasa media de paquetes perdidos, debido a que son usados para acceder a los dispositivos de la red en caso de fallas, las cuales deben ser atendidas de forma inmediata.

2.4.5 SEGURIDAD[52]

El activo más importante en las organizaciones públicas, privadas y de cualquier índole es la información que poseen, ya sea correos electrónicos, información local o mundial, transacciones, etc. La seguridad no es solamente el implementar usuarios y contraseñas, es establecer políticas que garanticen la seguridad tanto física como lógica de la información, asegurando su privacidad y la protección de las operaciones de daños no intencionados o deliberados.

Algunos protocolos del modelo de referencia TCP/IP han sido modificados para ofrecer seguridad de la información que transportan, como es el caso de IPsec.

2.4.5.1 IP *Security* (IPsec)[53][54]

IPsec es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el protocolo IP autenticando y/o cifrando cada paquete IP en un flujo de datos. Además, incluye protocolos para el establecimiento de claves de cifrado.

Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de capa 4, incluyendo TCP y UDP.

IPsec emplea dos protocolos diferentes, AH y ESP, para asegurar la autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores. Estos modos se denominan como modo túnel y modo transporte respectivamente.

2.4.5.2 *Generic Routing Encapsulation* (GRE)[55]

El protocolo GRE es utilizado para encapsular un paquete determinado dentro de un protocolo de transporte, creando túneles entre clientes o entre clientes y servidores. GRE no ocupa el puerto 47 de TCP ni de UDP sino que va directamente sobre IP; es decir, GRE es el protocolo número 47 de IP al igual que TCP es el número 6 de IP y UDP el número 17 de IP, pero GRE no va sobre TCP ni sobre UDP sino que va directamente sobre IP.

2.4.5.3 *Layer* 2 *Tunneling Protocol* (L2TP)[56][57]

L2TP es un protocolo de tunelización usado para soportar VPNs. Este protocolo no provee de ninguna encriptación o confidencialidad por sí mismo, sino que confía en el protocolo de encriptación usado a lo largo del túnel para proveer privacidad. A pesar de que actúa como un protocolo de capa 2, L2TP es en sí un protocolo de capa 5.

El protocolo L2TP utiliza *Point-to-Point* (PPP) para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. Además, define su propio protocolo de establecimiento de túneles y el transporte está definido para una gran variedad de tipos de paquete, incluyendo X.25, *Frame Relay* y ATM.

2.4.5.4 Requerimientos de QoS[34]

El tráfico de los protocolos para proveer seguridad a la información requiere velocidades de transmisión entre 1,2 y 9,6 Kbps, con retardos bajos entre 0,5 y 2 segundos, siendo tolerante al *jitter* y sensible a la tasa de paquetes perdidos, debido a lo delicado de la información que transporta.

2.4.6 *STREAMING*[58]

La tecnología *streaming* se utiliza para aligerar la descarga y ejecución de audio y vídeo en la web, ya que permite escuchar y visualizar los archivos mientras se están descargando. Al no utilizarla, para mostrar un contenido multimedia en la red, habrá que descargar primero el archivo entero al ordenador para ejecutarlo, con el fin de ver y escuchar lo que el archivo contiene.

2.4.6.1 *RealAudio*[59]

RealAudio es un formato de audio utilizado para transmisiones por Internet en tiempo real, es decir que una estación de radio puede transmitir su señal en vivo, directamente al usuario final, sin necesidad de generar primero el archivo de audio. O bien, el usuario puede escuchar, bajo demanda, un archivo almacenado en un servidor externo. En ambos casos, el archivo de audio no se descarga en el ordenador del usuario final. La reproducción se realiza mediante "paquetes" que el servidor envía al usuario. Cada "paquete" de audio es reproducido mientras que se recibe otro que lo sustituye en una carpeta temporal.

2.4.6.2 Vídeo[6]

La utilización de las redes para la transmisión de vídeo ha tenido un crecimiento masivo, ya que el Internet se utiliza para muchos fines como ver películas, descargar vídeos, enseñanza remota, televisión, etc.

A pesar de que las señales de vídeo son de naturaleza analógica, se pueden transmitir de forma digital con grandes ventajas como mayor fiabilidad, mecanismos de detección de errores, inmunidad a interferencias y ruido, mejor codificación y encriptado, etc. Los avances en la tecnología han permitido capturar, digitalizar, secuenciar y transmitir señales compuestas de vídeo y voz sobre Internet; la señal procesada y comprimida se almacena en un servidor de vídeo para luego enviarla a través de la red.

Existen tres tipos de vídeo sobre IP:

- **Vídeo *broadcast* sobre IP:** Consiste en la transmisión de un archivo con contenido de vídeo hacia ciertos puntos de la red. La transmisión es unidireccional, es decir los puntos de destino son visualizadores pasivos y no tienen ningún tipo de control en la sesión. Los vídeos pueden ser en tiempo real o pregrabados.
- **Vídeo bajo demanda sobre IP (VoD):** VoD sobre IP es un servicio que permite a un usuario seleccionar y ver el contenido de un vídeo almacenado en un servidor de red. Es diferente del vídeo *broadcast* porque se trata de un vídeo interactivo, en donde el usuario puede visualizar a tiempo real o iniciar y suspender un vídeo almacenado en un servidor central de vídeo.
- **Videoconferencia:** El servicio de videoconferencia sobre IP combina transmisiones full dúplex tanto de vídeo como de audio, permitiendo que usuarios ubicados en distintos puntos geográficos puedan verse y escucharse como si estuvieran en el mismo lugar. El abaratamiento y disponibilidad de los equipos y servicios de videoconferencia han ocasionado que esta industria sea de gran crecimiento en el mercado de teleconferencias.

2.4.6.2.1 Real Time Streaming Protocol (RTSP)[60]

El protocolo RTSP establece y controla uno o muchos flujos sincronizados de datos, ya sean de audio o de vídeo. RTSP actúa como un mando a distancia mediante la red para servidores multimedia. De forma intencionada, el protocolo es similar en sintaxis y operación a HTTP de forma que los mecanismos de expansión añadidos a HTTP pueden, en muchos casos, añadirse a RTSP.

RTSP es un protocolo no orientado a conexión, en lugar de esto el servidor mantiene una sesión asociada a un identificador. En la mayoría de los casos, RTSP usa TCP para datos de control del reproductor y UDP para los datos de audio y vídeo, aunque también puede usar TCP en caso de que sea necesario.

2.4.6.2.2 Real-Time Transport Protocol (RTP)[4]

RTP proporciona servicios de transporte extremo a extremo para aplicaciones que requieran transmisión en tiempo real a través de redes de paquetes; puede ser utilizado para vídeo bajo demanda (VoD), videoconferencia, telefonía IP u otros servicios. RTP incluye características como identificación del tipo de dato, secuenciamiento y marca de tiempo. RTP se encarga de entregar los paquetes en secuencia de forma que la información puede ser reconstruida por el receptor, mientras que la marca de tiempo permite la sincronización de la voz y/o el vídeo.

RTP se ejecuta normalmente sobre el protocolo UDP, pero puede igualmente funcionar sobre otros protocolos de transporte. Es usado frecuentemente junto a *Real Time Streaming Protocol* (RTSP), videoconferencia y H.323.

2.4.6.2.3 QQLive[61]

QQLive es un nuevo tipo de software para ver televisión en línea, diseñado por una corporación china y mayormente usado en ese mismo país. Se caracteriza porque los usuarios tienen preferencia en cargar más rápido los programas, es de fácil configuración y requiere acceso a Internet de banda ancha.

2.4.6.2.4 YouTube[62]

YouTube es un sitio web que permite a los usuarios compartir vídeos digitales a través de Internet, usando un reproductor en línea basado en Adobe Flash para servir su contenido. Este sitio aloja una variedad de clips de películas, programas de televisión, vídeos musicales y vídeos caseros. Los enlaces a vídeos de *YouTube* pueden ser también puestos en *blogs* y sitios web personales usando APIs o incrustando cierto código HTML.

2.4.6.2.5 Flash Video (FLV)[63]

FLV es un formato de archivo propietario usado para transmitir video sobre Internet usando Adobe Flash Player. Entre los sitios más notables que utilizan el formato FLV se encuentran *YouTube*, *Google Video*, *Yahoo! Video* y *MySpace*.

2.4.6.2.6 Symantec Live Update[64][65]

Symantec está proporcionando *streaming* de aplicaciones bajo demanda, optimizando el despliegue del software y la gestión de licencias, reduciendo así los costos de infraestructura. El *streaming* de aplicaciones es una forma de distribución de software bajo demanda, cuyo concepto básico tiene su fundamento en la forma moderna de los lenguajes de programación y sistemas operativos que producen y ejecutan el código de las aplicaciones. Sólo partes específicas de un programa computacional necesitan estar disponibles en cualquier momento para que el usuario final pueda realizar una función en particular, lo que significa que un programa no tiene porque ser plenamente instalado en un equipo cliente, pero si partes del mismo pueden ser prestadas a través de un bajo ancho de banda a medida que se requieren.

2.4.6.2.7 Requerimientos de QoS[34][44]

El tráfico *streaming* tiene fuertes requerimientos en cuanto a QoS se refiere, ya que exige un ancho de banda asegurado de extremo a extremo, con valores de retardo, *jitter* y tasa de paquetes perdidos muy bajos.

El vídeo sobre IP requiere velocidades de transmisión entre 33,6 Kbps y 34 Mbps, retardos entre 0,5 y 5 segundos y es sensible al *jitter* y a la tasa de paquetes perdidos.

El vídeo *broadcast* sobre IP requiere un ancho de banda alto, valores de retardo medios a altos, bajo *jitter* y es sensible a la tasa de paquetes perdidos.

El VoD requiere un ancho de banda alto, valores de retardo, *jitter* y tasa de paquetes perdidos bajos.

La videoconferencia necesita una velocidad mínima de transmisión de 128 Kbps, retardo menor a 0,5 segundos y es sensible al *jitter* y a la tasa de paquetes perdidos.

2.4.7 VoIP[6]

Este servicio consiste en aprovechar la infraestructura de Internet para la transmisión de voz mediante la utilización del protocolo IP. El gran crecimiento de las redes IP en Internet, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real y nuevos estándares de QoS, han creado el entorno adecuado para la transmisión de voz sobre IP.

Con la integración de tecnologías que permiten convergencia de redes de voz y datos en los mismos *routers* que controlan el tráfico a través de Internet, la "telefonía IP" se ha convertido en "comunicación IP", unificando telefonía, correo de voz, *e-mail*, servicios de datos, aplicaciones empresariales y videoconferencia a través de un teléfono IP.

2.4.7.1 H.323[66]

H.323 define los protocolos para proveer sesiones de comunicación audiovisual sobre paquetes de red. Es utilizado comúnmente para VoIP y videoconferencia basada en IP.

Esta recomendación es un conjunto de normas ITU para comunicaciones multimedia que hacen referencia a los terminales, equipos y servicios, estableciendo una señalización en redes IP. No garantiza calidad de servicio y en el transporte de datos puede o no ser fiable; en el caso de voz o vídeo, nunca es fiable. Además, es independiente de la topología de la red y admite pasarelas, permitiendo usar más de un canal de cada tipo (voz, vídeo o datos) al mismo tiempo.

2.4.7.2 H.225[67]

H.225 es un protocolo clave en la arquitectura de VoIP H.323. Este protocolo define la manera en que puede gestionarse el audio, video, datos e información de control en una red basada en paquetes para proveer servicios de conversación con equipos H.323.

2.4.7.3 *Session Initiation Protocol* (SIP)[68]

SIP es un protocolo desarrollado con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos *online* y realidad virtual.

La sintaxis de sus operaciones se asemeja a las de HTTP y SMTP, los protocolos utilizados en los servicios de páginas web y de distribución de correos electrónicos respectivamente. Esta similitud es natural ya que SIP fue diseñado para que la telefonía se vuelva un servicio más en Internet.

2.4.7.4 *Net2Phone*[69]

Existen varios programas que permiten la comunicación por voz, e inclusive por video, utilizando las bondades ahorrativas del Internet. Sin embargo, requieren que ambos usuarios, el que origina la llamada y el que la recibe, tengan Internet, computadora multimedia, estén conectados al mismo tiempo, en el mismo lugar y "corriendo" el mismo programa de comunicación; es decir, lo único que realmente hacen es una aplicación de chat o conversación en línea pero con voz.

A diferencia de estos programas, *Net2Phone* permite a los usuarios realizar llamadas telefónicas de alta calidad a bajos costos desde sus computadoras a cualquier teléfono convencional del mundo, evitando la necesidad de que el interlocutor esté conectado a Internet o disponga de un ordenador.

2.4.7.5 *Skype*[70]

Skype es un programa que permite a sus usuarios realizar llamadas a otros usuarios en cualquier lugar del mundo. Cuenta con opciones como videollamadas y chat; sumado a lo anterior y pagando una tarifa muy económica, los usuarios pueden realizar llamadas a teléfonos fijos y móviles alrededor del mundo.

La aplicación también incluye una característica denominada *Skype Out* que permite a los usuarios llamar a teléfonos convencionales, cobrando diversas tarifas según el país de destino. Otra opción que brinda *Skype* es *Skype In*,

gracias al cual se otorga un número de teléfono para que desde un aparato telefónico en cualquier parte del mundo se pueda contactar a un ordenador en particular. Además, proveen de un servicio de buzón de voz gratuito.

2.4.7.6 *UniqueFone*[71]

UniqueFone es un servicio de teléfono único que funciona tanto en la *WirelessLAN* del hogar como en una red celular fuera de casa. El servicio significa que las llamadas telefónicas dentro de la casa a otros fijos y móviles serán gratuitas, ya que operan en VoIP. Además, se tiene una simplificación en relación con el servicio telefónico, ya que el plan ofrece un teléfono, un número, una libreta de direcciones y una factura.

2.4.7.7 *Time Division Multiplexing over* IP (TDMoIP)[72]

TDMoIP es una tecnología de transporte que encapsula tramas TDM dentro de paquetes, ampliando las aplicaciones tradicionales de voz, datos y vídeo de forma transparente sobre infraestructuras de red IP, *Ethernet* o MPLS. Para aplicaciones de voz, TDMoIP soporta PBX tradicionales; además, soporta cualquier señalización, varios protocolos de comunicación y todas las velocidades de módem y fax disponibles, así como varios estándares de vídeo sobre IP.

Los *gateways* para TDMoIP reciben una trama de datos en sus interfaces T1/E1 o de voz analógica, las cuales son cortadas en paquetes de tamaño fijo y se les asigna una cabecera IP. Luego los paquetes son transmitidos sobre la red IP hacia el *gateway* del extremo receptor. El *gateway* receptor reconstruye la trama de datos original, quitando la cabecera IP, concatenando los paquetes y regenerando los relojes. Luego la trama es traspasada a su destino, donde es entregada al interfaz estándar T1/E1 o de voz analógica. Este proceso se indica en la figura 2.23.

Figura 2.23 Funcionamiento de TDMoIP[73]

Existen dos variantes de TDMoIP que son Emulación de Circuitos (CE) y Compresión de Voz (CV).

La emulación de circuitos en TDMoIP permite emular circuitos T1/E1 o T3/E3 sobre redes IP, *Ethernet* o MPLS. Esta tecnología es ideal cuando se requiere una baja latencia, alta calidad en la voz, vídeo y datos sobre IP. Los paquetes que se transportan por la red poseen alta prioridad y una estricta QoS para asegurar circuitos TDM libres de errores.

La compresión de voz en TDMoIP es utilizada para transparentar la voz, ya que posee la mayoría de sus características, con un transporte transparente de señalización que utiliza menor ancho de banda y es más tolerante a la pérdida de paquetes.

Además de su versatilidad, TDMoIP es más sencillo y menos costoso que la VoIP. Ambos servicios ofrecen convergencia, lo cual es la combinación de dos o más disciplinas o tecnologías dispares como el envío de voz y datos dentro de una única red. Sin embargo, hay diferencias que otorgan ventajas a TDMoIP como:

TDMoIP utiliza tecnologías estándar maduras como T1/E1 e IP; en cambio, la VoIP se mueve alrededor de nuevos y emergentes protocolos tales como H.323. Durante el tiempo que un equipo aprende un grupo de protocolos nuevos, se tiene que invertir más dinero para que puedan aprender el siguiente grupo de normas.

Con TDMoIP, el tamaño de los paquetes es configurable, a diferencia de la VoIP que depende de los estándares, los cuales a su vez incluyen más retardos a cada sesión de voz.

Como se mencionó anteriormente, tanto TDMoIP como la VoIP proporcionan convergencia para reducir los costos de administración, cableado y hardware. Sin embargo, la VoIP es más compleja para aplicaciones de conmutación de voz, en

donde TDMoIP tiene un papel mucho más importante debido a que transporta cualquier señal de voz, vídeo y datos basados en TDM sobre IP, lo cual protege las inversiones.

2.4.7.8 Requerimientos de QoS[34][44][74]

La VoIP necesita velocidades de transmisión entre 4 y 16 Kbps, retardos menores a 0,5 segundos y es sensible al *jitter* y al número de paquetes perdidos. Sin embargo, estos parámetros pueden variar dependiendo de la calidad ofrecida, como se indica en la tabla 2.7 los valores máximos para cada unos de ellos.

Parámetros de QoS	Calidad alta	Calidad media	Calidad baja
Retardo	150 ms	400 ms	600 ms
Jitter	20 ms	50 ms	75 ms
Tasa de paquetes perdidos	1%	3%	5%

Tabla 2.7 Parámetros de QoS para VoIP dependiendo de la calidad

La tecnología TDMoIP tiene sus propios requerimientos de QoS para las dos variantes que posee. La tabla 2.8 indica los valores máximos de los parámetros de QoS exigidos para CE en TDMoIP y CV en TDMoIP.

Parámetros de QoS	CE en TDMoIP	CV en TDMoIP
Velocidad de transmisión	74 Kbps	3,8 Kbps
Retardo	3 ms	45 ms
Jitter	20 ms	20 ms
Tasa de paquetes perdidos	Baja	Alta

Tabla 2.8 Parámetros de QoS para TDMoIP

2.4.8 BASES DE DATOS[75]

Una base de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En la actualidad, la mayoría de bases de datos están en formato digital debido al desarrollo tecnológico, ofreciendo un amplio rango de soluciones al problema de almacenar datos.

Las aplicaciones más usuales de las bases de datos son para la gestión de empresas e instituciones públicas como bancos, supermercados, registros, etc. La mayoría de información que almacenan de las instituciones es delicada y confidencial, por lo que se encuentra protegida por las leyes del estado y a su vez, por la seguridad que se debe ofrecer durante su transmisión.

Existen programas denominados Sistemas Gestores de Bases de Datos (SGBD), que permiten almacenar y posteriormente acceder a los datos de forma rápida y estructurada. Algunos de los SGBDs más utilizados en la actualidad son Microsoft SQL *Server*, *Oracle* y MySQL

2.4.8.1 Requerimientos de QoS[34]

El tráfico correspondiente a las bases de datos tiene prioridades de QoS debido al acceso de múltiples clientes a la información de las organizaciones. Este tráfico requiere velocidades de transmisión entre 1,2 y 9,6 Kbps, bajos retardos entre 0,5 y 2 segundos, siendo tolerante al *jitter* y sensible a la tasa de paquetes perdidos.

2.4.9 TRANSFERENCIA DE ARCHIVOS[76]

La transferencia de archivos es un término genérico para referirse al acto de transmisión de ficheros a través de una red informática. Un protocolo para la transferencia de archivos es una convención o una norma que controla o permite la transferencia de archivos entre dos computadoras. Su objetivo únicamente es enviar la secuencia de bits almacenado como una sola unidad en un sistema de ficheros con todos los metadatos como el nombre del archivo, el tamaño del archivo, la fecha y la hora.

2.4.9.1 *Network File System* (NFS)[77][78]

NFS es un servicio que permite a una o varias máquinas de una red compartir uno o varios directorios que se encuentran en una máquina principal llamada servidor. Usando NFS, los usuarios y los programas pueden acceder a archivos en sistemas remotos como si se tratase de su propia máquina. El ingreso en los directorios no significa que se pueda modificarlos, borrarlos o leerlos, ya que el administrador del servidor puede configurar y restringir ciertas posibilidades a sus clientes.

Este servicio permite a las estaciones de trabajo locales utilizar menos espacio en disco, debido a que los datos usados de forma común pueden ser guardados en una sola máquina y permanecer accesibles a toda la red.

2.4.9.2 *File Transfer Protocol* (FTP)[79]

FTP es un protocolo de red para la transferencia de archivos entre computadores dentro de una red, basado en la arquitectura cliente/servidor. Desde un equipo cliente haciendo uso de un nombre de usuario y una contraseña se puede conectar a un servidor para descargar archivos o para enviarlos, independientemente del sistema operativo utilizado en ese equipo.

Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información no tiene ningún tipo de cifrado, con lo que un posible atacante puede capturar ese tráfico, acceder al servidor o apropiarse de los archivos transferidos.

2.4.9.3 *Secure* FTP (SFTP)[80]

El protocolo de transferencia de archivos SFTP es un protocolo de red que proporciona la transferencia de archivos y la funcionalidad de manipulación de datos fiables sobre cualquier secuencia, ya que los datos circulan cifrados por la red. Los programas de SFTP ofrecen una interfaz interactiva similar a la de los tradicionales programas de FTP para interactuar con el cliente.

El protocolo SFTP en sí no facilita la autenticación y la seguridad, sino que espera que el protocolo subyacente lo asegure. Es utilizado frecuentemente como subsistema del protocolo SSH. Sin embargo, es posible ejecutarlo a través de SSH o de otros flujos de datos.

2.4.9.4 *System Logging Utility* (Syslog)[81]

Syslog es un sistema de logs que se encarga principalmente de su administración, los cuales son generados por eventos del sistema sucedidos sobre un dispositivo o servicio, sobre sus programas o por el Kernel. Para lograr capturar y administrar los logs que se generan permanentemente sin ningún aviso, syslog utiliza un demonio que se encarga de capturar cualquier *log* generado.

2.4.9.5 Requerimientos de QoS[34]

El tráfico para la transferencia de archivos requiere valores de ancho de banda medios a altos y puede soportar valores de retardo, *jitter* y tasa de paquetes perdidos altos, con respecto a los requerimientos de QoS para los servicios web.

2.4.10 *PEER-TO-PEER* (P2P)[82][83][84]

Una red informática P2P se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores respecto de los demás nodos de la red, con el fin de compartir archivos que contienen audio, video, texto, software y datos en cualquier formato digital. Cualquier nodo puede iniciar, detener o completar una transacción compatible. La eficacia de los nodos en el enlace y transmisión de datos puede variar según su configuración local, velocidad de proceso, disponibilidad de ancho de banda de su conexión a la red y capacidad de almacenamiento en disco.

El tráfico P2P, que es conocido por ser el que se emplea para descargar los archivos de las redes P2P, utiliza muchos programas que circulan por Internet

como *Ares*, *BitTorrent*, *Gnutella*, *Rapidshare*, entre otros. Este tráfico impacta a los ISPs en tres aspectos que son:

- Incrementando los costos de ancho de banda de la conexión a Internet, los que, debido a los modelos de precios existentes, no pueden ser transferidos a los clientes.
- Incrementando los costos de infraestructura asociados a los altos volúmenes y a la simetría de tráfico P2P.
- Aumentando la congestión en horarios pico la que, si no es adecuadamente resuelta, desembocará en una alta rotación de clientes

P2P consume gran cantidad de ancho de banda (demostrado por los porcentajes que presenta en el tráfico transmitido y recibido durante el análisis de tráfico), ya que existen muchísimos usuarios y conexiones simultáneas. Esto genera una especie de "tormentas de datos" en los accesos a Internet que llegan a saturar los canales de transmisión. Debido a este motivo, los ISPs limitan el tráfico de este tipo analizando el tipo de "paquetes de datos" que circulan por sus líneas. Si un usuario está enviando o recibiendo muchos paquetes de tipo P2P, se rechaza una cantidad por encima de un límite que la propia operadora determina.

2.4.10.1 Ventajas del tráfico P2P

En el modelo cliente/servidor, todos los usuarios tratan de descargar el mismo archivo de la misma máquina, lo cual conduce a una rápida saturación de las líneas. La capacidad de la red se desaprovecha y además, si el servidor se desconecta, todos los clientes se quedan sin servicio.

Mientras tanto que, en el modelo P2P, cuando varios usuarios se descargan un archivo, crean una copia local en su ordenador, por lo que otros equipos tratan de descargar trozos del archivo de sus vecinos más cercanos. Como están más cerca, el ancho de banda medio es mayor y cada cliente actúa al mismo tiempo como servidor, por lo que la transmisión es más rápida y el rendimiento total de la red es muy superior.

Cada día más y más usuarios de Internet descubren el tráfico P2P como una manera económica de acceder a una gran cantidad de información y contenidos como música, vídeos, documentos y programas de ordenador.

2.4.10.2 Controversia legal

Aunque las redes P2P pueden ser empleadas para compartir materiales de propiedad de los propios usuarios, no protegidos por derechos de autor o susceptibles de libre difusión, lo más frecuente es que se usen para intercambiar archivos con material protegido por derechos de propiedad intelectual ajenos, cuyos titulares pueden no desear que ese material sea distribuido a través de este medio.

Las leyes en materia de propiedad intelectual y derechos de autor, dan el derecho al titular de exigir que se ponga fin a la distribución de su material y a reclamar una indemnización por violación a sus derechos como autor.

Esto ha llevado a que la mayor parte de las empresas discográficas y distribuidoras y algunos defensores del sistema P2P, concluyan que estas redes suponen una gran amenaza a los modelos empresariales ya establecidos, aunque recientemente, algunas de estas compañías han optado por levantar servicios basados en esta tecnología. Además, debe tenerse en cuenta que existen aplicaciones específicas de redes P2P directamente orientadas al intercambio de este tipo de contenidos y obras, como por ejemplo *Skype*, VoIP o *Hello* de *Picasa*.

2.4.10.3 Requerimientos de QoS

El tráfico P2P forma parte del tráfico de “mejor esfuerzo” que no supone ningún tipo de requerimiento de QoS, llegando incluso a que los ISPs limiten este tipo de tráfico por las razones expuestas anteriormente.

REFERENCIAS CAPÍTULO 2

LIBROS Y MANUALES

[1] JIMÉNEZ, María Soledad. Folleto de comunicación digital. EPN. Marzo 2005

[2] CISCO SYSTEMS. Curriculum CCNA exploration 4.0: Accessing the WAN

[3] CISCO SYSTEMS. Curriculum CCNA exploration 4.0: Network fundamentals

[4] PARNELL, Teré. "Guía de redes de alta velocidad". 2da edición. Mc Graw Hill. Madrid. 2001

PROYECTOS DE TITULACIÓN

[5] CHÁVEZ, Diego; MONTERO, Silvana. "Diseño para la migración de la red de SETEL hacia un carrier que utiliza tecnología MPLS, para proveer servicios de VoIP en todo el Distrito Metropolitano de Quito". EPN. Marzo 2008

[6] GUANÍN, Francisco; GUERRERO, Raúl. "Determinación de parámetros que intervienen en la calidad del servicio prestado por Proveedores de Servicios de Internet (ISP) nacionales y análisis del ISP más conveniente en relación costos-beneficios para el cliente". EPN. Agosto 2006

[7] RACINES, Paola. "Diseño de un ISP considerando criterios de calidad de servicio para la transmisión de voz, datos y vídeo utilizando el estándar IEEE 802.16 (WiMax) para cubrir el área norte de la ciudad de Quito". EPN. Octubre 2007

[8] PADILLA, René; URQUIZA, Luis. "Rediseño de la red WAN de Petrocomercial con calidad de servicio". EPN. Enero 2008

ARTÍCULOS E INTERNET

[9] ECMWARE. "ISP (Proveedor de Servicios de Internet)"
http://www.ecmware.com/isp_proveedor_de_servicios_de_internet_.html

[10] ANÓNIMO. "Tier 1"
http://es.wikipedia.org/wiki/Tier_1

[11] ANÓNIMO. "El modelo jerárquico de tres capas de CISCO"
http://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

[12] ANÓNIMO. “Introducción informática”
http://webs.um.es/barzana/II/Ii09.html
[13] ANÓNIMO. “Cables”
http://radio.grupohg.es/tienda/index.php?main_page=index&cPath=15
[14] MARIANA. “La mayor velocidad de transmisión de datos por fibra óptica”
http://www.somospc.com/mayor-velocidad-de-transmision-de-datos-por-fibra
[15] ANÓNIMO. “Conexión por línea conmutada”
http://es.wikipedia.org/wiki/Conexi%C3%B3n_por_l%C3%ADnea_conmutada
[16] ALEGSA. “Tipos de conexiones a Internet”
http://www.alegsa.com.ar/Notas/135.php
[17] ANÓNIMO. “Asymmetric Digital Subscriber Line”
http://es.wikipedia.org/wiki/ADSL
[18] ANÓNIMO. “SDSL”
http://es.wikipedia.org/wiki/SDSL
[19] SEGURA, Ignacio. “Nuevas tecnologías para el acceso a Internet”
http://www.inegi.gob.mx/inegi/ciberhabitat/museo/estreno/cablemodem.htm
[20] ANÓNIMO. “Power Line Communications”
http://es.wikipedia.org/wiki/BPL
[21] ANÓNIMO. “Cacti”
http://es.wikipedia.org/wiki/Cacti
[22] CACTI. “Cacti, the complete rrdtool-based graphing solution”
http://cacti.net
[23] SANDVINE. “Sandvine incorporated: Intelligent broadband netwoks”
http://sandvine.com
[24] ANÓNIMO. “Web browser”
http://en.wikipedia.org/wiki/Web_browser
[25] ANÓNIMO. “Peer-to-peer”
http://es.wikipedia.org/wiki/Caracteristicas_p2p
[26] ANÓNIMO. “Tunneling”
http://es.wikipedia.org/wiki/Tunneling
[27] ANÓNIMO. “Streaming”
http://es.wikipedia.org/wiki/Buffer%C3%A9o
[28] ANÓNIMO. “El protocol HTTP”

http://neo.lcc.uma.es/evirtual/cdd/tutorial/aplicacion/http.html

[29] ANÓNIMO. “Hypertext Transfer Protocol”
http://es.wikipedia.org/wiki/HTTP

[30] ANÓNIMO. “Secure Hypertext Transfer Protocol”
http://es.wikipedia.org/wiki/Secure_Hypertext_Transfer_Protocol

[31] ANÓNIMO. “Secure Hypertext Transfer Protocol”
http://www.desire.org/html/research/deliverables/D3.1/qualratings/glossary.htm

[32] ANÓNIMO. “Facebook”
http://es.wikipedia.org/wiki/Facebook

[33] ANÓNIMO. “Opera (navegador)”.
http://es.wikipedia.org/wiki/Opera_(navegador)

[34] ANÓNIMO. “QoS”.
http://www2.ing.puc.cl/~iee3542/amplif_4.ppt

[35] ANÓNIMO. “Correo electrónico”
http://es.wikipedia.org/wiki/Correo_electr%C3%B3nico

[36] ANÓNIMO. “Definición de SNMP”
http://support.microsoft.com/kb/87022/es

[37] ANÓNIMO. “Post Office Protocol”
http://es.wikipedia.org/wiki/APOP

[38] ANÓNIMO. “Internet Message Access Protocol”
http://es.wikipedia.org/wiki/IMAP

[39] AGUILAR, VICTORIA. “Administración de redes”
http://www.monografias.com/administracion-redes/administracion-redes.shtml

[40] PIQUER, José. “El DNS”
http://www.dcc.uchile.cl/~jpiquer/Internet/DNS/node2.html

[41] ANÓNIMO. “Dynamic Host Configuration Protocol”
http://es.wikipedia.org/wiki/DHCP

[42] ANÓNIMO. “Internet Control Message Protocol”
http://es.wikipedia.org/wiki/ICMP

[43] ANÓNIMO. “Simple Network Management Protocol”
http://es.wikipedia.org/wiki/SNMP

[44] IBARRA, Edwin. “MPLS y Calidad de Servicio en las redes IP”.
http://www.tecnologicoamper.com/descargas/seminario01CC.pdf

[45] ANÓNIMO. “Protocolos RIP/OSPF/BGP”
http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/protocols.html
[46] ANÓNIMO. “EIGRP”
http://es.wikipedia.org/wiki/EIGRP
[47] ANÓNIMO. “Linea de comandos”
http://es.wikipedia.org/wiki/Terminal_(aplicación)
[48] ANÓNIMO. “Emulador de terminal”
http://es.wikipedia.org/wiki/Emulador_de_terminal
[49] ANÓNIMO. “Telnet”
http://es.wikipedia.org/wiki/Telnet
[50] ANÓNIMO. “Capítulo 20. Protocolo SSH”
http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html
[51] ANÓNIMO. “VNC”
http://es.wikipedia.org/wiki/Virtual_Network_Computing
[52] ARÁMBULA, Jesús. “Seguridad en redes de computadores”
http://www.monografias.com/trabajos30/seguridad-redes/seguridad-redes.shtml
[53] ANÓNIMO. “IPsec”
http://es.wikipedia.org/wiki/IPsec
[54] ANÓNIMO. “¿Qué es IPsec?”
http://www.ipsec-howto.org/spanish/x161.html
[55] ANÓNIMO. “Redirección protocolo GRE cisco 827”
http://www.todoexpertos.com/respuestas/redireccion-protocolo-gre-cisco-827
[56] ANÓNIMO. “Layer 2 Tunneling Protocol”
http://en.wikipedia.org/wiki/L2TP
[57] ANÓNIMO. “L2TP”
http://es.wikipedia.org/wiki/L2TP
[58] ALVAREZ, Miguel Ángel. “Qué es streaming”
http://www.desarrolloweb.com/articulos/482.php
[59] ANÓNIMO. “RealAudio”
http://es.wikipedia.org/wiki/RealAudio
[60] ANÓNIMO. “RTSP”
http://es.wikipedia.org/wiki/RTSP
[61] ANÓNIMO. “QQLive”

http://www.streamingstar.com/NetworkResource/qqlive.htm

[62] ANÓNIMO. “YouTube”
http://es.wikipedia.org/wiki/YouTube

[63] ANÓNIMO. “Flash Video”
http://es.wikipedia.org/wiki/Flash_Video

[64] ANÓNIMO. “Symantec transforma la gestión con la virtualización”
http://www.symantec.com/es/es/about/news/release/article.jsp?prid=20090

[65] ANÓNIMO. “Application streaming”
http://en.wikipedia.org/wiki/Application_streaming

[66] ANÓNIMO. “H.323”
http://es.wikipedia.org/wiki/H.323

[67] PEDRA, Marcelo. “H.225”
http://www.marcelopedra.com.ar/glosario_H.htm

[68] ANÓNIMO. “Session Initiation Protocol”
http://es.wikipedia.org/wiki/Session_Initiation_Protocol

[69] ANÓNIMO. “¿Qué es la telefonía IP?”
http://www.configurarequipos.com/doc77.html

[70] ANÓNIMO. “Skype”
http://es.wikipedia.org/wiki/Skype

[71] MAITLAND, Ambar. “Servicio de VoIP móvil y llama desde un teléfono”
http://www.pocket-lint.com/news/news.phtml?newsId=4880

[72] VILCO. “Multiplexación por división del tiempo sobre Protocolo Internet”
http://www.vilco.cl/index.php?option=com_content&task=view&id=30&Itemid=27

[72] ANÓNIMO. “TDMoIP”
www.aslan.es/n04/foros04/solucionesip/presentaciones/represa.ppt

[74] ATICA. “QoS en telefonía IP”
http://www.um.es/atica/qos-en-telefonia-ip

[75] ANÓNIMO. “Bases de datos”
http://es.wikipedia.org/wiki/Bases_de_Datos

[76] ANÓNIMO. “Transferencia de archivos”
http://es.wikipedia.org/wiki/Transferencia_de_archivos

[77] ANÓNIMO. “Definición de Network File System”
http://www.alegsa.com.ar/Dic/network%20file%20system.php

[78] ANÓNIMO. “Network File System”
http://doc.ubuntu-es.org/Network_File_System
[79] ANÓNIMO. “File Transfer Protocol”
http://es.wikipedia.org/wiki/File_Transfer_Protocol
[80] ANÓNIMO. “SFTP”
http://es.wikipedia.org/wiki/Sftp
[81] TORRES, Juan; GARCÍA, Richard. “Syslog”
http://www.wikilearning.com/monografia/control_administracion_
[82] ANÓNIMO. “Peer-to-peer”
http://es.wikipedia.org/wiki/Caracteristicas_p2p
[83] ANÓNIMO. “Administración de Tráfico Peer-to-Peer”
http://www.bfya.com/docs/admp2p.pdf
[84] ALONSO. “Por qué el tráfico P2P es bueno para todos (hasta los ISPs)”
http://alfonsoycia.blogspot.com/porqu-el-trfico-p2p-es-bueno-para-todos.html

OTROS

[85] ALVARADO, Alexandra. “Diagrama MPLS”. ESP PROY 06 Ver 07 May 08
[86] ALVAREZ, Víctor. “Análisis de tráfico de la red MPLS de Telconet S.A.” ESP PROY 03 Ver 23 May 08
[87] TIPÁN, Milton. “Diagrama PTS1UIO actual”. ESP PROY 06 Ver 29 Ene 09

CAPÍTULO 3

DISEÑO DE UN ESQUEMA DE CALIDAD DE SERVICIO (QoS) EN LA TECNOLOGÍA MPLS

3.1 CALIDAD DE SERVICIO (QoS) EN LA TECNOLOGÍA MPLS

El protocolo IP es el protocolo dominante en la mayoría de redes. Su creación, filosofía sin conexión y envío de tráfico de naturaleza “mejor esfuerzo” ha dado muy buenos resultados y, por lo tanto, ha contribuido a su expansión. Sin embargo, las nuevas aplicaciones que han ido surgiendo en los últimos años requieren más de lo que la actual tecnología IP puede proporcionar.

MPLS aparece como una tecnología alternativa escalable, haciendo más sencillo el ofrecimiento de nuevos servicios, debido a que es parte de la tecnología IP. Sin embargo, las redes IP no ofrecen QoS, por lo que es necesario integrar MPLS con arquitecturas de QoS. La arquitectura de QoS adoptada por muchos ISPs en sus redes es DiffServ, por el sinnúmero de ventajas que presenta sobre otras arquitecturas, expuestas en el **Capítulo 1**.

La integración de MPLS y DiffServ para alcanzar niveles de QoS es una buena línea para mejorar las redes IP, puesto que MPLS actúa al nivel de capa Enlace y capa Red, proporcionando un método de envío rápido gracias a su conmutación de etiquetas y a sus caminos LSPs, mientras que DiffServ realiza la diferenciación y priorización de tráfico necesaria para dotar a IP de QoS.

Actualmente, la integración de la tecnología MPLS con la arquitectura de QoS DiffServ es fuente de arduo trabajo en la IETF, organización que ha recomendado el RFC 3270, con el objetivo de proporcionar mecanismos que permitan integrar los módulos de trabajo de ambas tecnologías, ofreciendo una solución flexible para el soporte de DiffServ sobre MPLS y acorde con las necesidades de los ISPs.

3.1.1 SINERGIAS ENTRE MPLS Y DIFFSERV[3]

La tecnología MPLS simplifica el proceso de enrutamiento usado en las redes con tecnología IP, ya que en un dominio MPLS, cuando un flujo de datos atraviesa una ruta común, un LSP puede ser establecido usando protocolos de señalización MPLS. Un paquete se asigna a una FEC sólo una vez cuando ingresa a la red MPLS a través del LER, se le coloca una etiqueta que identifica a la FEC que pertenece y se lo envía al siguiente nodo. En cada LSR a través del LSP, sólo la etiqueta MPLS se usa para enviar el paquete al siguiente salto.

En un dominio DiffServ, todos los paquetes que cruzan un enlace y requieren el mismo comportamiento DiffServ se dice que constituyen un *Behavior Aggregate* (BA). En el nodo de ingreso al dominio DiffServ, los paquetes son clasificados y marcados con el DiffServ Code Point (DSCP), el cual corresponde a su BA. En los nodos de tránsito, el valor DSCP permite seleccionar el *Per-Hop Behavior* (PHB) que determinará la cola y el tratamiento planificado a utilizarse y, en algunos casos, la probabilidad de descarte para cada paquete.

En base a lo indicado anteriormente, se puede apreciar las similitudes entre MPLS y DiffServ: un LSP o una FEC es similar a un BA o a un PHB y la etiqueta MPLS es similar al valor DSCP de DiffServ en algunas situaciones. La diferencia está en que MPLS realiza conmutación, mientras que DiffServ más bien realiza encolamiento, planificación y descarte. Debido a esto, MPLS y DiffServ son ortogonales, lo que significa que la una no depende de la otra, ambas tecnologías ofrecen diferentes vías para proveer de altos niveles de calidad a los servicios. Además, esto significa que es posible tener a ambas arquitecturas trabajando al mismo tiempo en una simple red, pero también es posible tener sólo a una o a ninguna de ellas, dependiendo de la elección del operador de la red.

El LSR en el borde de ingreso del LSP realiza un rol adicional, ya que controla el tráfico que tiene permitido usar un determinado LSP. El elemento clasificador utilizado para seleccionar el tráfico aplicable para un determinado LSP es muy similar al acondicionador de tráfico de DiffServ. Si los dominios MPLS y Diffserv son idénticos, entonces la misma función dentro del nodo de ingreso puede ser utilizada para el acondicionamiento de tráfico en Diffserv y la determinación de

selección de tráfico en MPLS. Además, en muchos casos, un LSP transmitiendo un agregado de tráfico de muchos usuarios circula por la red, al igual que un BA de DiffServ generalmente llevando múltiples microflujos.

3.1.2 ESTRUCTURA DE LOS NODOS[4]

Las funciones de los nodos de una red que soporta tecnología IP y MPLS son redefinidas para permitir la integración entre DiffServ y MPLS. La estructura básica de un nodo en la nueva arquitectura se indica en la figura 3.1.

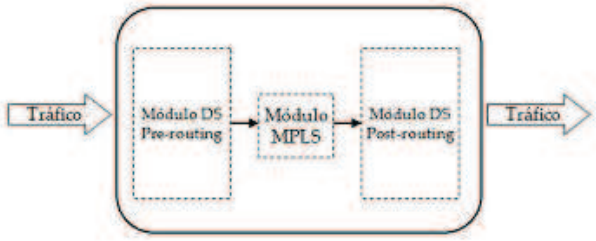

Figura 3.1 Estructura de un nodo en la integración DiffServ/MPLS

3.1.2.1 Módulo DiffServ *pre-routing*

Este módulo clasifica los paquetes, los marca y realiza las correspondientes funciones de acondicionamiento de tráfico si se trata de un LER. Este módulo sólo se encuentra en los LERs, aunque los procesos de marcación de los paquetes pueden darse en el *host* origen. La figura 3.2 muestra el módulo de *pre-routing*, donde pueden distinguirse los distintos componentes funcionales propios de la arquitectura DiffServ, así como las tablas de información y estado (perfiles y PHB) que usa. El cuadro punteado corresponde al módulo siguiente, el de MPLS a donde son reenviados todos los paquetes para la siguiente fase del proceso.

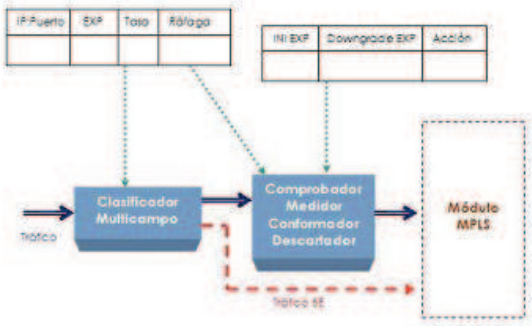

Figura 3.2 Módulo *pre-routing* en detalle

3.1.2.2 Módulo MPLS

El módulo MPLS realiza las funciones de enrutamiento propias de MPLS, etiquetando previamente el paquete si se trata de un LER. En este bloque se traduce directamente el subcampo DSCP de IP al campo EXP de MPLS. Además, se realizan las tareas propias de enrutamiento de MPLS que hacen que un paquete se inserte en un determinado módulo DiffServ *post-routing* u otro, dependiendo de su interfaz de salida.

3.1.2.3 Módulo DiffServ *post-routing*

El módulo MPLS dirige los paquetes a su interfaz de salida correspondiente. En cada interfaz se encuentra el módulo *post-routing*, que primero realiza una clasificación por BAs utilizando el campo EXP e inserta el paquete en la cola adecuada para el control de congestión, las cuales se gestionan mediante mecanismos de evasión de congestión, como se indica en la figura 3.3. A continuación, se elige un algoritmo de planificación de cola para el despachador de paquetes, cuyo principal requerimiento a la hora de elegirlo para DiffServ es que sea capaz de discriminar distintos tipos de tráfico.

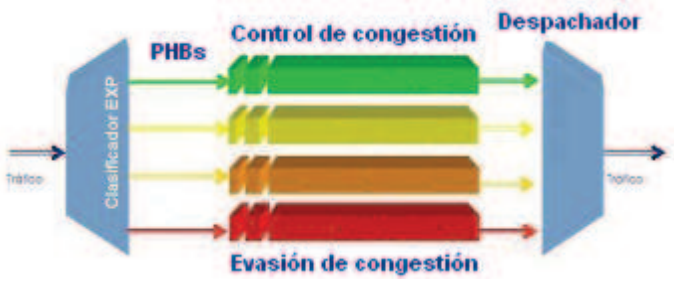

Figura 3.3 Funciones del módulo *post-routing*

3.1.3 REDEFINICIÓN DEL CAMPO EXP DE MPLS[4]

El campo EXP de 3 bits ubicado en la cabecera MPLS fue originalmente considerado de uso experimental, como indica la figura 3.4. Sin embargo, con el propósito de especificar la CoS a la que pertenece un paquete, se utiliza el soporte de MPLS para DiffServ, donde se redefine este campo para especificar dicha CoS.

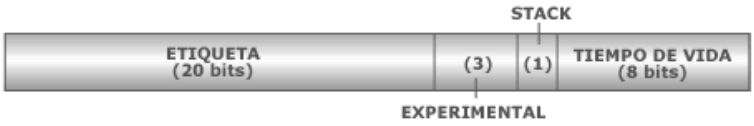

Figura 3.4 Formato de la etiqueta MPLS conteniendo el campo EXP[4]

Las clases de servicio que se proporcionan en la nueva arquitectura son las mismas que en el modelo DiffServ, ya que la integración de DiffServ con MPLS no modifica su filosofía ni su funcionamiento, de modo que se vuelve más sencilla la convivencia con los dominios DiffServ ya implantados.

Con el fin de soportar DiffServ sobre MPLS con la gran variedad de valores DSCP, es necesario configurar la apropiada QoS en cada LSR de la red. Debido a que las etiquetas MPLS fueron definidas antes que los valores DSCP, el campo EXP tiene sólo tres bits en correspondencia a los tres bits del subcampo Precedencia del paquete IP. El problema es que DiffServ puede soportar hasta 64 posibles valores DSCP, a diferencia de las etiquetas MPLS que admiten sólo 8 posibles valores de PHBs, por lo que fue necesario definir métodos que cubran esta necesidad.

3.1.4 MÉTODOS DE QoS SOBRE MPLS[2][6][7]

El RFC 3270 describe una solución flexible para el soporte de la arquitectura DiffServ sobre redes MPLS. Cuando un *router* MPLS envía un paquete al siguiente salto, lo envía con la respectiva etiqueta, por lo que los LSRs subsecuentes en la red no analizan la cabecera del paquete, simplemente leen la etiqueta MPLS, la cual es indexada a la tabla de enrutamiento mantenida por cada LSR para especificar el siguiente salto.

Ahora, cuando los paquetes marcados con los valores DSCP llegan a una red MPLS, se necesita de un método para transferir la información proporcionada por estos valores a las etiquetas MPLS. Esta necesidad debe ser cubierta con el fin de que la red con tecnología MPLS sea capaz de tomar decisiones que respeten los requerimientos de servicios diferenciados marcados en los paquetes, ya que las cabeceras IP no son examinadas cuando los paquetes han sido etiquetados. Por lo tanto, los paquetes no pueden ser diferenciados basados en los valores

DSCP, ya que éstos son parte de la cabecera IP. DiffServ debe proveer de una vía diferente para hacer viable la arquitectura DiffServ/MPLS.

El RFC 3270 describe dos métodos para transmitir información de la CoS de la cabecera IP a los LSRs en la cabecera MPLS, que son:

- EXP-*inferred*-PHB *Scheduling Class* LSP (E-LSP)
- *Label-only-inferred* LSP (L-LSP)

3.1.4.1 EXP-*inferred*-PHB *Scheduling Class* LSP (E-LSP)

Si una red soporta hasta ocho PHBs, entonces los bits del campo EXP son suficientes para esa red, permitiendo definir un E-LSP. Los LSRs almacenan un mapa de correspondencia entre valores EXP a PHBs, mientras que los LERs mantienen un mapa de correspondencia entre valores DSCP a EXPs, como se indica en la figura 3.5; estos mapas necesitan ser definidos y configurados en los nodos de la red. La etiqueta indica al LSR dónde enviar el paquete y los bits del campo EXP determinan el PHB que debe ser usado para el tratamiento del paquete durante su transmisión.

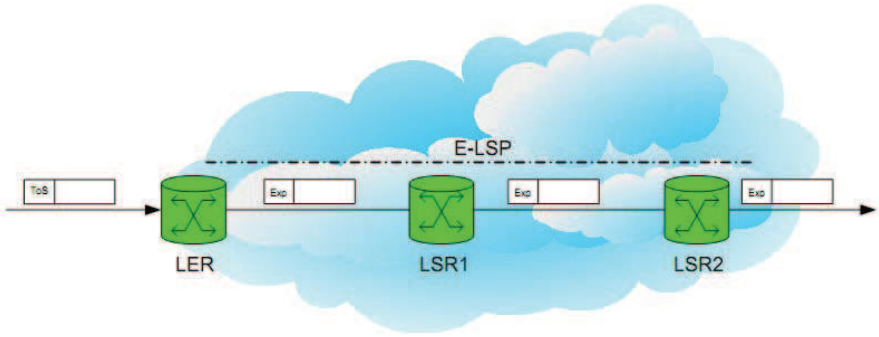

Figura 3.5 Establecimiento de un E-LSP[7]

Los E-LSPs pueden ser establecidos a través de varios protocolos de señalización como LDP y RSVP, aunque el PHB es determinado por los bits del campo EXP, sin necesidad de ningún tipo de señalización adicional. La figura 3.6 muestra el tratamiento que recibe un paquete que ingresa a una red con tecnología MPLS, configurada para establecer caminos E-LSP. Cuando el paquete llega al LER, éste revisa su cabecera en busca del campo ToS y su valor DSCP; busca en el mapa que tiene almacenado para determinar qué valor del

campo EXP le corresponde, lo encola de acuerdo a este valor colocado y lo envía al siguiente nodo. El LSR recibe el paquete, revisa la etiqueta en busca del campo EXP y el valor que contiene, busca en su mapa para determinar qué PHB le corresponde, lo encola y lo envía al siguiente nodo, repitiendo este proceso hasta que el paquete deja la red MPLS.

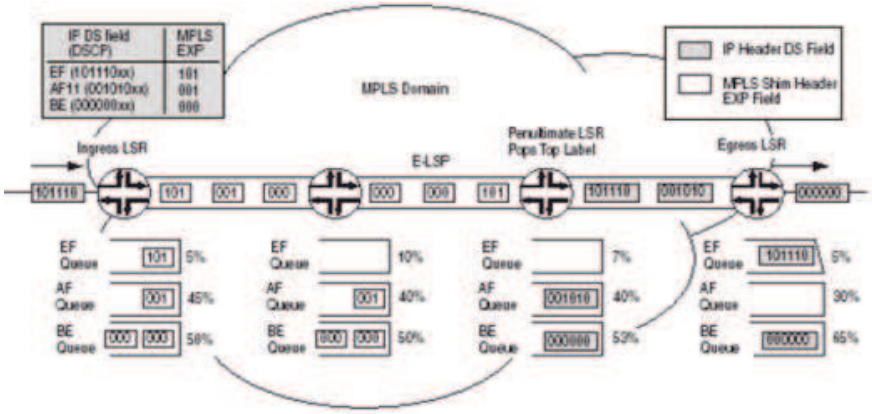

Figura 3.6 Ejemplo del tratamiento de un paquete dentro de un E-LSP[8]

3.1.4.2 *Label-only-inferred* LSP (L-LSP)

Si una red tiene más de ocho PHBs, entonces los bits del campo EXP no son suficientes para cubrir todos los PHBs a LSPs, por lo que surge un nuevo método de QoS denominado L-LSP. Los L-LSPs soportan arbitrariamente un gran número de correspondencias entre FECs y BAs, debido a que se hace uso del campo etiqueta para cubrir los PHBs. Los LERs setean el campo EXP de acuerdo a la prioridad de descarte del paquete y lo envían por el LSP correcto, mientras que los LSRs revisan el paquete en busca de los campos etiqueta y EXP para darle el respectivo tratamiento, como se indica en la figura 3.7. El campo etiqueta se usa para determinar el PHB respectivo y los bits del campo EXP se usan para codificar la prioridad de descarte.

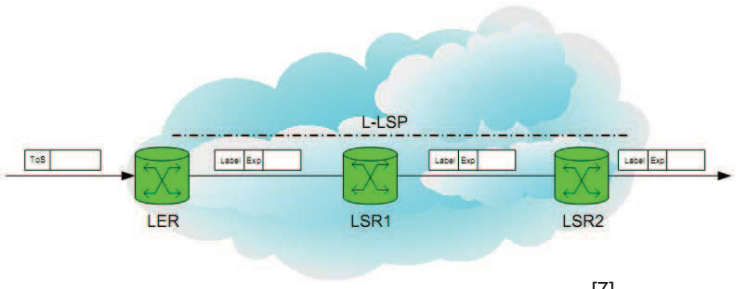

Figura 3.7 Establecimiento de un L-LSP[7]

Los L-LSPs pueden ser establecidos por una extensión de los protocolos de señalización como LDP y RSVP (CR-LDP, TE-RSVP). La figura 3.8 muestra el tratamiento que recibe un paquete que ingresa a una red con tecnología MPLS, configurada para establecer caminos L-LSP. Cuando el paquete llega al LER, éste revisa su cabecera en busca del campo ToS y su valor DSCP, busca en el mapa que tiene almacenado para determinar qué valor de los campos etiqueta y EXP le corresponden, lo encola de acuerdo al campo etiqueta colocado y lo envía por el PHB correspondiente. El LSR recibe el paquete, revisa la etiqueta en busca del campo etiqueta y el valor que contiene, determina el siguiente salto en el LSP que le corresponde y lo envía al siguiente nodo, repitiendo este proceso hasta que el paquete deja la red MPLS.

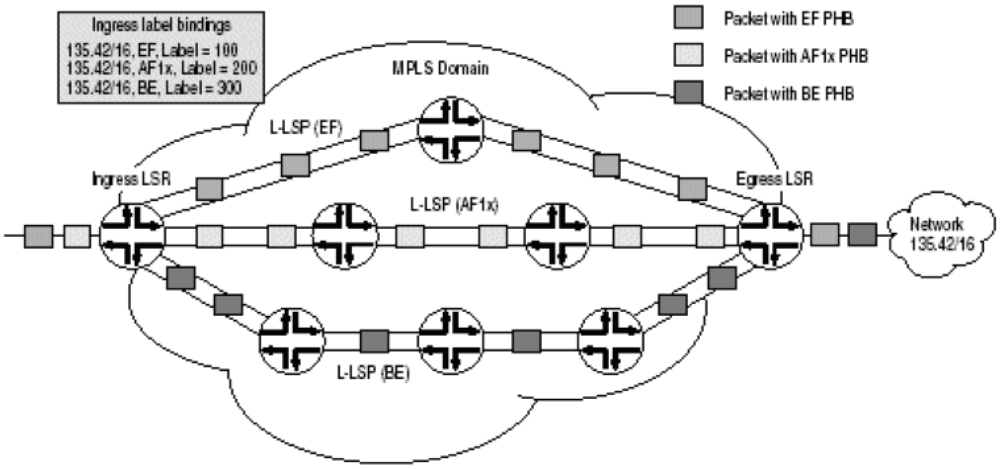

Figura 3.8 Ejemplo del tratamiento de un paquete dentro de un L-LSP[8]

3.1.4.3 Diferencias entre los métodos de QoS[6]

Los métodos de QoS se diferencian claramente en las funciones que realizan para permitir el soporte de la arquitectura DiffServ sobre la tecnología MPLS. La tabla 3.1 muestra las diferencias que existen entre los métodos E-LSP y L-LSP de QoS sobre MPLS.

E-LSP	L-LSP
El PHB es determinado por el campo EXP	El PHB es determinado por el campo etiqueta o por la combinación de los campos etiqueta/EXP
No se necesita de ningún tipo de señalización adicional	El PHB o el grupo PHB planificado es señalizado en la configuración del LSP
El mapa de correspondencia entre el campo EXP y el PHB necesita ser configurado	El mapa de correspondencia entre el campo etiqueta y el PHB necesita ser configurado, mientras que el del campo EXP a PHB es conocido
La cabecera *shim* es requerida. No es posible utilizar los E-LSPs en ATM	La cabecera *shim* o la cabecera PDU pueden ser utilizadas, por consiguiente, es soportado por enlaces ATM
Puede usar hasta ocho PHBs por LSP	Sólo admite un PHB por LSP
Soporta hasta ocho PHBs	Soporta más de ocho PHBs

Tabla 3.1 Diferencias entre E-LSP y L-LSP

3.1.4.4 Desventajas de los métodos de QoS[6]

El problema con los E-LSPs es su habilidad de utilizar sólo tres bits para representar sólo ocho PHBs por cada LSP dado, lo que no es muy útil cuando más de ocho PHBs son definidos. Sin embargo, los L-LSPs soportan arbitrariamente un gran número de PHBs, pero el problema radica en la escalabilidad. En una red con diferentes LSPs para diferentes PHBs, el número de etiquetas que un LSR debe mantener se incrementa. Con el incremento del número de PHBs, el mantenimiento de esa gran cantidad de etiquetas se convierte en un problema.

3.1.5 MODOS DE TUNELIZACIÓN DE DIFFSERV SOBRE MPLS[2][9][10]

La tunelización es la habilidad de la QoS para ser transparente de un extremo de la red, al otro extremo de la misma. El túnel empieza donde se da el

procedimiento de imposición de la etiqueta y termina en el punto del procedimiento de disposición de la etiqueta, donde se da la operación pop sobre la pila de etiquetas y el paquete sale como un paquete MPLS con un PHB diferente o como un paquete IP con un PHB de IP.

Los modos de tunelización de DiffServ sobre MPLS permiten a los proveedores de servicios manejar la QoS que un *router* proveerá a un paquete MPLS en una red con tecnología MPLS. Sin embargo, existe una restricción en cuanto a su uso ya que no soportan L-LSPs, solamente E-LSPs.

Existen tres modos de tunelización para enviar los paquetes a través de una red MPLS que son:

- Modo uniforme
- Modo tubería
- Modo tubería corta

Los modos de tubería y tubería corta proveen QoS transparente, es decir, que el marcado IP de los usuarios en la cabecera IP es preservado.

Los tres modos de tunelización afectan el comportamiento de los LERs y de los penúltimos LSRs del LSP cuando se realizan las operaciones *push* y *pop* sobre las etiquetas. Sin embargo, no afectan a la operación *swap* en los nodos intermedios.

3.1.5.1 Modo uniforme

El modo de tunelización uniforme tiene una sola capa de QoS que va de extremo a extremo de la transmisión. El LER de ingreso copia ó corresponde el valor DSCP contenido en el paquete IP entrante al campo EXP de la cabecera MPLS de la etiqueta impuesta. A medida que los bits del campo EXP atraviesan la red, éstos pueden o no ser modificados por los LSRs. La figura 3.9 indica un ejemplo del comportamiento de los *routers* configurados con el modo uniforme.

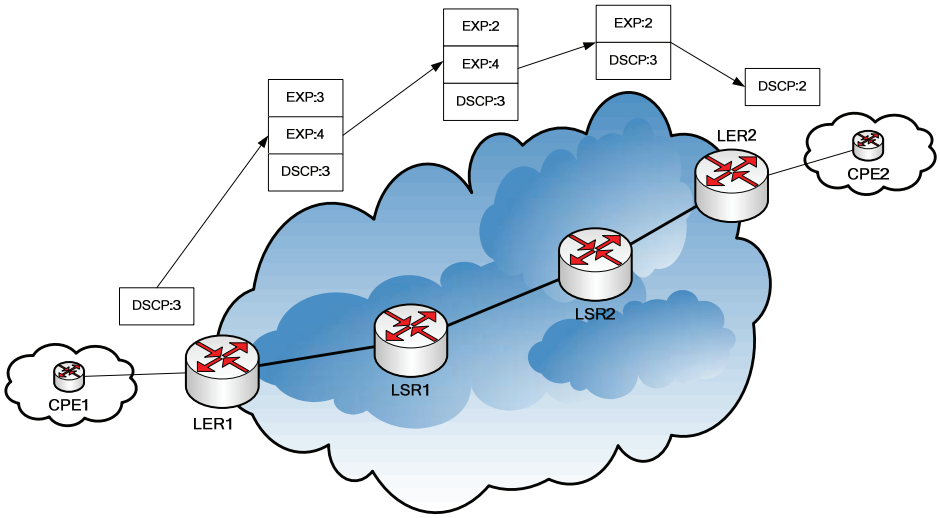

Figura 3.9 Modo de tunelización uniforme

En este ejemplo, el *router* LSR1 modifica los bits del campo EXP de la etiqueta superior de la pila de etiquetas. El LSR2 copia los bits del campo EXP a los bits del campo EXP de la nueva etiqueta expuesta después de la extracción de la etiqueta en el penúltimo LSR. Finalmente, el LER2 copia los bits del campo EXP a los bits del subcampo DSCP del paquete IP.

3.1.5.2 Modo tubería

El modo tubería brinda una QoS en la interfaz de salida del LER de egreso, basada en el campo EXP de la cabecera MPLS recibida, aún cuando una o más etiquetas MPLS hayan sido removidas. El subcampo precedencia del paquete IP, los bits del campo EXP y el subcampo DSCP no son alterados cuando el paquete es transmitido por la red MPLS.

Cualquier cambio en el marcado de los paquetes en el interior de la red MPLS no es permanente ni propagado cuando el paquete deja la red. El LER de egreso usa el marcado que fue usado por los LSRs. Sin embargo, este LER debe remover las etiquetas impuestas al paquete original, después de guardar una copia interna del marcado para clasificar el paquete en la interfaz de salida. La figura 3.10 indica un ejemplo del comportamiento de los *routers* configurados con el modo tubería.

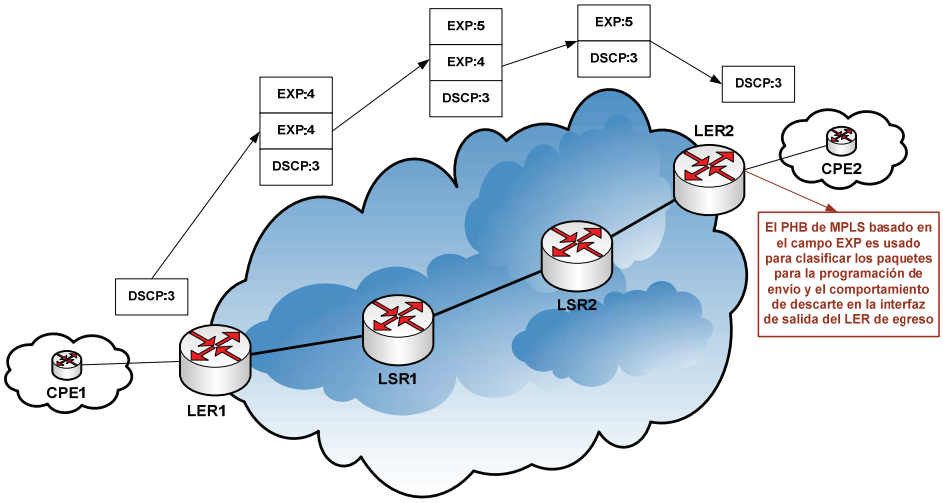

Figura 3.10 Modo de tunelización tubería

3.1.5.3 Modo tubería corta

El modo tubería corta usa las mismas reglas y técnicas que el modo tubería. La diferencia reside en que el LER de egreso clasifica los paquetes IP para la cola de salida basado en el valor DSCP original del paquete IP. La figura 3.11 indica un ejemplo del comportamiento de los *routers* configurados con el modo tubería corta.

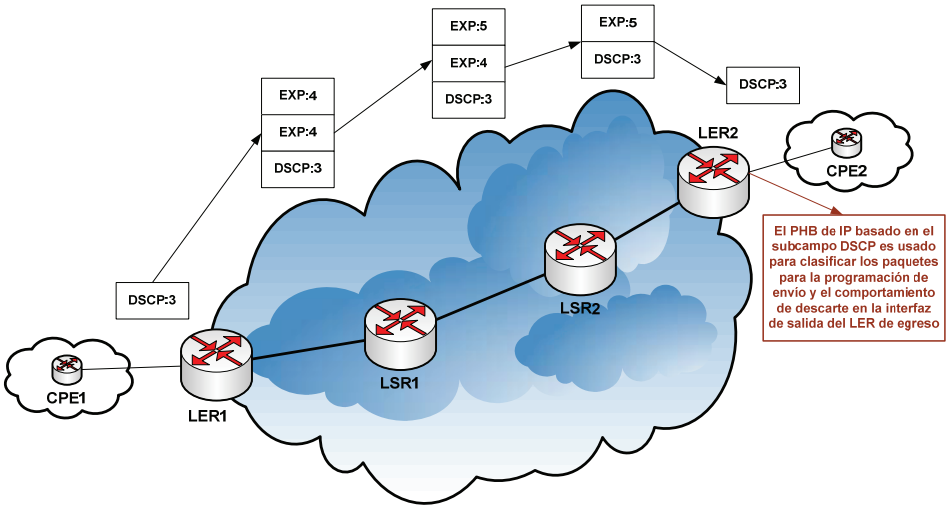

Figura 3.11 Modo de tunelización tubería corta

3.1.5.4 Determinación del modo de tunelización apropiado[10]

El modo de tunelización apropiado para manejar la QoS puede ser escogido de acuerdo a las siguientes recomendaciones:

- Si el equipo terminal del lado del abonado (CPE) soporta MPLS, se recomienda usar el modo tubería, de manera que la QoS ofrecida a través del PHB del proveedor del servicio estará en el enlace entre el CPE y el *router* PoP.
- Si el CPE no soporta MPLS, entonces se recomienda hacer uso del modo tubería corta.
- Si no existe marcado de los paquetes o si hay pocas marcas, entonces los usuarios preferirán hacer uso del modo de tunelización uniforme.

3.1.6 IMPLEMENTACIÓN DE DIFFSERV SOBRE MPLS[3]

El proceso de implementación para la integración de DiffServ y MPLS requiere el desarrollo del módulo DiffServ/MPLS con la extensión y modificación de los módulos de ambas tecnologías.

3.1.6.1 Modificaciones en los módulos de DiffServ

El principal punto en la modificación de los módulos de DiffServ es adaptar los módulos de la arquitectura MPLS. La arquitectura MPLS diferencia los paquetes pertenecientes a diferentes flujos de acuerdo a sus etiquetas, de manera que en el módulo modificado, la base para la diferenciación de los paquetes será con la etiqueta y el campo EXP de la cabecera *shim*.

3.1.6.2 Modificaciones en los módulos de MPLS

Estas modificaciones cubren el manejo de los tipos de LSPs (E-LSP y L-LSP), así como la configuración de los enlaces de DiffServ. Durante la modificación de los módulos, se consideran los siguientes puntos:

- En una red DiffServ/MPLS sólo debe haber LSPs predefinidos con el fin de cumplir con los parámetros de QoS definidos previamente.
- Los mensajes de señalización usados en el caso de crear o borrar LSPs deben ser una extensión de los protocolos conocidos y usados comúnmente.

- Los paquetes transferidos en un LSP tienen que tener PHBs definidos estrictamente.
- Debería existir una forma de asignar rutas alternativas a un LSP, las cuales serán usadas en caso de falla de un enlace.
- Un LSP debería ser capaz de llevar más de un microflujo.

3.1.7 ETAPAS DE LA QoS EN MPLS[11]

La implementación de QoS en una red que maneja tecnología MPLS requiere de varias etapas similares a las funciones que maneja la arquitectura DiffServ, que van cumpliéndose a medida los paquetes son transmitidos. Estas etapas son las siguientes:

- **Identificar el tráfico y sus requerimientos:** Esta etapa analiza cada paquete para determinar el tipo de información que contiene y por ende, reconocer los requerimientos que pueda necesitar.
- **Dividir el tráfico en clases y marcarlo:** Este proceso permite dividir el tráfico en diferentes categorías y marcarlo, de modo que los dispositivos de red puedan reconocer a qué categoría o clase pertenece y operar en consecuencia.
- **Definir políticas para las clases:** Este proceso incluye los mecanismos de perfiles de tráfico, control de congestión, evasión de congestión y acondicionamiento del tráfico.

3.1.7.1 Algoritmos de regulación de tráfico[12][13]

Una de las principales causas de la congestión es que el tráfico es a ráfagas, por lo que los algoritmos de regulación de tráfico obligan a las fuentes a transmitir de forma más predecible. En realidad, lo que pretenden es regular la tasa de velocidad y la variabilidad del tráfico de entrada a la red.

Los algoritmos para regular el tráfico de entrada más comunes son *leaky bucket* y *token bucket*.

3.1.7.1.1 Algoritmo leaky bucket

El algoritmo *leaky bucket* es el más ampliamente usado para describir el tráfico de una red. Este algoritmo regula el tráfico a modo de un cubo con goteo, como se indica en la figura 3.12. Se usan dos parámetros para describir el algoritmo que son la capacidad del cubo s y la tasa de drenaje p.

El funcionamiento del algoritmo es simple: siempre que el cubo tenga contenido se envía datos a la red a una tasa p, todo paquete entrante se introduce en el cubo y en el caso de que el cubo esté lleno, el paquete entrante se pierde. De esta forma, se limita la tasa de transmisión del tráfico al valor de p. El valor de s para un determinado flujo debe ser calculado de tal forma que no se pierdan paquetes.

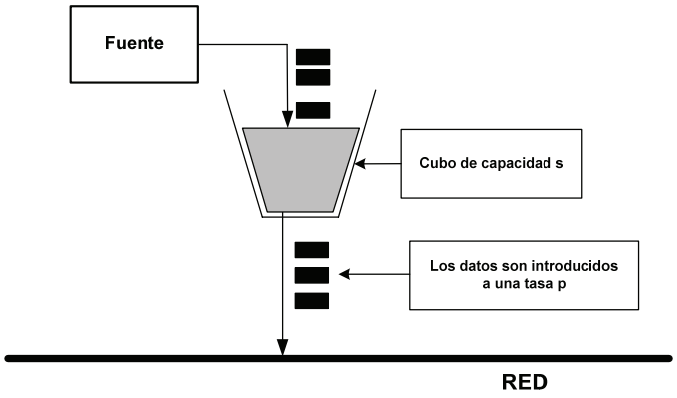

Figura 3.12 Funcionamiento del algoritmo *leaky bucket*

3.1.7.1.2 Algoritmo token bucket

Token bucket es un algoritmo de gestión de tasas de velocidades utilizado para establecer perfiles de tráfico, basado en el conformador de tráfico para transmitir a mayores velocidades cuando se recibe un pico.

Este algoritmo es de tipo bucle abierto, lo que significa que no reacciona cuando ya se ha producido la congestión, sino que previene que se produzca, limitándose a dejar pasar paquetes que lleguen a una tasa que no exceda una impuesta administrativamente, pero con la posibilidad de permitir ráfagas cortas que excedan esta tasa.

El funcionamiento del algoritmo es el siguiente: el cubo contiene *tokens* generados a una tasa r, como indica la figura 3.13. El cubo puede admitir como máximo b *tokens* estando lleno al inicio, por lo que para transmitir un bit se tiene que coger un *token* del cubo y eliminarlo. Mientras existan *tokens* en el cubo, la fuente puede insertar tráfico en la red de acuerdo a la tasa deseada. Cuando se acaban los *tokens*, habrá que esperar al próximo *token* que se genere, lo que implica que la tasa de transmisión disminuye a r. En esencia, lo que permite el algoritmo es poder transmitir en un determinado intervalo a tasas superiores a r.

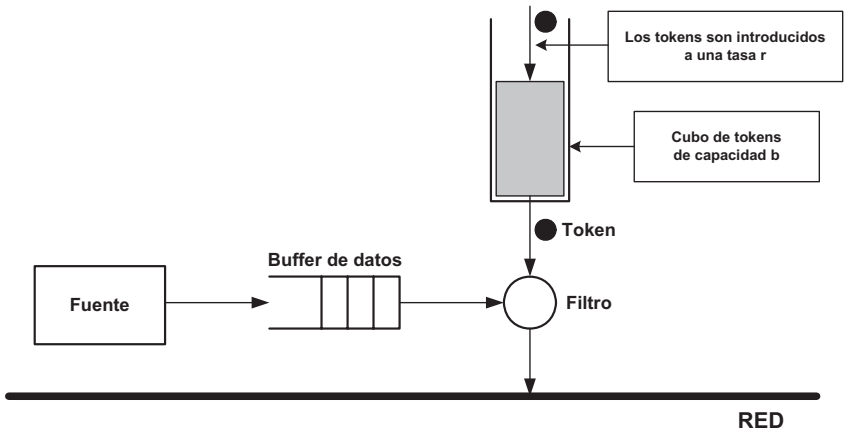

Figura 3.13 Funcionamiento del algoritmo *token bucket*

El asociar este algoritmo con los flujos *tokens* y datos, corresponde a tres posibles situaciones:

- Los datos llegan al filtro a una tasa igual a la de los *tokens* entrantes. En este caso, cada paquete entrante tiene su *token* correspondiente y pasa a la cola sin retrasos.
- Los datos llegan al filtro a una tasa menor a la de los *tokens*. En este caso, sólo una parte de los *tokens* se borran con la salida de cada paquete que se envía fuera de la cola, de manera que se acumulan los *tokens* hasta llenar el *bucket*. Los *tokens* sin usar se pueden utilizar para enviar datos a velocidades mayores que la tasa de *tokens*, en cuyo caso se produce una corta ráfaga de datos.
- Los datos llegan a una tasa mayor a la de los *tokens*. Esto significa que el *bucket* se quedaría pronto sin *tokens*, lo que causaría que el filtro se

acelere a sí mismo por un rato, creando una situación sobrelímite. Si siguen llegando paquetes, empezarían a ser descartados.

Esta última situación es muy importante porque permite ajustar administrativamente el ancho de banda disponible a los datos que están pasando por el filtro, de manera que se puedan establecer perfiles de tráfico de acuerdo a los SLAs.

3.2 DESCRIPCIÓN DE LA RED CON TECNOLOGÍA IP/MPLS DE TELCONET S.A.

Con el fin de desarrollar el presente proyecto, se realizó el levantamiento de información de la red de la empresa Telconet S.A. La información fue obtenida del Departamento de Proyectos y de los instructivos facilitados por la empresa. Sin embargo, se debe recalcar que no toda la información entregada puede ser publicada en detalle debido a las políticas de seguridad de la empresa, estipuladas en el acuerdo de confidencialidad firmado para el desarrollo del presente proyecto, aunque se pudo obtener los datos necesarios para el diseño.

Telconet S.A. es una empresa portadora dedicada a ofrecer servicios de acceso a Internet y transmisión de datos, con sucursales en más de 100 ciudades del país, cuya matriz se encuentra ubicada en la ciudad de Guayaquil y su sucursal más importante corresponde a la ciudad de Quito en la dirección Pedro Gosseal 148 y Mariano Echeverría, donde se realizará el desarrollo del presente proyecto.

Dentro de la amplia gama de servicios que ofrece Telconet S.A. a sus clientes se pueden destacar los siguientes:

- Internet mediante conexión telefónica (*dial-up*)
- Internet dedicado a través de fibra óptica
- Transmisión de datos por fibra óptica y radio enlaces
- Transmisión de canales de video
- Internet 2

El tipo de clientes que maneja esta empresa portadora son tanto corporativos como residenciales; entre los clientes corporativos se tiene todo tipo de organizaciones como empresas, bancos, centros comerciales, universidades, instituciones gubernamentales, comisariatos, entre otras.

Telconet S.A. tiene una gran trayectoria de telecomunicaciones en el país, ofreciendo su portafolio de servicios a través de su Red de Próxima Generación (NGN), utilizando la tecnología MPLS para permitir accesos entre 1 Mbps y 10 Gbps, cubriendo las diferentes necesidades que tengan los clientes.

3.2.1 SITUACIÓN ACTUAL DE TELCONET S.A.[1]

La red de Telconet S.A. usa como medio de transmisión principal la fibra óptica, gracias al gran número de ventajas que presenta ante otros medios de transmisión como el par trenzado. El extenso tendido de fibra consta de más de 8500 Km instalados en todo el país, compuesto completamente por fibra monomodo, con el fin de interconectar redes de datos geográficamente distantes y dar garantía de rutas físicas completamente independientes.

La tecnología IP es manejada por la red *Gigabit Ethernet* de Telconet S.A. para brindar servicios de calidad y confiabilidad a un gran número de clientes corporativos, que poseen sucursales alrededor de todo el país, por lo que trabaja con una topología de respuesta a fallas a través de enlaces de microondas.

Con el fin de conectar las diferentes redes de sus clientes corporativos, Telconet S.A. tiene enlaces de fibra óptica y microondas con varias ciudades del país por medio de la tecnología SDH, como se indica en la figura 3.14. La conexión entre las ciudades de Guayaquil y Quito es a través de un anillo de fibra óptica con tecnología MPLS, que va de Quito a Guayaquil pasando por Santo Domingo y retorna a Quito pasando por Cuenca, de capacidad igual a 1 Gbps. En caso de que existiera una doble ruptura de este anillo, se tiene otro contingente entre Quito y Guayaquil a través de un enlace de microondas con una capacidad de un STM-1 (155 Mbps).

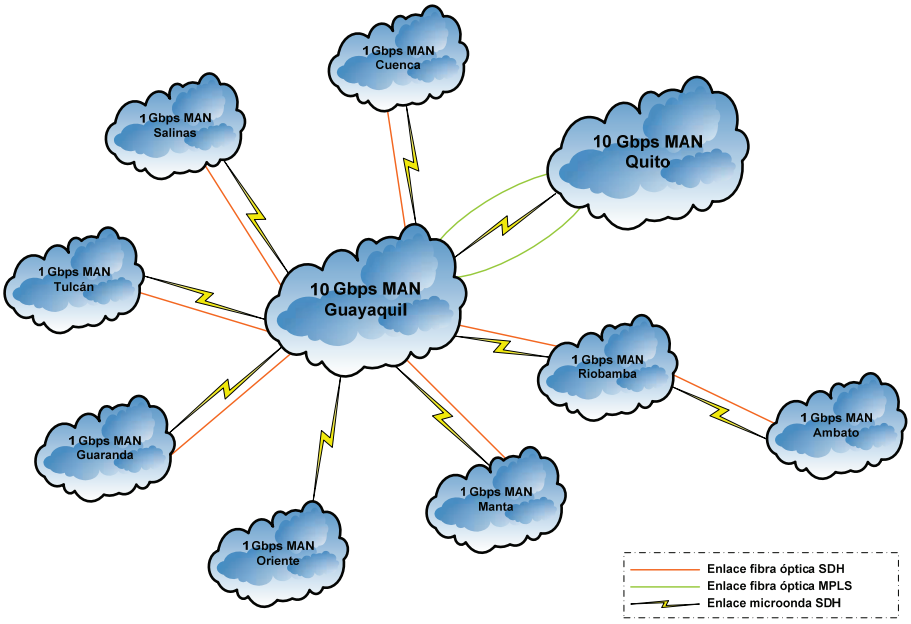

Figura 3.14 Enlaces SDH de la red de Telconet S.A.

El servicio de Internet dedicado de la empresa cuenta con una interconexión al proveedor principal, TIWS, en la ciudad de Salinas con capacidad de 600 Mbps. En caso de que esta conexión falle, se tiene redundancia de interconexión internacional a los principales proveedores Tier 1 de Internet como son Sprint y NTT, con capacidad contratada de 250 Mbps con cada uno. Adicionalmente, si la conexión con los tres proveedores principales falla, se tiene una conexión en Quito a través del proveedor internacional Transnexa con capacidad de 2 T3 (90 Mbps) y una negociación de incremento de capacidad en caso de ser requerida.

En la actualidad, Telconet S.A. ha optado por ampliar su área de cobertura y elegir una tecnología que mejore su desempeño, conservando la mayoría de su infraestructura actual, de modo que le permita ofrecer mejores niveles de calidad y diversificar sus servicios. La tecnología que esta empresa portadora está implementando en las ciudades de Quito y Guayaquil es MPLS.

3.2.2 ESTRUCTURA DEL *BACKBONE* DE TELCONET S.A. EN QUITO[14]

Telconet S.A. se encuentra en un proceso de migración de su red *Gigabit Ethernet* con tecnología IP, ubicada en la ciudad de Quito y conectando a la mayoría de clientes, a su red diseñada que está siendo instalada con tecnología MPLS.

El *backbone* de Telconet S.A. en Quito es una red diseñada bajo el modelo jerárquico de tres capas (*core*, distribución y acceso), constituida por un conjunto de equipos de conmutación y enrutamiento marca Cisco que cumplen diferentes funciones dependiendo de la capa en la que se encuentren y que usan como medios de transmisión la fibra óptica y los enlaces de microondas.

Posee enlaces redundantes como respaldo para no interrumpir el servicio ofrecido a los clientes y cuenta con un nodo principal, donde se encuentra ubicado el Centro de Operaciones y Monitoreo (NOC), que ofrece soporte técnico y realiza funciones de administración de red las 24 horas del día, los 365 días del año.

Los clientes acceden a la red de Telconet S.A. a través de equipos entregados en modalidad de alquiler por la empresa, utilizando como medios de transmisión de última milla fibra óptica y enlaces de microondas.

3.2.2.1 Características de la fibra óptica utilizada por Telconet S.A.[15]

La red de Telconet S.A. utiliza fibra óptica monomodo tendida en la ciudad de Quito vía aérea, trabajando en las ventanas de 1300 nm para recepción y 1550 nm para transmisión. Esta fibra utiliza a los postes de alumbrado público de la Empresa Eléctrica Quito (EEQ) como infraestructura y consta de 12 hilos, donde un solo hilo sirve para la conexión entre nodos del *backbone* y el resto de hilos son para la conexión de clientes, de manera que cada cliente utiliza un solo hilo de fibra óptica, ya que los enlaces son uno a uno sin compartición.

De acuerdo a la zona en la que se va a ubicar la fibra óptica, se tienen dos tipos de tendido:

- **Fibra óptica urbana:** Se caracteriza por tener en su interior cerca de la chaqueta final, dos cables de acero de 1,5 milímetros de espesor, para darle resistencia y permitir que sea fijada de forma aérea a los postes de energía eléctrica.
- **Fibra óptica interurbana:** Se diferencia de la fibra urbana porque posee una guía metálica para brindar mayor rigidez al tendido, haciendo que la distancia entre los postes pueda ser más grande.

El tendido de fibra óptica al llegar donde el cliente tiene instalado unas cajas para realizar la fusión entre el cable de fibra óptica y el *patch cord*, lo que permitirá la conexión a los equipos activos.

3.2.2.2 Características generales de los nodos[16]

Los nodos de la red de Telconet S.A. se encuentran ubicados en lugares estratégicos de la ciudad de Quito y están constituidos por elementos que permiten su correcto funcionamiento, como son:

- *Switches* o *routers* marca Cisco
- *Racks*
- *Transceivers* para fibra óptica
- Bancos de baterías
- *Patch cords* de fibra óptica y cable UTP
- Ventiladores
- Sistema de alimentación ininterrumpida (UPS)

Los *switches* o *routers* son marca Cisco y dependiendo de la capa en la que trabajen, se utilizan para la conexión entre nodos ó para la conexión entre nodos y el acceso de clientes a la red.

Todos los equipos que pertenecen al nodo se ubican en los racks, incluyendo a los ventiladores que evitan el excesivo calentamiento de los equipos.

Los *transceivers* se utilizan para acoplar la fibra óptica con el cable UTP, de tal manera que se asigne un puerto del equipo para cada cliente.

Los bancos de baterías y los UPS son colocados como medida preventiva de seguridad ante fallas en la energía eléctrica, con el fin de que el nodo se encuentre siempre operativo.

3.2.2.3 Descripción de la capa *core*[14]

La capa *core* es el núcleo de la red de Telconet S.A. y está formada por dos nodos principales que poseen las siguientes características:

- Concentran la mayor cantidad de tráfico de la red, por lo que su estructura de transporte es fiable, ofrecen baja latencia y buena capacidad de trabajo, con el propósito de reenviar el tráfico a altas velocidades.
- Los equipos de estos nodos no están configurados para trabajar con listas de acceso, encriptación de datos, conversión de direcciones o cualquier otro tipo de configuración que disminuya el procesamiento en la conmutación de paquetes.
- Poseen enlaces redundantes listos para ser levantados en caso de que el enlace principal deje de funcionar; los equipos instalados son tolerantes a fallas.
- Se encuentran ubicados de forma estratégica en lugares con buenas condiciones geográficas dentro del área de cobertura, debido a la geografía irregular que posee la ciudad de Quito.

Los dos nodos principales de esta capa están interconectados con fibra óptica monomodo y forman enlaces redundantes tipo malla con otros equipos ubicados en la ciudad de Guayaquil. Estos nodos están configurados con IP debido a la presencia de un enlace con la capa distribución y con MPLS para trabajar como LSRs, y son denominados como:

- CAT6500G (Gosseal)
- CAT6500M (Muros)

La figura 3.15 indica la conexión entre los dos nodos principales, con las respectivas interfaces configuradas a cada extremo del enlace, que tiene 1 Gbps de capacidad.

Figura 3.15 Conexión de los nodos principales de la capa *core*

Adicionalmente, la capa *core* implementa otros nodos que concentran y distribuyen grandes cantidades de tráfico, y permiten la migración de la tecnología IP a la tecnología MPLS. Estos equipos están configurados con MPLS para

trabajar como LSRs y LERs a la vez y son utilizados para indicar las rutas al *backbone*. Los nodos que trabajan como LERs son responsables de enrutar el tráfico entrante a la red MPLS, usando un protocolo de señalización de etiquetas y distribución de tráfico saliente. Estos equipos son denominados como:

- PE1UIOG
- PE2UIOG
- PE1UIOM
- PE2UIOM

La figura 3.16 indica la conexión entre todos los nodos de la capa *core*, con las respectivas interfaces configuradas a cada extremo de los enlaces, que tienen 1 Gbps de capacidad.

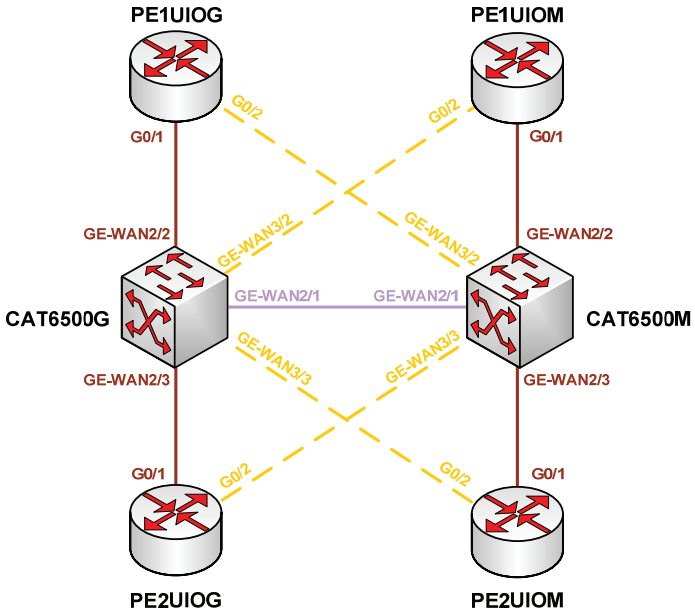

Figura 3.16 Conexión de todos los nodos de la capa *core*

3.2.2.3.1 Nodo CAT6500G

El nodo Gosseal se encuentra ubicado en el Norte de la ciudad de Quito y es el nodo más grande de la red de Telconet S.A., ya que aquí se encuentra el Centro de Operaciones y Monitoreo (NOC). Este nodo contiene a los siguientes equipos:

- Un *switch* Cisco Catalyst 6500 de capa 3 que se utiliza para enrutar el tráfico de los clientes a altas velocidades

- Un *switch* Cisco Catalyst 3750 de 48 puertos, que se utiliza para formar los pétalos MPLS de los nodos de la capa acceso
- Un *switch* de respaldo Cisco Catalyst 3750 de 48 puertos en caso de que falle el equipo principal
- La red de gestión formada por los servidores principales como DNS, *Proxy*, *Radius*, correo electrónico, web, antivirus, anti-*spams*, entre otros

Además, en este nodo se ubican los equipos de los nodos PE1UIOG y PE2UIOG, que son *routers* marca Cisco modelo 7200VXR.

3.2.2.3.2 Nodo CAT6500M

Este nodo se encuentra ubicado en la zona centro-norte de la ciudad de Quito, como *backup* del nodo CAT6500G y con un tiempo de respuesta en caso de falla de un minuto. Contiene a los siguientes equipos:

- Un *switch* Cisco Catalyst 6500 de capa 3
- Un equipo de microondas marca Redline
- Una red de gestión de respaldo de los servidores principales para casos en que falle el nodo principal CAT6500G

El nodo Muros permite establecer la conexión con la matriz de Telconet S.A. en la ciudad de Guayaquil mediante un anillo de fibra óptica con tecnología MPLS como enlace principal y, a la vez, sirve como punto de acceso para la comunicación con el resto de sucursales del país. Adicionalmente, se tiene un enlace SDH de microondas como enlace secundario en caso de que exista una falla en el anillo principal.

Adicionalmente, en este nodo se ubican los equipos de los nodos PE1UIOM y PE2UIOM, que son *routers* marca Cisco modelo 7200VXR.

3.2.2.4 Descripción de la capa distribución[14]

Los nodos PE indicados en la capa *core* forman también parte de la capa distribución, debido a que realizan funciones relacionadas a esta capa, como son:

- Implementación de políticas de enrutamiento y seguridad
- Enrutamiento entre VLANs
- Implementación de políticas para filtrar paquetes que cumplan con las condiciones configuradas
- Distribución del tráfico entre los diferentes nodos de la capa acceso

La capa distribución contiene otros nodos que permiten formar segmentos de red más pequeños denominados anillos, con enlaces redundantes para casos de fallas, cuya principal función es administrar los anillos que dependan de ellos. Los nodos de la capa distribución que forman los anillos tienen las siguientes características:

- Definen límites en el tráfico a través del uso de listas de acceso, filtros, políticas, medidas de seguridad, entre otras, con el propósito de determinar cuándo y cómo el tráfico de datos puede acceder a los servicios principales de la red
- Permiten segmentar la red en múltiples dominios de difusión
- Enrutan el tráfico para proporcionar acceso a los grupos de trabajo
- Sirven como punto de concentración para acceder desde los dispositivos de la capa acceso

Los nodos que permiten formar los segmentos no están configurados con tecnología MPLS, pero sí con tecnología IP con el fin de poder administrar los anillos a su cargo y son denominados como:

- SW1AGUIOG
- SW2AGUIOG
- SW1AGUIOM
- SW2AGUIOM

La figura 3.17 indica la conexión los nodos de la capa *core* y la capa distribución, con las respectivas interfaces configuradas a cada extremo de los enlaces, que tienen 1 Gbps de capacidad.

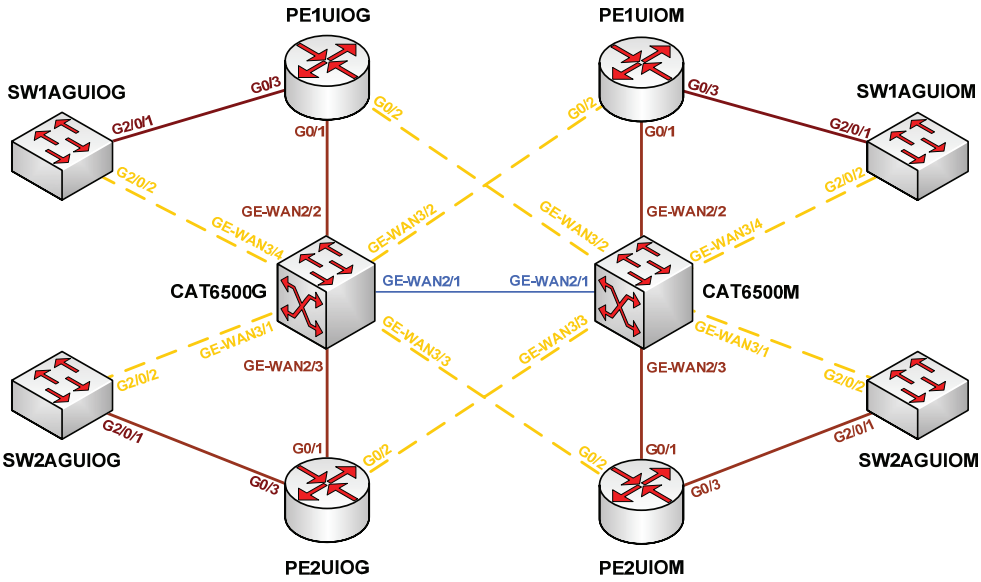

Figura 3.17 Conexión de los nodos de la capas *core* y distribución

3.2.2.5 Descripción de la capa acceso[14]

La capa acceso permite la interconexión de los clientes con la red de Telconet S.A., utilizando como medio de transmisión de última milla la fibra óptica y los enlaces de microondas para los lugares en donde no se pueda acceder con fibra. En esta capa se encuentran múltiples grupos de usuarios que necesitan de diferentes recursos, por lo que los nodos incluyen un número alto de puertos de acceso de forma equilibrada para mantener las solicitudes de acceso dentro de la capacidad de las capas superiores.

Esta capa está formada por 48 nodos distribuidos de forma estratégica dentro de la ciudad de Quito que no soportan tecnología MPLS, formando anillos administrados por los nodos de la capa distribución, con un máximo de siete nodos por anillo. Un anillo ocupa dos puertos del equipo concentrador de la capa distribución, de manera que se tenga enlaces redundantes en caso de falla.

La capa acceso implementa un CPE para interconectar la red del cliente con la red de Telconet S.A.; estos equipos son entregados por la empresa en modalidad de alquiler y permiten manejar los protocolos de capa enlace y capa red para realizar las VPNs.

Los CPEs no manejan tecnología MPLS y dependiendo de los requerimientos y el tipo de acceso que el cliente haya contratado, se manejan dos tipos de enlaces que son punto a punto y multipunto. Los enlaces punto a punto disponen de una última milla sin compartición, en tanto que los enlaces multipunto comparten la última milla.

La figura 3.18 indica la forma en la que los clientes acceden a la red de Telconet S.A. y los medios de transmisión utilizados en la última milla.

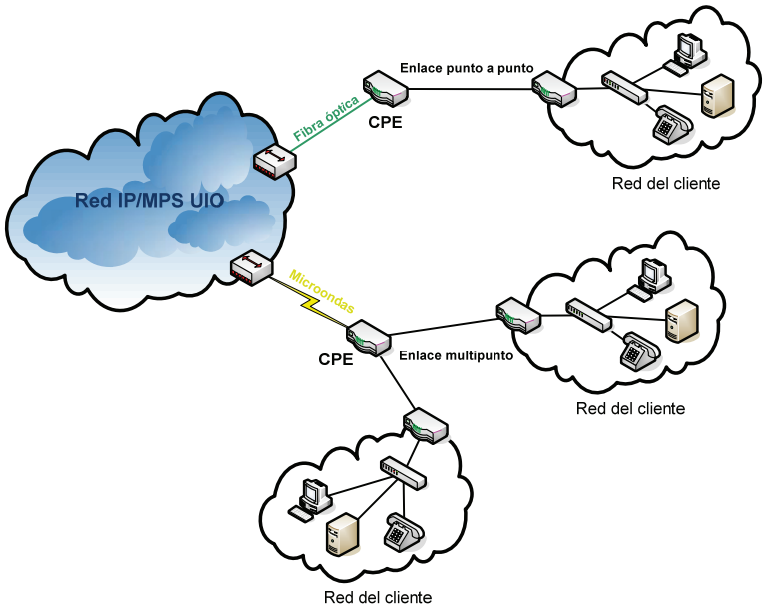

Figura 3.18 Acceso de los clientes a la red IP/MPLS de Telconet S.A.

3.2.2.6 Componentes del *backbone*[14][17]

El *backbone* de la red de Telconet S.A. tiene varios componentes como normativas y tecnologías que permiten su correcta operación. Entre los principales componentes configurados y características en los equipos de la red se tiene:

- Una normativa configurada en los equipos es utilizar los primeros cinco puertos *FastEthernet* y los puertos *GigabitEthernet* de los *switches* del *backbone* para la interconexión de los mismos y un puerto para el monitoreo de los UPS, mientras que el resto de puertos son utilizados para la conexión con los clientes.

- El uso de *Virtual Local Area Networks* (VLANs) para segmentar la red de forma lógica de acuerdo a un uso específico. Se tienen diferentes tipos de VLANs de acuerdo a las necesidades de cada grupo de clientes, tanto para clientes que utilizan enlaces de datos como para clientes con enlaces de Internet, con el propósito de segmentar el tráfico que circula por la red.

3.2.2.7 Protocolos del *backbone*[14]

Los equipos del *backbone* de Telconet S.A. están configurados con diferentes protocolos que les permiten comunicarse, administrar la red, proveer seguridad, evitar casos de congestión, entre otros. Los protocolos configurados son:

- Los *switches* del *backbone* usan el protocolo *Spanning Tree* para evitar la presencia de lazos debido a la existencia de enlaces redundantes. El protocolo asigna ciertos puertos del *switch* a un estado de bloqueo para permitir sólo una trayectoria activa a la vez entre dos dispositivos de la red.
- El protocolo VLAN *Trunking Protocol* (VTP) es configurado en los *switches* para distribuir y sincronizar información acerca de las VLANs, con el fin de minimizar los errores que puedan producirse durante la configuración de las mismas.
- *Security Shell* (SSH) es un protocolo configurado para administrar remotamente a los equipos del *backbone* mediante una comunicación segura, para resolver de forma inmediata los problemas que se presenten en la red.
- El protocolo SNMPv2 es configurado en los equipos del *backbone* para la supervisión del desempeño de la red, de modo que se pueda obtener los datos que permitan la administración de los dispositivos.
- Se utiliza el protocolo de enrutamiento OSPF en los *routers* del *backbone* para enviar el tráfico que permita el cálculo de la ruta más corta posible a un punto. Adicionalmente, se tiene configurado MD5 para autentificar a otros equipos antes de aceptar una nueva ruta.
- BGP-4 es el protocolo configurado para el intercambio de tablas de enrutamiento entre los sistemas autónomos de Telconet S.A., que cuenta con diferentes definiciones de trayectorias hacia Internet.

- El protocolo LDP es el protocolo usado para la distribución de las etiquetas MPLS que serán utilizadas para el establecimiento de los LSPs dentro de la red MPLS de Telconet S.A.

3.2.2.8 Administración de la red[17]

Las funciones de administración de la red de Telconet S.A. son realizadas por los diferentes departamentos de la empresa de acuerdo a sus responsabilidades. La mayoría de los equipos de los departamentos de la empresa salen a través de un equipo configurado como un *proxy*, conectado como un cliente normal al *backbone*, pero con ciertos privilegios de acceso a los equipos del *backbone* o de los clientes, ya que la dirección IP del *proxy* está configurada en todos los equipos de la red para permitir el acceso.

Los equipos del departamento del NOC salen a través de otro equipo configurado de igual manera como un *proxy*, pero con mayores accesos a los equipos de la red, debido a sus funciones de monitoreo tanto de clientes como de equipos de los nodos.

3.2.3 SLAs ESTABLECIDOS POR TELCONET S.A.

Telconet S.A establece SLAs con sus clientes para determinar las condiciones sobre las que se efectuará la prestación de un determinado servicio. Estos SLAs contienen una serie de parámetros valorizados que se indican a continuación:

- La disponibilidad mensual del servicio de Internet sobre la base de 720 horas es del 99%.
- La disponibilidad mensual del servicio de transmisión de datos sobre la base de 720 horas es del 99%.
- La pérdida de paquetes se define como cercana al 0%.
- Las latencias al *backbone* en USA son de 100 ms.
- La latencia hacia portales como *Yahoo* ó *Google* es de 112 ms.
- La presencia de un centro de monitoreo NOC para recibir requerimientos de los clientes, que serán registrados en el sistema mediante la apertura de

un número de seguimiento (*trouble ticket*) y con un MTTR (*Mid Time To Repair*) de 2 horas.

3.3 DISEÑO DE UN ESQUEMA DE CALIDAD DE SERVICIO (QoS) PARA IP/MPLS

La empresa Telconet S.A. maneja la tecnología MPLS en su red de *core* y la tecnología IP en el resto de su red de *backbone*, por lo que se debe trabajar con esquemas de integración de QoS sobre ambas tecnologías. Además, se debe tomar en cuenta los SLAs y los requerimientos de tráfico que la empresa solicite para el diseño del presente proyecto.

3.3.1 ESQUEMA DE QoS PARA EL TRÁFICO DE LA RED DE TELCONET S.A.

La empresa Telconet S.A. eligió migrar a la tecnología MPLS debido a los grandes beneficios que presta para brindar QoS al tráfico que circula por una red. El objetivo de esta migración es poner a disposición de los clientes, diferentes categorías de tráfico y que, durante periodos de congestión, se garantice que las aplicaciones más críticas como la voz y el video, dispongan de mayor prioridad.

La red IP/MPLS de Telconet S.A. fue diseñada por el departamento de Proyectos para que sus enlaces soporten el tráfico de las aplicaciones actuales y de nuevas aplicaciones, de manera que el servicio ofrecido por la empresa esté en función de la capacidad de transmisión que los clientes requieran.

El esquema diseñado de QoS va a administrar los enlaces para asegurar el cumplimiento del ancho de banda contratado por el cliente en el SLA, evitando que se produzcan periodos de congestión y ocasionen una alta tasa de paquetes perdidos, disminuyendo la eficiencia de la red.

Los procedimientos para administrar el ancho de banda en los enlaces de los clientes, eliminarán el tráfico que esté fuera del perfil contratado. Sin embargo, los paquetes que estén seteados con alta prioridad, serán encolados y no

descartados, aunque forman parte del tráfico que esté fuera del perfil contratado ó durante periodos de congestión.

La simulación del esquema diseñado de QoS proporcionará la correcta elección de los parámetros de configuración de los procedimientos para ofrecer las diferentes categorías de tráfico, de modo que se garantice el cumplimiento de las clases de servicio contratadas por el cliente con la empresa.

3.3.2 SLAs OFRECIDOS A LOS CLIENTES

Telconet S.A. desea ofrecer a sus clientes dentro de sus SLAs los servicios denominados “olímpicos”, constituidos por cuatro clases de servicio de acuerdo a un conjunto de parámetros establecidos; las categorías ofrecidas son denominadas como Premium, Oro, Plata y Bronce, y los parámetros comprometidos para cada una de ellas son tasa de paquetes entregados, latencia y *jitter*. La tabla 3.2 indica los parámetros comprometidos para cada CoS.

Parámetro	Clase de Servicio (CoS)			
	Premium	Oro	Plata	Bronce
Paquetes entregados	99,9%	99,5%	99,0%	-
Latencia	28 ms	68 ms	-	-
Jitter	15 ms	-	-	-

Tabla 3.2 Parámetros comprometidos por Clase de Servicio (CoS)

3.3.3 REQUERIMIENTOS DEL TRÁFICO DE TELCONET S.A.

El departamento de Proyectos de Telconet S.A. solicita que algunos agregados de tráfico que circulan por la red deben tener un cierto nivel de prioridad definido dentro de los requerimientos de la empresa; los agregados de tráfico que deben ser tomados en cuenta y el nivel de prioridad que deben tener se indican a continuación:

- El tráfico generado por la tecnología TDMoIP que manejan algunos CPEs debe recibir la máxima prioridad para evitar retardos y obtener valores de *jitter* menores a 20 ms.
- El tráfico de VoIP siendo una aplicación en tiempo real debe cumplir con valores de retardo y *jitter* mínimos, por lo que debe recibir alta prioridad.
- El tráfico *streaming* es una aplicación sensible al *jitter* por lo que su prioridad debe ser alta.
- El tráfico de aplicaciones empresariales personalizadas como bases de datos o de algún protocolo en particular deben recibir una prioridad media.

Los agregados de tráfico mencionados deben tener las prioridades indicadas dentro del tráfico de red ó tráfico cliente que maneja la empresa.

3.3.4 ELECCIÓN DE LA ARQUITECTURA DE QoS

De acuerdo a la IETF, se tienen dos arquitecturas que permiten establecer QoS en equipamientos de red, cada una claramente diferenciada por su modo de operación y denominadas como Servicios Integrados (IntServ) y Servicios Diferenciados (DiffServ). Ambas arquitecturas son soportadas por la tecnología IP y pueden ser integradas con la tecnología MPLS.

La arquitectura de Servicios Diferenciados (DiffServ) es la más usada por la mayoría de ISPs, gracias a las ventajas que ofrece sobre la arquitectura de Servicios Integrados (IntServ) como su buen funcionamiento, flexibilidad, escalabilidad, entre otras. El tratamiento diferenciado de los agregados de tráfico es la filosofía sobre la que se basa esta arquitectura para dotar de QoS a las redes IP.

De acuerdo a los motivos expuestos, se designa a la arquitectura de DiffServ como la base para el desarrollo del presente esquema de QoS, utilizando el RFC 3270 para la integración con la tecnología MPLS.

3.3.5 DESCRIPCIÓN DE LOS PHBs

La arquitectura DiffServ maneja el concepto de PHBs para definir la planificación, el encolamiento y la política de un nodo con un paquete perteneciente a un agregado de tráfico, es decir, el tratamiento de retransmisión que recibirá ese paquete. Se tienen cuatro estándares disponibles de PHBs con sus respectivos valores DSCP, de los cuales se van a utilizar sólo tres estándares con algunos valores DSCP escogidos para clasificar el tráfico de la red en el diseño, que serán acordes con las categorías y los parámetros indicados en la **sección 3.3.1**.

3.3.5.1 *Default* PHB

El *default* PHB tiene un valor de DSCP igual a 000000 según el RFC 2474 y el servicio ofrecido es igual al de "mejor esfuerzo" tradicional. El tráfico perteneciente a este PHB no recibirá ningún tipo de tratamiento y será atendido luego de los PHBs EF y AF.

3.3.5.2 *Assured Forwarding* (AF) PHB

El AF PHB está descrito en el RFC 2597 para "asegurar" que el tráfico conforme al perfil contratado para un flujo sea entregado sin pérdidas con probabilidad muy alta, definiendo 4 clases AF para reservar recursos y 3 categorías de descarte.

Para el presente diseño, se va a hacer uso de la clase 1, clase 2 y clase 3 del AF PHB, que van a corresponder a las clases de servicio Oro, Plata y Bronce respectivamente, definidas en los SLAs que la empresa desea ofrecer, con 2 categorías de preferencia de descarte, bajo y alto. La tabla 3.3 indica los valores DSCP asignados a las clases de servicio de los SLAs.

% de descarte	Oro	Plata	Bronce
Bajo	AF11=001010	AF21=010010	AF31=011010
Alto	AF13=001110	AF23=010110	AF33=011110

Tabla 3.3 Valores DSCP correspondientes a las CoS

Este PHB utilizará el tipo de encolamiento *Low Latency Queueing* (LLQ) como medida de control de congestión, utilizando las colas de prioridad personalizadas con WFQ basado en clases (CBWFQ). Con ello se podrá especificar la cantidad exacta de ancho de banda del enlace para cada una de las clases de servicio, de manera que se pueda cumplir con los parámetros comprometidos en los SLAs.

Con el fin de evitar la congestión, se configurará el mecanismo *Weighted Random Early Detection* (WRED) para proporcionar un mecanismo de descarte aleatorio en base a los diferentes agregados AF con sus diferentes preferencias de descarte.

3.3.5.3 *Expedited Forwarding* (EF) PHB

Definido en el RFC 2598, el EF PHB tiene un valor de DSCP igual a 101110 y ofrece un servicio de bajas pérdidas, baja latencia, bajo *jitter* y un ancho de banda asegurado para aplicaciones en tiempo real.

Este PHB corresponderá a la clase de servicio Premium definida en los SLAs de la empresa, por ser el servicio con mejores prestaciones en lo que se refiere a parámetros de calidad de servicio.

El tipo de encolamiento que se utilizará en este PHB para controlar la congestión será *Low Latency Queueing* (LLQ), usando la cola de prioridad que tiene preferencia absoluta sobre las colas del mecanismo CBWFQ configurado en el AF PHB, de manera que el tráfico asignado sea atendido de forma inmediata y, en caso de que no exista tráfico en la cola, el resto de colas sean atendidas, evitando el desperdicio de recursos.

El EF PHB no necesita un mecanismo de evasión de congestión, ya que el tráfico asignado tiene siempre prioridad sobre otro tráfico y no se esperan situaciones de congestión. Sin embargo, si no se configura ningún mecanismo, se utiliza por defecto a *tail drop*.

3.3.6 ASIGNACIÓN DE VALORES DSCP AL TRÁFICO DE LA RED

La tabla 3.4 indica los resultados obtenidos en el análisis realizado en la **sección 2.3.6** sobre el tráfico recibido de las aplicaciones por categoría en la semana de monitoreo, indicando los protocolos y aplicaciones asignados a cada categoría indicada.

Categoría	Protocolos y aplicaciones	% de tráfico rx
Navegación vía web	HTTP	70,90%
P2P	*Ares* UDP, *BitTorrent*, *eDondkey*, *Ares*, *Gnutella*, *RapidShare*	23,63%
Tunelización	SSL, IPsec, SSH, GRE	3,66%
Protocolos *streaming*	*YouTube*, *Flash Vídeo*, RTSP, QQLive	1,81%
VoIP	*Skype*, *UniqueFone*, SIP, RTP, SIP, H.323 *Data*, *Skype In/Out*, MSN *Media Data*	Despreciable
Juegos	Xbox Live, *World of Warcraft*, *Yahoo games*, *Blizzard Battle.net*, *PlayStation2 Unclassified*, *PlayStation2 Control*	Despreciable

Tabla 3.4 Tráfico recibido de las aplicaciones durante el monitoreo

La tabla 3.5 indica los resultados obtenidos en el análisis realizado en la **sección 2.3.6** sobre el tráfico transmitido de las aplicaciones por categoría en la semana de monitoreo, indicando los protocolos y aplicaciones asignados a cada categoría indicada.

Categoría	Protocolos y aplicaciones	% de tráfico tx
P2P	*eDondkey Encripted*, *Ares* UDP, *BitTorrent*, *eDondkey*, *Ares*	72,26%
Navegación vía web	HTTP, *Facebook*	16,55%
Tunelización	SSL, IPsec, SSH, GRE	7,16%
VoIP	*Skype*, *UniqueFone*, SIP, H.323 *Data*, *Skype In/Out*, MSN *Media Data*	2,25%
Protocolos *streaming*	*YouTube*, *Flash Vídeo*, QQLive, *Symantec Live Update*	1,78%
Juegos	*World of Warcraft*, *Yahoo games*, *Blattlefield* 2	Despreciable

Tabla 3.5 Tráfico transmitido de las aplicaciones durante el monitoreo

El tráfico indicado en las tablas 3.4 y 3.5 tendrá un valor de DSCP asignado para distinguir el tratamiento que recibirá durante su transmisión por la red. Además, se debe tomar en cuenta otros agregados de tráfico que circulan por la red, como son:

- Servicios web: HTTPS
- Correo electrónico: SMTP, POP3, IMAP4
- Infraestructura de red: DNS, DHCP, ICMP, SNMP
- Terminales: TELNET, SSH, VNC
- Videoconferencia: RTSP
- Bases de datos
- Transferencia de archivos: NFS, FTP, SFTP, Syslog

Los diferentes tipos de tráfico van a ser clasificados de acuerdo a los requerimientos de la empresa y a los requerimientos de QoS expuestos en el **Capítulo 2** dentro de los PHBs descritos con anterioridad, de la siguiente manera:

- El servicio Premium estará orientado a la aplicación con mayores exigencias de QoS, la VoIP, debido a que es la aplicación de tiempo real que tiene un comportamiento bastante regular y no sería necesario configurar una gran cantidad de ancho de banda en el EF PHB para eliminar las ráfagas de datos que originarían otras aplicaciones.
- El servicio Oro será para las aplicaciones *streaming* por ser el AF PHB con mejores prestaciones de QoS para cumplir con las exigencias que este tipo de tráfico requiere en cuanto a retardo, *jitter* y tasa de paquetes perdidos.
- El servicio Plata brindará QoS al tráfico orientado a las aplicaciones de tipo empresarial como bases de datos, tunelización y transacciones seguras, transmitido por los clientes corporativos como empresas, bancos, y comisariatos, que requieren mejores prestaciones para acceder a sus redes privadas.
- El servicio Bronce será destinado a los protocolos y aplicaciones del tráfico para la administración de la red, que generalmente es considerado de "mejor esfuerzo", pero que debe tener un mejor tratamiento para acceder y resolver de forma rápida los problemas que se presenten en el *backbone*.
- El servicio "mejor esfuerzo" no recibirá ningún tipo de QoS, acogiendo el resto de aplicaciones que circulan por la red y que no hayan sido marcadas con valores DSCP para recibir un determinado tratamiento durante su transmisión.

Tomando en cuenta todas las consideraciones y los requerimientos de QoS de los diferentes tipos de tráfico, la tabla 3.6 indica la clasificación de tráfico y los respectivos valores DSCP que se utilizarán para marcarlo.

El tráfico de navegación vía web y P2P corresponde a la mayoría del tráfico que circula por la red, pero es considerado de "mejor esfuerzo" porque no requiere servicios de QoS, sino que consume recursos necesarios para otras aplicaciones como las de tiempo real.

El tráfico de tunelización está presente luego del tráfico de navegación vía web y P2P porque la mayoría de clientes de Telconet S.A. son corporativos y se enlazan con sus sucursales a través de VPNs. A pesar de que los requerimientos de QoS

de este tráfico no son tan exigentes, debe tener un mejor tratamiento de acuerdo a los requerimientos de tráfico de la empresa.

CoS	Valor DSCP	Tipo de aplicación
Premium	EF=46	VoIP (TDMoIP, RTP, *Skype*, *Net2Phone*, *UniqueFone*, SIP, H.323)
Oro	AF11=10	Videoconferencia (RTSP)
	AF13=14	Aplicaciones *streaming* personalizadas
Plata	AF21=18	Bases de datos, SSL, IPsec, GRE, L2TP
	AF23=22	Transacciones web (HTTPS), SFTP
Bronce	AF31=26	SNMP, TELNET, SSH
	AF33=30	SMTP, POP3, IMAP4, VNC, Syslog, DHCP, ICMP
Mejor esfuerzo	BE=0	P2P, juegos, HTTP, *Facebook*, FTP, NFS, DNS y el resto de aplicaciones que cursan por la red y que no recibirán ninguna garantía de QoS

Tabla 3.6 Clasificación y asignación de valores DSCP al tráfico de la red

3.3.7 CLASIFICACIÓN Y ACONDICIONAMIENTO DE TRÁFICO

Dentro de la red de Telconet S.A. circula tráfico originado por los clientes y tráfico destinado a la administración de la misma, que debe ser tratado de acuerdo a ciertas condiciones.

El tráfico cliente debe ser tratado de acuerdo al SLA que haya contratado con la empresa, bajo los parámetros de QoS estipulados en el contrato y los puntos desde donde se debe ofrecerla.

El tráfico de red está determinado por los requerimientos de QoS para un determinado tipo de tráfico, de manera que se ofrezcan soluciones rápidas y eficientes ante fallas en la operación del *backbone*.

La capa acceso implementa un CPE en el lado del cliente, entregado en modalidad de alquiler y administrado por la empresa. Se ofrece la oportunidad de brindar una QoS extremo a extremo, ya que el módulo de clasificación de tráfico de la arquitectura Diffserv será establecido dentro del dominio origen, simplificando este proceso porque el tráfico está menos mezclado y las reglas son más sencillas mientras más cerca se está del origen.

Las funciones de administración de la red son realizadas a través de equipos conectados como clientes normales al *backbone*, por lo que el módulo de clasificación será establecido en dichos equipos para brindar QoS

El tráfico cliente y el tráfico de red serán clasificados utilizando un clasificador *Multi-field* (MF), de manera que se seleccione los paquetes combinando a uno ó más de los siguientes campos de la cabecera:

- Dirección IP origen
- Dirección IP destino
- Puerto origen
- Puerto destino
- Protocolo

Los paquetes clasificados serán marcados con los valores DSCP para asociarlos con las CoS definidas en los SLAs y entregarlos al módulo de acondicionamiento. Estos valores fueron asignados a cada tipo de tráfico en base a los requerimientos de la empresa y de QoS indicados. Sin embargo, esta asignación puede variar en el tráfico cliente dependiendo del servicio contratado con la empresa dentro del SLA para un determinado tipo de tráfico.

El módulo de acondicionamiento mide el flujo de tráfico originado en la red del cliente y lo compara con el perfil respectivo, de modo que los paquetes que estén fuera del perfil, sean descartados para asegurar el cumplimiento del SLA contratado y prevenir la congestión. Este módulo estará ubicado dependiendo del

tipo de enlace contratado y utilizará el algoritmo *token bucket* para medir el tráfico entrante del cliente y compararlo con el ancho de banda contratado en el SLA.

En los enlaces punto a punto, la última milla no es compartida, por lo que los CPEs no necesitan administrar el ancho de banda, de modo que el módulo de acondicionamiento se ubicará en los puertos del equipo de la capa acceso del cual dependan.

Los enlaces multipunto disponen de una última milla compartida, por lo que los CPEs deben administrar el ancho de banda para que determinadas aplicaciones de los clientes no superen el ancho de banda contratado y provoquen la saturación del canal de transmisión.

Los paquetes pre-marcados y acondicionados ingresarán a la red del proveedor para ser distribuidos mediante un clasificador *Behavior Aggregate* (BA) en base al subcampo DSCP que contienen y definir el tratamiento que recibirán durante su transmisión por la red.

3.3.8 ELECCIÓN DEL MÉTODO DE QoS SOBRE MPLS

El problema en la integración de Diffserv con MPLS consiste en la traducción de los valores DSCP a las etiquetas MPLS, de manera que los requerimientos de QoS de los agregados de tráfico se respeten durante su transmisión por ambas tecnologías. Con el fin de permitir esta integración, el RFC 3270 recomienda dos métodos de QoS denominados como E-LSP y L-LSP, descritos con anterioridad en la **sección 3.1.4**.

El método que se escoge para brindar QoS en la red de Telconet S.A. es el E-LSP porque es un método no escalable, con un número máximo de ocho PHBs, evitando que los equipos de la red de *core* donde se debe hacer la integración no mantengan una gran cantidad de correspondencias entre valores DSCP, campo EXP y PHBs, ya que deben reenviar el tráfico a altas velocidades y evitar nuevas configuraciones que disminuyan el procesamiento en la conmutación de paquetes.

3.3.9 DEFINICIÓN DEL MAPA DE CORRESPONDENCIAS

El método E-LSP permite transmitir información de la CoS de la cabecera IP a los LSRs en la cabecera MPLS, determinando el PHB al que pertenece un paquete en base al campo EXP de la etiqueta MPLS. Haciendo uso de este método es posible utilizar hasta ocho PHBs por cada LSP, por lo que es necesario definir y configurar el mapa de correspondencia entre los valores DSCP y el campo EXP.

La tabla 3.7 indica la correspondencia entre los valores DSCP definidos en los PHBs descritos para clasificar el tráfico transmitido a través de la red y los valores exp7-exp0 del campo EXP, que serán mapeados en los nodos de borde LERs de la red MPLS.

CoS	Valor DSCP	Valor EXP
Premium	EF	exp7
Oro	AF11	exp6
	AF13	exp5
Plata	AF21	exp4
	AF23	exp3
Bronce	AF31	exp2
	AF33	exp1
Mejor esfuerzo	BE	exp0

Tabla 3.7 Mapa de correspondencias entre el subcampo DSCP y el campo EXP

3.3.10 ELECCIÓN DEL MODO DE TUNELIZACIÓN DE DIFFSERV SOBRE MPLS

Los modos de tunelización de DiffServ sobre MPLS permiten manejar la QoS que un *router* proveerá a un paquete MPLS en una red con tecnología MPLS, de modo que se pueda interactuar el campo DS de DiffServ en la cabecera IP y en la cabecera MPLS.

De acuerdo al RFC 3270, existen tres modos de tunelización que afectan el comportamiento de los LERs y de los penúltimos LSRs del LSP, siendo soportados sólo por el método E-LSP; estos modos son uniforme, tubería y tubería corta, cuyo funcionamiento fue descrito en la **sección 3.1.5**.

El CPE entregado al cliente por la empresa no soporta tecnología MPLS y los paquetes son pre-marcados en el origen, por lo que siguiendo las recomendaciones de la **sección 3.1.5.4** sobre la determinación del modo de tunelización apropiado, se escoge el modo tubería corta para brindar QoS a los paquetes que son transmitidos por la red de *core* con tecnología MPLS de la empresa Telconet S.A.

El modo tubería corta provee de QoS transparente mediante la preservación del marcado IP de los paquetes y los clasifica en la interfaz de salida del LER de egreso en base al subcampo DSCP.

REFERENCIAS CAPÍTULO 3

PROYECTOS DE TITULACIÓN

[1] MARCHÁN, Julia; YÁNEZ, Daniel. “Estudio y diseño para la migración de una red gigabit ethernet de datos de una empresa portadora de servicios a la tecnología MPLS”. EPN. Abril 2008

ARTÍCULOS E INTERNET

[2] LE FAUCHEUR, F. “Multi-Protocol Label Switching (MPLS) support of Differentiated Services”. IETF RFC 3270. 2002

[3] DREILINGER, Tímea. “DiffServ and MPLS”
http://saturn.acad.bg/bis/pdfs/04_doklad.pdf

[4] JIMÉNEZ, Raúl. “Integración de MPLS y DiffServ en una arquitectura para la provisión de QoS”
http://gitaca.es/javiercg/uploads/ES/jimenez05jitel.pdf

[5] SIENRA, Luis Gabriel. “Ofreciendo Calidad de Servicio mediante MPLS: Fundamentos y aplicación a las redes de cable”.
http://www.cinit.org.mx/articulo.php?idArticulo=14

[6] RAHUL, Asha. “MPLS DiffServ: A combined approach”
https://guinness.cs.stevens-tech.edu/~lbernste/papers/MPLSDiffServ.pdf

[7] IP IN FUSION. “Quality of Service and MPLS methodologies”
http://www.ipinfusion.com/pdf/IP_InfusionQoS_MPLS2.pdf

[8] IBARRA, Edwin. “MPLS (MultiProtocol Label Switching) y Calidad de Servicio en las redes IP”.
http://www.tecnologicoamper.com/descargas/seminario01CC.pdf

[9] CISCO SYSTEMS. “DiffServ tunneling modes for MPLS networks”
http://www.cisco.com/en/US/tech/technologies_note09186a008022ad7e.shtml

[10] CISCO SYSTEMS. “MPLS DiffServ tunneling modes”
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftdtmode.html

[11] GEROMETTA, Oscar. “Elementos básicos de QoS”
http://librosnetworking.blogspot.com/2008/04/elementos-bsicos-de-qos.html

[12] VEGA, Carlos. “Algoritmos de Optimización de Tráfico en redes WAN” http://www.eumed.net/libros/2008a/348/Algoritmos%20de%20Optimizacion%20de%20Trafico%20en%20redes%20WAN.htm

[13] ANÓNIMO. “Disciplinas de cola simples, sin clases” http://www.gulic.org/almacen/03_www/comos/LARTC/html/x660.html

OTROS

[14] ALVARADO, Alexandra. “Diagrama MPLS”. ESP PROY 06 Ver 07 May 08

[15] PROAÑO, Hugo. “Manual de procedimiento para el tendido de la fibra óptica de Telconet S.A.”. Enero 2008

[16] PROAÑO, Hugo. “Descripción y generalidades de la red de backbone de Telconet S.A.”. Instructivo INS UIO BACK 2008

[17] PROAÑO, Hugo. “Manual de procedimientos de Telconet S.A.”. Enero 2008

CAPÍTULO 4

CONFIGURACIÓN Y SIMULACIÓN DEL ESQUEMA DE CALIDAD DE SERVICIO (QoS)

4.1 ANÁLISIS TÉCNICO DE LA RED DE TELCONET S.A. PARA EL SOPORTE DE QoS

El esquema de QoS diseñado va a ser configurado en los equipos del núcleo de la red de Telconet S.A., por lo que se debe realizar un análisis de los modelos de los equipos, los tipos de módulos, las características técnicas que poseen y las versiones de IOS, con el fin de establecer la forma en la que se soportarán los mecanismos de QoS propuestos, ya que no todos los equipos configuran QoS de la misma forma ó en su defecto sólo permiten configurar ciertos mecanismos.

4.1.1 MODELOS DE LOS EQUIPOS DEL NÚCLEO DE LA RED DE TELCONET S.A.

Los equipos del núcleo de la red de Telconet S.A. utilizan plataforma certificada marca Cisco por su reconocimiento a nivel mundial, gracias a las ventajas que ofrecen sobre otras marcas como su amplio portafolio de tecnologías y dispositivos de extremo a extremo, confiabilidad, seguridad, certificaciones, entre otras. A continuación se indica los modelos de los equipos implementados en la red de Telconet S.A.

4.1.1.1 Equipos de la capa *core*

Los dos nodos principales de la capa *core* están configurados tanto con IP por la presencia de un enlace con la capa distribución y como con MPLS para trabajar como LSRs, utilizando un *switch* marca Cisco modelo Catalyst WS-C6509-E cada uno. La figura 4.1 indica el modelo de los equipos de estos nodos. La capacidad total de la red de *core* es de 10 Gbps de acuerdo al modelo de las tarjetas de los equipos.

Figura 4.1 Equipo Cisco Catalyst WS-C6509-E[5]

La capa *core* también implementa otros nodos que distribuyen grandes cantidades de tráfico y permiten la migración de la tecnología IP a la tecnología MPLS, configurados para trabajar como LSRs y LERs a la vez. Los equipos de estos nodos son *routers* marca Cisco modelo 7206 VXR. La figura 4.2 indica el modelo de los equipos mencionados.

Figura 4.2 Equipo Cisco 7206 VXR[6]

4.1.1.2 Equipos de la capa distribución

La capa distribución está formada por los nodos PE indicados en la capa *core*, debido a que realizan funciones concernientes a esta capa, y por otros nodos utilizados para formar anillos. Los equipos de los nodos que forman los anillos mantienen un balance de carga para mejorar el desempeño en la administración de la red y son *switches* marca Cisco modelo WS-C3750G-12S. La figura 4.3 indica el modelo de los equipos de estos nodos. La capacidad total de la red de distribución es de 1 Gbps de acuerdo al modelo de las tarjetas de los equipos.

Figura 4.3 Equipo Cisco WS-C3750G-12S[7]

4.1.2 TIPOS DE MÓDULOS DE EXPANSIÓN EN LOS EQUIPOS DE LA RED DE TELCONET S.A.

La marca Cisco ofrece una gran variedad de módulos de conectividad para los diferentes modelos de sus equipos, de manera que los clientes puedan elegir una solución que se ajuste a sus necesidades y expanda el soporte de nuevas tecnologías en sus equipos. Estos módulos permiten incrementar el rendimiento, el número de puertos ó incluir servicios adicionales.

Algunos equipos de la red de Telconet S.A. incluyen módulos con características de soporte de QoS que deben ser analizados para determinar la forma en que se va a configurar el esquema de QoS diseñado. Los módulos incluidos en los equipos de la red son los siguientes:

- Cada *switch* Cisco Catalyst WS-C6509-E de la capa *core* tiene dos módulos modelo *Enhanced Optical Services Modules* (OSM) con cuatro puertos WAN *Gigabit Ethernet* y dos puertos LAN *Gigabit Ethernet* cada uno (OSM-2+4GE-WAN+).
- Los *switches* Catalyst WS-C6509-E también incluyen una tarjeta de características de perfiles (PFC) modelo PFC3BXL que provee de características avanzadas de QoS y de seguridad.

4.1.3 CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS DE TELCONET S.A.

El núcleo de la red de Telconet S.A. tiene implementado diferentes modelos de equipos y módulos, por lo que se debe realizar un análisis de las características técnicas que poseen, relacionadas con el soporte de los mecanismos para ofrecer QoS al tráfico de la red.

4.1.3.1 Características de los equipos de la capa *core*[1][2][8][9]

El equipo Cisco Catalyst WS-C6509-E de la capa *core* posee las siguientes características en cuanto al soporte de QoS:

- Configuración de mapas de clases y mapas de políticas

- Clasificación de paquetes marcados en base al subcampo Precedencia, subcampo DSCP ó campo EXP
- Configuración de QoS sobre la tecnología MPLS usando los modos de tunelización
- Soporte de los procedimientos de control de congestión LLQ y CBWFQ
- Soporte de los mecanismos de evasión de congestión *tail drop* y CBWRED
- Acondicionamiento y conformación de tráfico

Los equipos Catalyst WS-C6509-E de la capa *core* están configurados con IP y MPLS, por lo que sus funciones para ofrecer QoS son agrupar los paquetes con un clasificador BA en base al campo EXP ó al subcampo DSCP, traducir el subcampo DSCP de IP al campo EXP de MPLS con el método E-LSP, manejar la QoS sobre MPLS con el modo de tunelización tubería corta y enviar los paquetes al siguiente nodo de acuerdo al PHB que les corresponde.

Las características técnicas de los equipos indicados soportan las funciones que deben tener los nodos para proveer de QoS a la red de Telconet S.A., así como los mecanismos y métodos definidos en el diseño del esquema de QoS para proveer del tratamiento diferenciado a los agregados de tráfico en la red con tecnología MPLS.

El equipo Cisco 7206 VXR de la capa *core* posee las siguientes características relacionadas al soporte de QoS:

- Clasificación de paquetes utilizando Listas de Control de Acceso (ACLs)
- Soporte de *Modular* QoS *command-line interface* (MQC)
- Clasificación de paquetes marcados en base al subcampo Precedencia, subcampo DSCP ó campo EXP
- Clasificación de paquetes en base a la aplicación con *Network-Based Application Recognition* (NBAR)
- Configuración de QoS sobre la tecnología MPLS usando los modos de tunelización
- Soporte de los procedimientos de control de congestión LLQ y CBWFQ
- Soporte de los mecanismos de evasión de congestión *tail drop* y CBWRED
- Imposición y disposición de etiquetas MPLS

- Acondicionamiento y conformación de tráfico

Los equipos Cisco 7206 VXR de la capa *core* están configurados para permitir la integración entre las tecnologías IP y MPLS, por lo que sus funciones para ofrecer QoS son agrupar los paquetes con un clasificador BA en base al subcampo DSCP, traducir el subcampo DSCP de IP al campo EXP de MPLS con el método E-LSP, agrupar los paquetes con un clasificador BA en base al campo EXP, manejar la QoS sobre MPLS con el modo de tunelización tubería corta y enviar los paquetes al siguiente nodo de acuerdo al PHB que les corresponde.

Las características técnicas que poseen los equipos mencionados soportan las funciones que estos nodos deben realizar para proveer de QoS a la red de Telconet S.A., así como los mecanismos y métodos definidos en el diseño del esquema de QoS para proveer del tratamiento diferenciado a los agregados de tráfico.

4.1.3.2 Características de los equipos de la capa distribución[3]

El equipo WS-C3750G-12S de la capa distribución soporta las siguientes características de QoS:

- Marcación y clasificación por dirección IP origen, dirección IP destino, dirección MAC origen, dirección MAC destino o número de puerto TCP/UDP en capa 4
- Clasificación de paquetes utilizando Listas de Control de Acceso (ACLs)
- Clasificación de paquetes marcados en base a 802.1p Clase de Servicio ó subcampo DSCP
- Soporte de cuatro colas de egreso por puerto para un control diferenciado de hasta cuatro tipos de tráfico
- Programación de envío de datos con *Shaped Round Robin* (SRR) para una priorización diferenciada de flujos de paquetes a través de un servicio inteligente de las colas de ingreso y egreso
- *Weigted Tail Drop* (WTD) para evadir la congestión en las colas de ingreso y egreso antes que se produzca

- Encolamiento prioritario estricto PQ para asegurar que los paquetes de más alta prioridad sean servidos antes que el resto de tráfico

Los equipos WS-C3750G-12S de la capa distribución están configurados con tecnología IP para enrutar el tráfico proveniente de los equipos de la capa acceso, por lo que sus funciones para ofrecer QoS son agrupar los paquetes con un clasificador BA en base al subcampo DSCP y enviarlos al siguiente nodo de acuerdo al PHB que les corresponde.

Las características técnicas de los equipos Cisco 3750 para el soporte de QoS utilizan mecanismos diferentes a los indicados para los equipos mencionados anteriormente, aunque los parámetros de configuración y los conceptos sobre los que se basan son similares.

La configuración de los equipos Cisco 3750 será realizada utilizando los mecanismos que soporta para brindar QoS, pero basándose en los procedimientos propuestos en el diseño del esquema de QoS para brindar el tratamiento indicado a los diferentes tipos de tráfico que circulan por la red de la empresa.

4.1.4 ANÁLISIS DE LAS VERSIONES DE IOS DE LOS EQUIPOS[11]

Los diferentes modelos de dispositivos de red marca Cisco dependen de dos tipos de software para su funcionamiento, el IOS y la configuración.

El *Internetwork Operating System* (IOS) es un sistema operativo creado por la empresa Cisco Systems para programar y mantener sus equipos de interconexión de redes informáticas como *switches*, *routers*, *firewalls*, entre otros. Este software facilita la operación básica de los componentes de hardware del dispositivo.

Los archivos de configuración contienen los comandos del software IOS de Cisco utilizados para personalizar la funcionalidad de un dispositivo Cisco. Los comandos son analizados por el software IOS de Cisco cuando inicia el sistema o cuando se ingresan los comandos en modo configuración.

Los comandos que pueden ser utilizados para configurar un equipo dependen en gran medida de la versión de IOS instalada, independientemente de las tecnologías que dichos equipos puedan soportar. Por este motivo, se debe realizar un análisis de las versiones de IOS instaladas en los equipos de la red de Telconet S.A. para el soporte de la configuración del esquema de QoS diseñado. La tabla 4.1 indica las versiones de IOS instaladas actualmente en los equipos de la red de la empresa.

Equipo	Versión de IOS
Cisco Catalyst WS-C6509-E	12.2(18)SXE6
Cisco 7206 VXR	12.4(4)XD7
Cisco WS-C3750G-12S	12.2(25)SEB4

Tabla 4.1 Versiones de IOS de los equipos de Telconet S.A.

De acuerdo a las indicaciones de los manuales de configuración de QoS de los diferentes equipos, la versión de IOS recomendada para configurar la arquitectura DiffServ y QoS en MPLS es 12.2(13)T o superior, por lo que si se realiza un análisis de los datos de la tabla 4.1, se concluye que no es necesario actualizar el IOS en los equipos de la empresa para configurar el esquema de QoS diseñado.[10][12][13][14][15][16][17]

4.2 CONFIGURACIÓN DEL ESQUEMA DISEÑADO DE CALIDAD DE SERVICIO (QoS)

Una vez analizadas las características técnicas de los equipos del núcleo de la red de Telconet S.A., se procederá a indicar y describir los comandos de configuración para el desarrollo del esquema de QoS diseñado. La configuración será realizada en un nodo por capa del modelo jerárquico, que servirá de ejemplo para la configuración del resto de nodos de la red.

4.2.1 HERRAMIENTAS DE CISCO PARA LA CONFIGURACIÓN DE QoS[18][19][20][21][22]

El software IOS de Cisco brinda herramientas muy útiles que permiten la configuración de los comandos para el soporte de QoS. Cisco IOS brinda varias posibilidades que dependen de las características que posea el equipo, como son:

- **Configuración por *Command Line Interface* (CLI):** Configura manualmente interfaz por interfaz las opciones de QoS. Es un método poco escalable.
- **Configuración por *Modular* QoS *CLI* (MQC):** Permite una configuración modular de QoS a partir de la definición de clases y políticas. Es la opción más apropiada para la configuración detallada de QoS en dispositivos Cisco IOS actualmente.
- ***Multilayer Switching* QoS (MLS):** Provee de una configuración de QoS basada en hardware para algunas series de *switches* Cisco, usado para identificar características de tráfico y brindar QoS a través del uso de colas.
- ***Auto*QoS *Enterprise***: Implementación que en base a la operación de *Network Based Application Recognition* (NBAR) detecta hasta 10 tipos diferentes de tráfico que atraviesan enlaces WAN. Disponible a partir de la versión de IOS 12.3(7)T.

La configuración por MQC está disponible en los equipos del núcleo de la red de Telconet S.A. Esta configuración utiliza dos procedimientos básicos de clasificación y asignación de prioridad para manipular los agregados de tráfico y otorgarles QoS, denominados como mapas de clases y mapas de políticas.

Un mapa de clase es un mecanismo que agrupa un tipo de tráfico de la red bajo un mismo criterio, de tal manera que los paquetes agrupados tengan un mismo tratamiento cuando lleguen al equipo. El criterio permite comparar el tráfico entrante y clasificarlo, usando varias herramientas de clasificación como ACL estándar o extendida, dirección IP, subcampo DSCP, campo EXP de MPLS ó NBAR. Los agregados de tráfico que no entren en ningún mapa de clase, pertenecen a la clase de tráfico por defecto que puede ser configurada por el usuario, pero no eliminada.

Un mapa de política asocia mapas de clases y especifica las acciones que se tomarán sobre esas clases. Las acciones pueden ser confiar en los valores de CoS, DSCP o Precedencia de la clase de tráfico, establecer un valor específico de éstos ó especificar las limitaciones de ancho de banda y la acción a tomar cuando el tráfico cae fuera del perfil definido en el mapa de política. Previo a que un mapa de política sea efectivo, debe ser adjuntado a una interfaz.

La configuración por MLS está disponible en los *switches* del núcleo de la red de Telconet S.A. Esta configuración trabaja bajo los conceptos de uso de *Shaped Round Robin* (SRR) y *Weighted Tail Drop* (WTD).

Shaped Round Robin (SRR) es un mecanismo de conformación que limita el tráfico saliente en las colas. Este mecanismo es configurado mediante la asignación de un peso máximo a cada cola, convertido en un porcentaje de ancho de banda del enlace. El tráfico en cada cola es conformado de acuerdo al peso configurado, usando el ancho de banda convertido en base al peso asignado.

Weighted Tail Drop (WTD) es una versión mejorada del mecanismo de evasión de congestión *tail drop*. WTD es usado para diferenciar clases de tráfico y regular los tamaños de las colas en base a la clasificación realizada.

4.2.2 TOPOLOGÍA FÍSICA DE LOS NODOS A SER CONFIGURADOS

Como se indicó anteriormente, la configuración será realizada sobre un nodo por capa del modelo jerárquico. La figura 4.4 indica las conexiones de los nodos que van a ser configurados como ejemplo para el resto de equipos de la red, con sus respectivas interfaces a cada extremo de los enlaces.

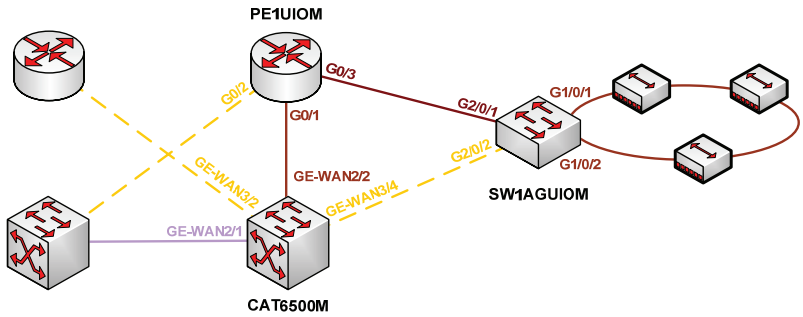

Figura 4.4 Topología física de los equipos a ser configurados

4.2.3 CONFIGURACIÓN DEL NODO SW1AGUIOM DE LA CAPA DISTRIBUCIÓN[15][16]

Los nodos de la capa distribución envían y reciben el tráfico pre-marcado en la capa acceso y el tráfico de la capa *core*, por lo que sus funciones son agrupar los paquetes utilizando un clasificador BA en base al subcampo DSCP marcado y enviarlos al siguiente nodo de acuerdo al PHB que les corresponde.

El equipo de este nodo utiliza MLS para configurar QoS a través del uso de colas de ingreso y egreso para clasificar los paquetes. A continuación, se procederá a configurar el nodo SW1AGUIOM con los comandos para brindar la QoS deseada como nodo de la capa distribución.

a. Se ingresa al modo de configuración global y se habilita QoS en todo el equipo.

```
sw1aguiom#conf t
sw1aguiom(config)#mls qos
```

b. Se utilizan los siguientes comandos para verificar que la QoS ha sido habilitada en el equipo.

```
sw1aguiom(config)#exit
sw1aguiom#show mls qos
```

c. Por defecto, las interfaces del equipo no confían en ningún campo para brindar QoS, por lo que es necesario configurarlas para que confíen en el subcampo DSCP seteado en los CPEs y asignen ese mismo valor para uso interno.

```
sw1aguiom#conf t
sw1aguiom(config)#interface gigabitethernet1/0/1
sw1aguiom(config-if)#mls qos trust dscp
sw1aguiom(config-if)#exit
sw1aguiom(config)#interface gigabitethernet1/0/2
sw1aguiom(config-if)#mls qos trust dscp
sw1aguiom(config-if)#exit
sw1aguiom(config)#interface gigabitethernet2/0/1
```

```
sw1aguiom(config-if)#mls qos trust dscp
sw1aguiom config-if)#exit
sw1aguiom(config)#interface gigabitethernet2/0/2
sw1aguiom(config-if)#mls qos trust dscp
sw1aguiom(config-if)#exit
```

d. El equipo de este nodo ofrece dos colas con tres profundidades cada una en el ingreso de las interfaces, así como la opción de utilizar a una de las dos colas como prioritaria. La cola prioritaria debe tener asignado un porcentaje de ancho de banda garantizado del enlace, mientras que el resto de ancho de banda se comparte entre las dos colas en base a porcentajes configurados. Además, se debe configurar el porcentaje de *buffer* de ingreso asignado para cada cola.

Cada cola tiene 3 profundidades, donde la profundidad 3 tiene el 100% de uso por defecto para paquetes encolados antes de comenzar a descartarlos, mientras que para las profundidades 1 y 2 es posible configurarlo.

La tabla 4.2 indica la configuración que será realizada sobre este nodo como es la asignación de los valores DSCP a las colas y los porcentajes de *buffer*, ancho de banda y profundidades asignados a cada cola.

<table>
<tr><th>CoS</th><th>Valor DSCP</th><th>Cola</th><th>Umbral</th><th>% Buffer</th><th>% AB</th><th>% Umbral</th><th>PQ</th></tr>
<tr><td>Premium</td><td>EF=46</td><td>1</td><td>3</td><td rowspan="3">40%</td><td rowspan="3">25%</td><td>100%</td><td rowspan="3">PQ con un 30% de ancho de banda del enlace</td></tr>
<tr><td rowspan="2">Oro</td><td>AF11=10</td><td>1</td><td>2</td><td>60%</td></tr>
<tr><td>AF13=14</td><td>1</td><td>1</td><td>50%</td></tr>
<tr><td rowspan="2">Plata</td><td>AF21=18</td><td>2</td><td>3</td><td rowspan="5">60%</td><td rowspan="5">75%</td><td rowspan="2">100%</td><td rowspan="5">--</td></tr>
<tr><td>AF23=22</td><td>2</td><td>3</td></tr>
<tr><td rowspan="2">Bronce</td><td>AF31=26</td><td>2</td><td>2</td><td rowspan="2">40%</td></tr>
<tr><td>AF33=30</td><td>2</td><td>2</td></tr>
<tr><td>Mejor esfuerzo</td><td>BE=0</td><td>2</td><td>1</td><td>30%</td></tr>
</table>

Tabla 4.2 Parámetros de configuración de ingreso de las interfaces del nodo SW1AGUIOM

Los parámetros de configuración de ingreso de las interfaces fueron obtenidos en base a una estimación de velocidades de las aplicaciones y a la definición de los PHBs propuestos en el diseño; la estimación de las velocidades fue proporcionada por el departamento de Proyectos de Telconet S.A. Estos

parámetros están asociados a valores que cumplen con los estándares establecidos por los protocolos de las aplicaciones para su correcto funcionamiento, tomando como referencia el valor especificado por el fabricante para el envío de datos más un valor igual reservado para la recepción de los mismos. Adicionalmente, se añade aproximadamente un 10% al valor de la capacidad para evitar la saturación de los enlaces.

e. Se asignan los valores DSCP correspondientes a cada cola de ingreso.

```
sw1aguiom(config)#mls qos srr-queue input dscp-map queue 1 threshold 1 14
sw1aguiom(config)#mls qos srr-queue input dscp-map queue 1 threshold 2 10
sw1aguiom(config)#mls qos srr-queue input dscp-map queue 1 threshold 3 46
sw1aguiom(config)#mls qos srr-queue input dscp-map queue 2 threshold 1 0
sw1aguiom(config)#mls qos srr-queue input dscp-map queue 2 threshold 2 26 30
sw1aguiom(config)#mls qos srr-queue input dscp-map queue 2 threshold 3 18 22
```

f. Se ingresa el siguiente comando para verificar que los valores DSCP han sido asignados correctamente a la cola correspondiente configurada.

```
sw1aguiom(config)#do show mls qos maps dscp-input-q
```

g. Se configuran los porcentajes de *buffer* de ingreso asignados a cada cola. La suma de los porcentajes de *buffer* no debe ser mayor al 100%.

```
sw1aguiom(config)#mls qos srr-queue input buffers 40 60
```

h. Se asignan los porcentajes de uso de las profundidades 1 y 2 para cada cola, ya que la profundidad 3 tiene el valor de 100% por defecto. El valor máximo para cada profundidad es del 100%. Las colas utilizan estas profundidades para soportar distintos porcentajes de descarte para diferentes tipos de agregados de tráfico mediante WTD.

```
sw1aguiom(config)#mls qos srr-queue input threshold 1 50 60
sw1aguiom(config)#mls qos srr-queue input threshold 2 30 40
```

i. Se configuran los porcentajes de uso del ancho de banda restante para cada cola, que va a ser compartido luego de haber atendido la cola prioritaria. La suma de los porcentajes del ancho de banda no debe ser mayor al 100%. SRR sirve a las colas en base al ancho de banda configurado para enviar los paquetes a un anillo apilado antes de ser transmitidos a las colas de egreso.

```
sw1aguiom(config)#mls qos srr-queue input bandwidth 25 75
```

j. Se indica a las interfaces que la cola 1 será prioritaria con un ancho de banda garantizado del enlace igual al 30%.

```
sw1aguiom(config)#mls qos srr-queue input priority-queue 1 bandwidth 30
```

k. Se ingresa el siguiente comando para verificar que la configuración realizada ha sido asignada correctamente a las dos colas de ingreso de las interfaces.

```
sw1aguiom(config)#do show mls qos input
```

l. Se ingresa los siguientes comandos para guardar la configuración realizada.

```
sw1aguiom(config)#exit
sw1aguiom#copy running-config startup-config
```

m. De igual manera que en el ingreso de una interfaz, el equipo de este nodo ofrece cuatro colas con tres profundidades cada una en el egreso de cada interfaz, así como la opción de utilizar a la cola 1 como prioritaria. La cola prioritaria es atendida hasta ser vaciada antes de servir al resto de colas.
Se debe configurar el porcentaje de *buffer* de egreso asignado para cada cola, los porcentajes de las profundidades 1 y 2 de cada cola, el porcentaje de *buffer* reservado por cola y el porcentaje del umbral máximo por cola. Estos valores pueden ser agrupados en dos opciones, con el fin de ser aplicados a diferentes interfaces.

El uso del ancho de banda del enlace en las colas puede ser utilizado en base a la elección de una de las tres configuraciones posibles como son compartido, limitado ó conformado.

La tabla 4.3 indica la configuración que se va a realizar en el egreso de las interfaces de este nodo con las asignaciones de los valores DSCP y los porcentajes de *buffer*, ancho de banda y profundidades para cada cola, obtenidos en base a la definición de los PHBs en el esquema de QoS diseñado.

CoS	Valor DSCP	Cola	Umbral	% *Buffer*	% Umbral	% AB compartido
Premium	EF=46	1	3	40%	100%	PQ
Oro	AF11=10	2	1	25%	350%	45%
	AF13=14	2	2		280%	
Plata	AF21=18	3	1	20%	260%	35%
	AF23=22	3	2		140%	
Bronce	AF31=26	4	3	15%	100%	20%
	AF33=30	4	2		260%	
Mejor esfuerzo	BE=0	4	1		150%	

Tabla 4.3 Parámetros de configuración de egreso de las interfaces del nodo SW1AGUIOM

Al igual que en el ingreso de las interfaces, los parámetros de configuración de egreso se obtuvieron en base a la estimación de velocidades de las aplicaciones, con los valores especificados por los fabricantes de los protocolos, y a la definición de los PHBs propuestos en el diseño.

n. Se asignan los valores DSCP correspondientes a cada cola de egreso.

```
sw1aguiom#conf t
sw1aguiom(config)#mls qos srr-queue output dscp-map queue 1 threshold 3 46
sw1aguiom(config)#mls qos srr-queue output dscp-map queue 2 threshold 1 10
sw1aguiom(config)#mls qos srr-queue output dscp-map queue 2 threshold 2 14
sw1aguiom(config)#mls qos srr-queue output dscp-map queue 3 threshold 1 18
sw1aguiom(config)#mls qos srr-queue output dscp-map queue 3 threshold 2 22
sw1aguiom(config)#mls qos srr-queue output dscp-map queue 4 threshold 3 26
sw1aguiom(config)#mls qos srr-queue output dscp-map queue 4 threshold 2 30
```

```
sw1aguiom(config)#mls qos srr-queue output dscp-map queue 4 threshold 1 0
```

o. Se ingresa el siguiente comando para verificar que los valores DSCP han sido asignados correctamente a la cola correspondiente configurada.

```
sw1aguiom(config)#exit
sw1aguiom#show mls qos maps dscp-output-q
```

p. Haciendo uso de una sola opción de configuración para todas las interfaces, se define los porcentajes de *buffer* de egreso asignados a cada cola. La suma de los porcentajes de *buffer* no debe ser mayor al 100%.

```
sw1aguiom#conf t
sw1aguiom(config)#mls qos queue-set output 1 buffers 40 25 20 15
```

q. Se asignan los porcentajes de uso de las profundidades 1 y 2 para cada cola, el porcentaje de *buffer* reservado a ser garantizado y la profundidad máxima de cada cola antes de comenzar a descartar paquetes; la profundidad 3 tiene el 100% de uso por defecto. Los porcentajes de la profundidad 1, profundidad 2 y la profundidad máxima tienen un valor máximo de 400% cada uno, mientras que el porcentaje de *buffer* reservado es máximo del 100%. Las colas utilizan dos profundidades para soportar distintos porcentajes de descarte para diferentes tipos de agregados de tráfico mediante WTD.

```
sw1aguiom(config)#mls qos srr-queue output 1 threshold 2 350 280 100 320
sw1aguiom(config)#mls qos srr-queue output 1 threshold 3 260 140 90 250
sw1aguiom(config)#mls qos srr-queue output 1 threshold 4 150 260 80 160
```

r. Se ingresan los siguientes comandos para verificar que la configuración indicada ha sido asignada correctamente a las colas de egreso de las interfaces.

```
sw1aguiom(config)#exit
sw1aguiom#show mls qos queue-set 1
```

s. Se enlaza la opción 1 de configuración a cada interfaz.

```
sw1aguiom#conf t
sw1aguiom(config)#interface gigabitethernet1/0/1
sw1aguiom(config-if)#queue-set 1
sw1aguiom(config-if)#exit
sw1aguiom(config)#interface gigabitethernet1/0/2
sw1aguiom(config-if)#queue-set 1
sw1aguiom(config-if)#exit
sw1aguiom(config)#interface gigabitethernet2/0/1
sw1aguiom(config-if)#queue-set 1
sw1aguiom config-if)#exit
sw1aguiom(config)#interface gigabitethernet2/0/2
sw1aguiom(config-if)#queue-set 1
sw1aguiom(config-if)#exit
```

t. Haciendo uso de la configuración de uso de ancho de banda compartido, se deben especificar los porcentajes que las colas van a usar en cada interfaz. Al especificar la cola 1 como prioritaria, sin importar el ancho de banda configurado, siempre será atendida hasta quedar vacía, por lo que la suma de los porcentajes de ancho de banda del resto de colas no debe ser mayor al 100%. SRR sirve a las colas en base al ancho de banda configurado, enviando los paquetes al puerto de egreso.

```
sw1aguiom(config)#interface gigabitethernet1/0/1
sw1aguiom(config-if)#share 1 45 35 20
sw1aguiom(config-if)#priority-queue out
sw1aguiom(config-if)#exit
sw1aguiom(config)#interface gigabitethernet1/0/2
sw1aguiom(config-if)#share 1 45 35 20
sw1aguiom(config-if)#priority-queue out
sw1aguiom(config-if)#exit
sw1aguiom(config)#interface gigabitethernet2/0/1
sw1aguiom(config-if)#share 1 45 35 20
```

```
sw1aguiom(config-if)#priority-queue out
sw1aguiom config-if)#exit
sw1aguiom(config)#interface gigabitethernet2/0/2
sw1aguiom(config-if)#share 1 45 35 20
sw1aguiom(config-if)#priority-queue out
sw1aguiom(config-if)#exit
```

u. Se utilizan los siguientes comandos para verificar la correcta configuración del ancho de banda compartido en una de las interfaces.

```
sw1aguiom(config)#exit
sw1aguiom#show mls qos interface gigabitethernet1/0/1 queueing
```

v. Se ingresa el siguiente comando para guardar la configuración realizada.

```
sw1aguiom#copy running-config startup-config
```

4.2.4 CONFIGURACIÓN DEL NODO PE1UIOM DE LA CAPA *CORE*[12][13][17]

Los nodos PE de la capa *core* envían y reciben el tráfico de los nodos que forman los anillos de la capa distribución y de los nodos principales de la capa *core*, por lo que sus funciones son agrupar los paquetes utilizando un clasificador BA en base al subcampo DSCP, traducir el subcampo DSCP al campo EXP con el método E-LSP, agrupar los paquetes en base al campo EXP, manejar la QoS sobre MPLS con el modo de tunelización tubería corta y enviar el tráfico al siguiente nodo de acuerdo al PHB que le corresponde.

El equipo de este nodo utiliza MQC para configurar QoS a través del uso de mapas de clases y mapas de políticas. Los parámetros de configuración de los mapas de políticas fueron obtenidos en base a la estimación de velocidades de las aplicaciones que circulan por la red y a la definición de los PHBs propuestos en el diseño.

A continuación, se procederá a configurar el nodo PE1UIOM con los comandos para brindar la QoS deseada como nodo de la capa *core*.

a. Se ingresa al modo de configuración global.

```
pe1uiom#conf t
```

b. Se definen mapas de clases para agrupar los paquetes IP de acuerdo al subcampo DSCP que contienen.

```
pe1uiom(config)#class-map IP-EF
pe1uiom(config-cmap)#match ip dscp ef
pe1uiom(config-cmap)#exit
pe1uiom(config)#class-map IP-AF11
pe1uiom(config-cmap)#match ip dscp af11
pe1uiom(config-cmap)#exit
pe1uiom(config)#class-map IP-AF13
pe1uiom(config-cmap)#match ip dscp af13
pe1uiom(config-cmap)#exit
pe1uiom(config)#class-map IP-AF21
pe1uiom(config-cmap)#match ip dscp af21
pe1uiom(config-cmap)#exit
pe1uiom(config)#class-map IP-AF23
pe1uiom(config-cmap)#match ip dscp af23
pe1uiom(config-cmap)#exit
pe1uiom(config)#class-map IP-AF31
pe1uiom(config-cmap)#match ip dscp af31
pe1uiom(config-cmap)#exit
pe1uiom(config)#class-map IP-AF33
pe1uiom(config-cmap)#match ip dscp af33
pe1uiom(config-cmap)#exit
```

c. Se ingresan los siguientes comandos para verificar que los mapas de clases han sido creados correctamente.

```
pe1uiom(config)#exit
pe1uiom#show class-map
```

d. Se crea un mapa de política para configurar el mapa de correspondencias entre los valores DSCP y los valores EXP con el método E-LSP, definido en el diseño del esquema de QoS. El campo EXP tendrá el mismo valor para todas las etiquetas de la pila.

```
pe1uiom#conf t
pe1uiom(config)#policy-map politica_DSCP-EXP
pe1uiom(config-pmap)#class IP-EF
pe1uiom(config-pmap-c)#set mpls experimental imposition 7
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class IP-AF11
pe1uiom(config-pmap-c)#set mpls experimental imposition 6
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class IP-AF13
pe1uiom(config-pmap-c)#set mpls experimental imposition 5
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class IP-AF21
pe1uiom(config-pmap-c)#set mpls experimental imposition 4
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class IP-AF23
pe1uiom(config-pmap-c)#set mpls experimental imposition 3
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class IP-AF31
pe1uiom(config-pmap-c)#set mpls experimental imposition 2
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class IP-AF33
pe1uiom(config-pmap-c)#set mpls experimental imposition 1
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class class-default
pe1uiom(config-pmap-c)#set mpls experimental imposition 0
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#exit
```

e. Se ingresan los siguientes comandos para verificar que el mapa de política ha sido creado correctamente.

```
pe1uiom(config)#exit
pe1uiom#show policy-map politica_DSCP-EXP
```

f. Se adjunta el mapa de política a las interfaces configuradas con IP para hacerlo efectivo y poder setear el campo EXP en el tráfico entrante durante la imposición de las etiquetas.

```
pe1uiom#conf t
pe1uiom(config)#interface gigabitethernet0/3
pe1uiom(config-if)#service-policy input politica_DSCP-EXP
pe1uiom(config-if)#exit
```

g. Se definen mapas de clases para clasificar los paquetes MPLS en base al campo EXP que contiene la etiqueta MPLS superior y agruparlos de acuerdo a la CoS a la que pertenecen.

```
pe1uiom(config)#class-map MPLS-premium
pe1uiom(config-cmap)#match mpls experimental topmost 7
pe1uiom(config-cmap)#exit
pe1uiom(config)#class-map match-any MPLS-oro
pe1uiom(config-cmap)#match mpls experimental topmost 6 5
pe1uiom(config-cmap)#exit
pe1uiom(config)#class-map match-any MPLS-plata
pe1uiom(config-cmap)#match mpls experimental topmost 4 3
pe1uiom(config-c-map)#exit
pe1uiom(config)#class-map match-any MPLS-bronce
pe1uiom(config-cmap)#match mpls experimental topmost 2 1
pe1uiom(config-cmap)#exit
```

h. Se ingresan los siguientes comandos para verificar que los mapas de clases han sido creados correctamente.

```
pe1uiom(config)#exit
pe1uiom#show class-map
```

i. Se crea un mapa de política para manejar la QoS sobre MPLS con el modo de tunelización tubería corta y brindar los PHBs correspondientes a cada CoS, definidos en el diseño del esquema de QoS.

```
pe1uiom#conf t
pe1uiom(config)#policy-map politica_setMPLS-PHBs
pe1uiom(config-pmap)#class MPLS-premium
pe1uiom(config-pmap-c)#priority percent 29
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class MPLS-oro
pe1uiom(config-pmap-c)#bandwidth percent 21
pe1uiom(config-pmap-c)#random-detect
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class MPLS-plata
pe1uiom(config-pmap-c)#bandwidth percent 15
pe1uiom(config-pmap-c)#random-detect
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class MPLS-bronce
pe1uiom(config-pmap-c)#bandwidth percent 10
pe1uiom(config-pmap-c)#random-detect
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#exit
```

Cuando se configura un procedimiento de control de congestión como LLQ, los equipos Cisco automáticamente reservan un 25% del ancho de banda del enlace en cada interfaz para el tráfico por defecto, dejando el 75% restante para ser repartido entre las clases creadas.

j. Se ingresan los siguientes comandos para verificar que el mapa de política ha sido creado correctamente.

```
pe1uiom(config)#exit
pe1uiom#show policy-map setMPLS-PHBs
```

k. Se adjunta el mapa de política correspondiente a las interfaces configuradas con MPLS para hacerlo efectivo y brindar los PHBs al tráfico de salida de acuerdo a la CoS a la que pertenecen.

```
pe1uiom#conf t
pe1uiom(config)#interface gigabitethernet0/1
pe1uiom(config-if)#service-policy output politica_setMPLS-PHBs
pe1uiom(config-if)#exit
pe1uiom(config)#interface gigabitethernet0/2
pe1uiom(config-if)#service-policy output politica_setMPLS-PHBs
pe1uiom(config-if)#exit
```

l. Se definen mapas de clases para clasificar los paquetes IP en base al subcampo DSCP que contienen y agruparlos de acuerdo a la CoS a la que pertenecen.

```
pe1uiom(config)#class-map IP-premium
pe1uiom(config-cmap)#match ip dscp ef
pe1uiom(config-cmap)#exit
pe1uiom(config)#class-map match-any IP-oro
pe1uiom(config-cmap)#match ip dscp af11 af13
pe1uiom(config-cmap)#exit
pe1uiom(config)#class-map match-any IP-plata
pe1uiom(config-cmap)#match ip dscp af21 af23
pe1uiom(config-cmap)#exit
pe1uiom(config)#class-map match-any IP-bronce
pe1uiom(config-cmap)#match ip dscp af31 af33
pe1uiom(config-cmap)#exit
```

m. Se ingresan los siguientes comandos para verificar que los mapas de clases han sido creados correctamente.

```
pe1uiom(config)#exit
pe1uiom#show class-map
```

n. Se crea un mapa de política para manejar la QoS sobre IP y brindar los PHBs correspondientes a cada CoS, definidos en el diseño del esquema de QoS.

```
pe1uiom(config)#conf t
pe1uiom(config)#policy-map politica_setIP-PHBs
pe1uiom(config-pmap)#class IP-premium
pe1uiom(config-pmap-c)#priority percent 29
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class IP-oro
pe1uiom(config-pmap-c)#bandwidth percent 21
pe1uiom(config-pmap-c)#random-detect dscp-based
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class IP-plata
pe1uiom(config-pmap-c)#bandwidth percent 15
pe1uiom(config-pmap-c)#random-detect dscp-based
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#class IP-bronce
pe1uiom(config-pmap-c)#bandwidth percent 10
pe1uiom(config-pmap-c)#random-detect dscp-based
pe1uiom(config-pmap-c)#exit
pe1uiom(config-pmap)#exit
```

Cuando se configura un procedimiento de control de congestión como LLQ, los equipos Cisco automáticamente reservan un 25% del ancho de banda del enlace en cada interfaz para el tráfico por defecto, dejando el 75% restante para ser repartido entre las clases creadas.

o. Se ingresan los siguientes comandos para verificar que el mapa de política ha sido creado correctamente.

```
pe1uiom(config)#exit
```

```
pe1uiom#show policy-map setIP-PHBs
```

p. Se adjunta el mapa de política correspondiente a las interfaces configuradas con IP para hacerlo efectivo y brindar los PHBs al tráfico de salida de acuerdo a la CoS a la que pertenecen.

```
pe1uiom(config)#conf t
pe1uiom(config)#interface gigabitethernet0/3
pe1uiom(config-if)#service-policy output politica_setIP-PHBs
pe1uiom(config-if)#exit
```

q. Se ingresan los siguientes comandos para guardar la configuración realizada.

```
pe1uiom(config)#exit
pe1uiom#copy running-config startup-config
```

4.2.5 CONFIGURACIÓN DEL NODO CAT6500M DE LA CAPA *CORE*[10][13][14]

Los dos nodos principales de la capa *core* envían y reciben tráfico de los nodos PE y de los nodos de la capa distribución, por lo que sus funciones relacionadas con la QoS son agrupar los paquetes utilizando un clasificador BA en base al campo EXP ó al subcampo DSCP, traducir el subcampo DSCP de IP al campo EXP de MPLS mediante E-LSP, manejar la QoS sobre MPLS con el modo de tunelización tubería corta y enviar el tráfico al siguiente nodo de acuerdo al PHB que le corresponde.

El equipo de este nodo es un *switch* que configura QoS usando el modo MLS y algunos comandos del modo MQC, gracias a los módulos de expansión que contiene. Los parámetros de configuración de los mapas de políticas fueron obtenidos en base a la estimación de velocidades de las aplicaciones que circulan por la red y a la definición de los PHBs propuestos en el diseño.

A continuación, se procederá a configurar el nodo CAT6500M con los comandos para brindar la QoS deseada como uno de los nodos principales de la capa *core*.

a. Se ingresa al modo de configuración global y se habilita QoS en todo el equipo.

```
cat6500m#conf t
cat6500m(config)#mls qos
```

b. Se utilizan los siguientes comandos para verificar que la QoS ha sido habilitada en el equipo.

```
cat6500m(config)#exit
cat6500m#show mls qos
```

c. Se definen mapas de clases para clasificar los paquetes MPLS en base al campo EXP que contiene la etiqueta MPLS superior y agruparlos de acuerdo a la CoS a la que pertenecen.

```
cat6500m#conf t
cat6500m(config)#class-map match-all MPLS-premium
cat6500m(config-cmap)#match mpls experimental 7
cat6500m(config-cmap)#exit
cat6500m(config)#class-map match-any MPLS-oro
cat6500m(config-cmap)#match mpls experimental 6 5
cat6500m(config-cmap)#exit
cat6500m(config)#class-map match-any MPLS-plata
cat6500m(config-cmap)#match mpls experimental 4 3
cat6500m(config-cmap)#exit
cat6500m(config)#class-map match-any MPLS-bronce
cat6500m(config-cmap)#match mpls experimental 2 1
cat6500m(config-cmap)#exit
```

d. Se ingresan los siguientes comandos para verificar que los mapas de clases han sido creados correctamente.

```
cat6500m(config)#exit
cat6500m#show class-map
```

e. Se crea un mapa de política para manejar la QoS sobre MPLS con el modo de tunelización tubería corta y brindar los PHBs correspondientes a cada CoS, definidos en el diseño del esquema de QoS.

```
cat6500m#conf t
cat6500m(config)#policy-map politica_setMPLS-PHBs
cat6500m(config-pmap)#class MPLS-premium
cat6500m(config-pmap-c)#priority percent 30
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class MPLS-oro
cat6500m(config-pmap-c)#bandwidth percent 21
cat6500m(config-pmap-c)#random-detect
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class MPLS-plata
cat6500m(config-pmap-c)#bandwidth percent 14
cat6500m(config-pmap-c)#random-detect
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class MPLS-bronce
cat6500m(config-pmap-c)#bandwidth percent 10
cat6500m(config-pmap-c)#random-detect
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#exit
```

Cuando se implementa un procedimiento de control de congestión como LLQ, los equipos Cisco automáticamente reservan un 25% del ancho de banda del enlace en cada interfaz para el tráfico por defecto, dejando un 75% para ser repartido entre el resto de clases creadas.

f. Se ingresan los siguientes comandos para verificar que el mapa de política ha sido creado correctamente.

```
pe1uiom(config)#exit
pe1uiom#show policy-map setMPLS-PHBs
```

g. Se adjunta el mapa de política respectivo a las interfaces configuradas con MPLS para hacerlo efectivo y brindar los PHBs correspondientes al tráfico de salida de cada CoS. Las interfaces confían por defecto en el valor del campo EXP seteado en el paquete MPLS entrante.

```
cat6500m#conf t
cat6500m(config)#interface ge-wan2/1
cat6500m(config-if)#service-policy output politica_setMPLS-PHBs
cat6500m(config-if)#exit
cat6500m(config)#interface ge-wan2/2
cat6500m(config-if)#service-policy output politica_setMPLS-PHBs
cat6500m(config-if)#exit
cat6500m(config)#interface ge-wan3/2
cat6500m(config-if)#service-policy output politica_setMPLS-PHBs
cat6500m(config-if)#exit
```

h. Debido a la presencia de un enlace configurado con IP en este equipo, se debe establecer el mapa de correspondencias para la integración con la tecnología MPLS. Se definen mapas de clases para agrupar los paquetes IP de acuerdo al subcampo DSCP que contienen.

```
cat6500m(config)#class-map IP-EF
cat6500m(config-c-ap)#match ip dscp ef
cat6500m(config-c-map)#exit
cat6500m(config)#class-map IP-AF11
cat6500m(config-cmap)#match ip dscp af11
cat6500m(config-c-map)#exit
cat6500m(config)#class-map IP-AF13
cat6500m(config-cmap)#match ip dscp af13
cat6500m(config-cmap)#exit
cat6500m(config)#class-map IP-AF21
cat6500m(config-cmap)#match ip dscp af21
cat6500m(config-cmap)#exit
```

```
cat6500m(config)#class-map IP-AF23
cat6500m(config-cmap)#match ip dscp af23
cat6500m(config-cmap)#exit
cat6500m(config)#class-map IP-AF31
cat6500m(config-cmap)#match ip dscp af31
cat6500m(config-cmap)#exit
cat6500m(config)#class-map IP-AF33
cat6500m(config-cmap)#match ip dscp af33
cat6500m(config-c-map)#exit
```

i. Se ingresan los siguientes comandos para verificar que los mapas de clases han sido creados correctamente.

```
cat6500m(config)#exit
cat6500m#show class-map
```

j. Se crea un mapa de política para establecer la correspondencia entre los valores DSCP y los valores EXP con el método E-LSP. El campo EXP tendrá el mismo valor para todas las etiquetas de la pila.

```
cat6500m#conf t
cat6500m(config)#policy-map politica_DSCP-EXP
cat6500m(config-pmap)#class IP-EF
cat6500m(config-pmap-c)#set mpls experimental imposition 7
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class IP-AF11
cat6500m(config-pmap-c)#set mpls experimental imposition 6
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class IP-AF13
cat6500m(config-pmap-c)#set mpls experimental imposition 5
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class IP-AF21
cat6500m(config-pmap-c)#set mpls experimental imposition 4
```

```
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class IP-AF23
cat6500m(config-pmap-c)#set mpls experimental imposition 3
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class IP-AF31
cat6500m(config-pmap-c)#set mpls experimental imposition 2
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class IP-AF33
cat6500m(config-pmap-c)#set mpls experimental imposition 1
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class class-default
cat6500m(config-pmap-c)#set mpls experimental imposition 0
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#exit
```

k. Se ingresan los siguientes comandos para verificar que el mapa de política ha sido creado correctamente.

```
cat6500m(config)#exit
cat6500m#show policy-map politica_DSCP-EXP
```

l. Se adjunta el mapa de política respectivo a las interfaces configuradas con IP para hacerlo efectivo y setear el campo EXP durante la imposición de las etiquetas. Además, se debe indicar a las interfaces que confíen en el subcampo DSCP seteado en los CPEs y asignen ese mismo valor para uso interno.

```
cat6500m#conf t
cat6500m(config)#interface ge-wan3/4
cat6500m(config-if)#mls qos trust dscp
cat6500m(config-if)#service-policy input politica_DSCP-EXP
cat6500m(config-if)#exit
```

m. Se definen mapas de clases para clasificar los paquetes IP en base al subcampo DSCP que contienen y agruparlos de acuerdo a la CoS a la que pertenecen.

```
cat6500m(config)#class-map match-all IP-premium
cat6500m(config-cmap)#match ip dscp ef
cat6500m(config-cmap)#exit
cat6500m(config)#class-map match-any IP-oro
cat6500m(config-cmap)#match ip dscp af11 af13
cat6500m(config-cmap)#exit
cat6500m(config)#class-map match-any IP-plata
cat6500m(config-cmap)#match ip dscp af21 af23
cat6500m(config-cmap)#exit
cat6500m(config)#class-map match-any IP-bronce
cat6500m(config-cmap)#match ip dscp af31 af33
cat6500m(config-cmap)#exit
```

n. Se ingresan los siguientes comandos para verificar que los mapas de clases han sido creados correctamente.

```
cat6500m(config)#exit
cat6500m#show class-map
```

o. Se crea un mapa de política para manejar la QoS sobre IP y brindar los PHBs correspondientes a cada CoS, definidos en el diseño del esquema de QoS.

```
cat6500m#conf t
cat6500m(config)#policy-map politica_setIP-PHBs
cat6500m(config-pmap)#class IP-premium
cat6500m(config-pmap-c)#priority percent 30
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class IP-oro
cat6500m(config-pmap-c)#bandwidth percent 21
cat6500m(config-pmap-c)#random-detect dscp-based
```

```
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class IP-plata
cat6500m(config-pmap-c)#bandwidth percent 14
cat6500m(config-pmap-c)#random-detect dscp-based
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#class IP-bronce
cat6500m(config-pmap-c)#bandwidth percent 10
cat6500m(config-pmap-c)#random-detect dscp-based
cat6500m(config-pmap-c)#exit
cat6500m(config-pmap)#exit
```

p. Se ingresan los siguientes comandos para verificar que el mapa de política ha sido creado correctamente.

```
cat6500m(config)#exit
cat6500m#show policy-map politica_setIP-PHBs
```

q. Se adjunta el mapa de política respectivo a la interfaz configurada con IP para hacerlo efectivo y brindar los PHBs correspondientes al tráfico de salida de cada CoS.

```
cat6500m#conf t
cat6500m(config)#interface ge-wan3/4
cat6500m(config-if)#service-policy output politica_setIP-PHBs
cat6500m(config-if)#exit
```

r. Se ingresan los siguientes comandos para guardar la configuración realizada.

```
cat6500m(config)#exit
cat6500m#copy running-config startup-config
```

4.3 SIMULACIÓN DEL ESQUEMA DISEÑADO DE CALIDAD DE SERVICIO (QoS)

La configuración del esquema de QoS diseñado será simulada en el programa Dynamips, con el fin de obtener los resultados que demuestren el tratamiento diferenciado que los agregados de tráfico deben recibir. Este programa es utilizado por la empresa Telconet S.A. para realizar pruebas de configuración en un entorno que contiene los equipos y las versiones de IOS instalados en su red de *backbone*.

4.3.1 CARACTERÍSTICAS DEL PROGRAMA DYNAMIPS[22]

Dynamips es un programa emulador para *routers* marca Cisco que corre sobre Linux, Mac OS X ó Windows. Este programa emula el hardware de las plataformas de enrutamiento de las series de equipos Cisco, cargando una imagen real del sistema operativo de Cisco IOS en el emulador, lo que permite construir topologías complejas de redes para probar la funcionalidad del IOS en una PC de escritorio, sin la necesidad de usar el dispositivo Cisco real. Actualmente, Dynamips soporta diferentes medios de redes como *Ethernet*, enlaces seriales, ATM y *Packet over Sonet* (POS) interfaces para las plataformas de hardware Cisco 1700, 2600, 3600, 3700 y 7200.

Dynamips está en activo desarrollo y existe un número reducido de complementos escritos especialmente para este programa. Uno de los complementos más populares es Dynagen, un *front-end* que permite el uso de un archivo de configuración INI para provisionar a Dynamips de la emulación de redes y proporcionar una gestión de CLI para listar los dispositivos, suspender y recargar instancias, determinar y gestionar inactividad de los valores de PC, capturar paquetes de rendimiento, etc.

4.3.2 CONFIGURACIÓN DEL ESQUEMA DE QoS EN DYNAMIPS[25]

Telconet S.A. utiliza el programa licenciado Dynamips para emular el hardware implementado en su red con las versiones de IOS instaladas en los equipos, de

modo que los comandos de configuración no sean ingresados directamente en equipamiento real y las pruebas puedan ser realizadas sin inconvenientes.

Haciendo uso del programa Dynamips de Telconet S.A., se ingresarán los comandos de configuración del esquema de QoS diseñado y se presentará su verificación en cualquier nodo de las capas del modelo jerárquico.

4.3.2.1 Configuración de los nodos de la capa distribución en Dynamips

La figura 4.5 indica la habilitación de QoS en un nodo de la capa distribución.

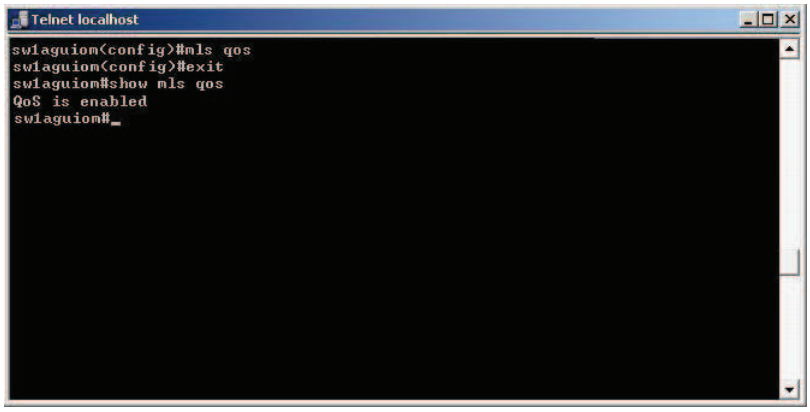

Figura 4.5 Habilitación de QoS en la capa distribución

La figura 4.6 indica la configuración de las interfaces de los nodos de la capa distribución para que confíen en el subcampo DSCP seteado en los CPEs.

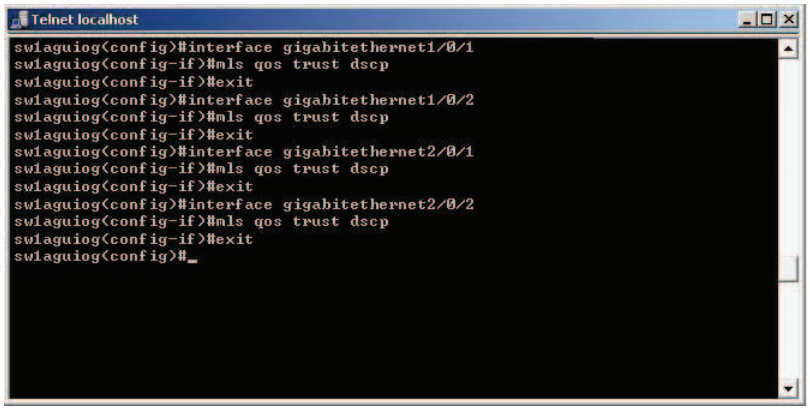

Figura 4.6 Configuración de las interfaces para confiar en el subcampo DSCP

La figura 4.7 muestra la verificación de la correcta asignación de los valores DSCP a las colas de ingreso de las interfaces de los nodos de la capa distribución.

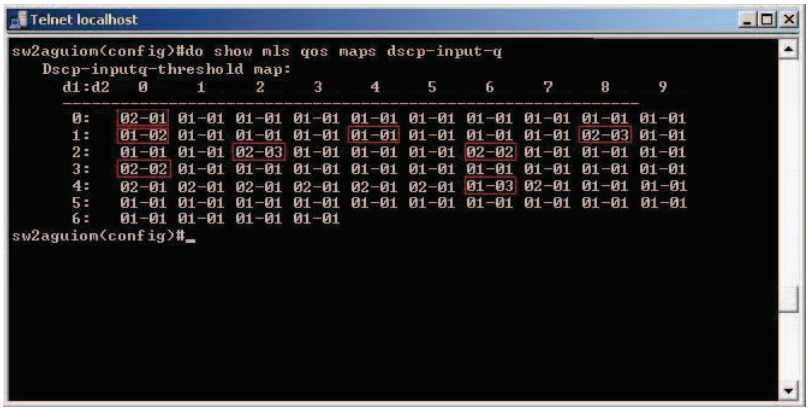

Figura 4.7 Verificación de la asignación de valores DSCP a las colas de ingreso

La figura 4.8 indica la verificación de la configuración de las dos colas de ingreso de las interfaces de los nodos de la capa distribución.

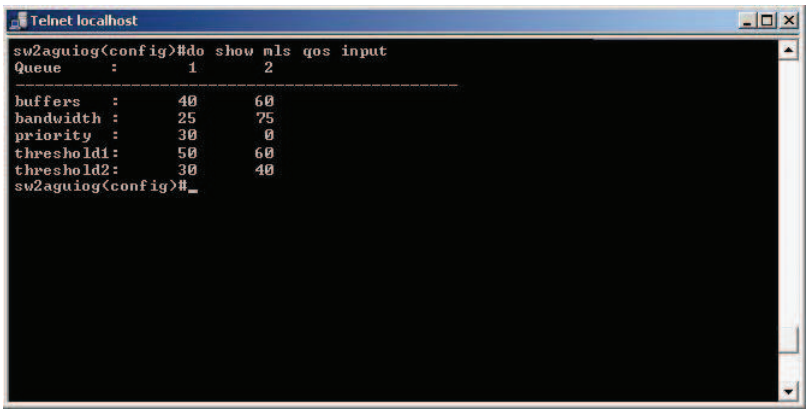

Figura 4.8 Verificación de la configuración de las colas de ingreso

La figura 4.9 muestra la verificación de la correcta asignación de los valores DSCP a las colas de egreso de las interfaces de los nodos de la capa distribución.

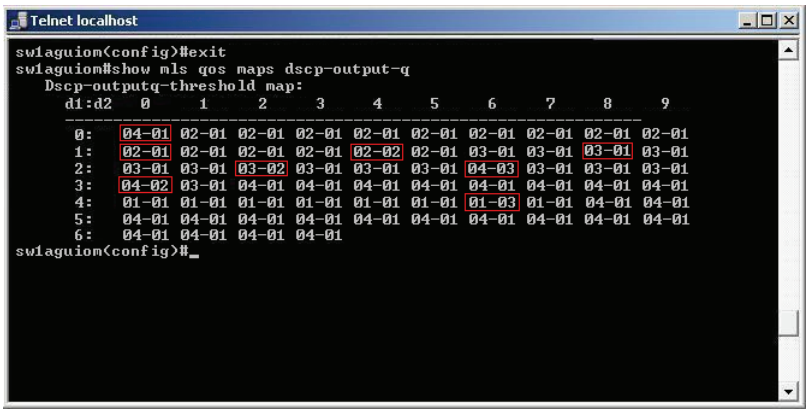

Figura 4.9 Verificación de la asignación de valores DSCP a las colas de egreso

La figura 4.10 indica la verificación de la configuración de las cuatro colas de egreso de las interfaces de los nodos de la capa distribución.

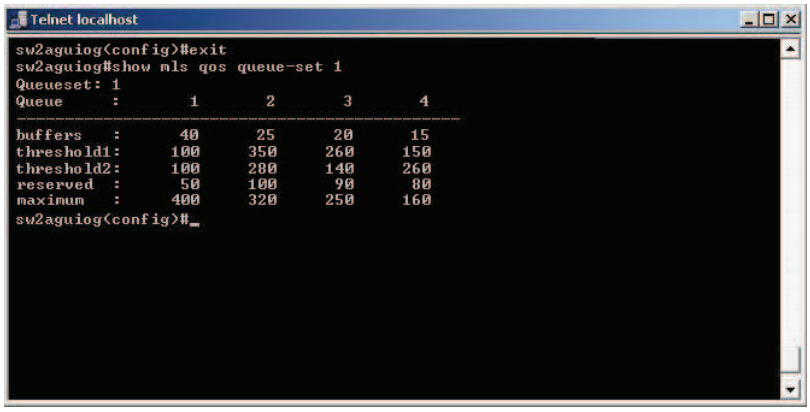

Figura 4.10 Verificación de la configuración de las colas de egreso

La figura 4.11 muestra la verificación de la configuración del ancho de banda compartido en las cuatro colas de egreso de los nodos de la capa distribución.

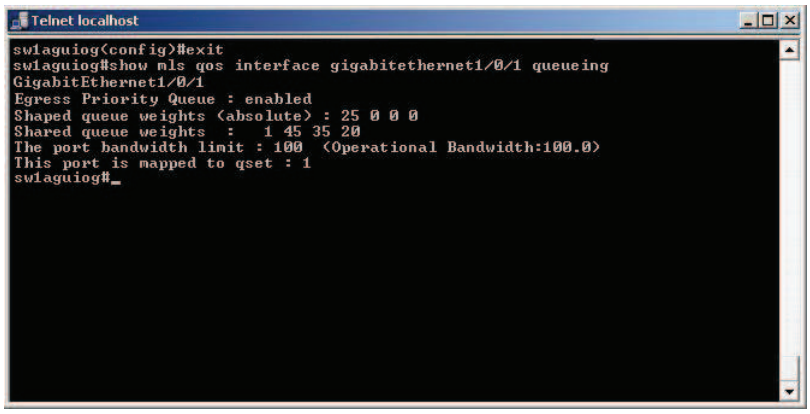

Figura 4.11 Verificación de la configuración del ancho de banda compartido

4.3.2.2 Configuración de los nodos de la capa *core* en Dynamips

4.3.2.2.1 Configuración de los nodos PE en Dynamips

La figura 4.12 muestra los mapas de clases creados para agrupar los paquetes IP de acuerdo al subcampo DSCP, clasificar los paquetes MPLS en base al campo EXP para agruparlos por CoS y seleccionar los paquetes IP de acuerdo al subcampo DSCP para reunirlos por CoS.

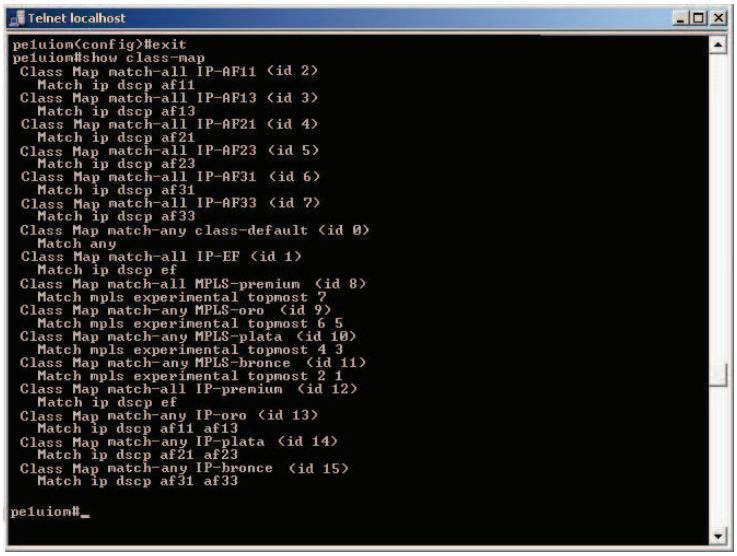

Figura 4.12 Mapas de clases para agrupar paquetes por un mismo criterio

La figura 4.13 indica el mapa de política creado para configurar el mapa de correspondencias entre los valores DSCP y los valores EXP.

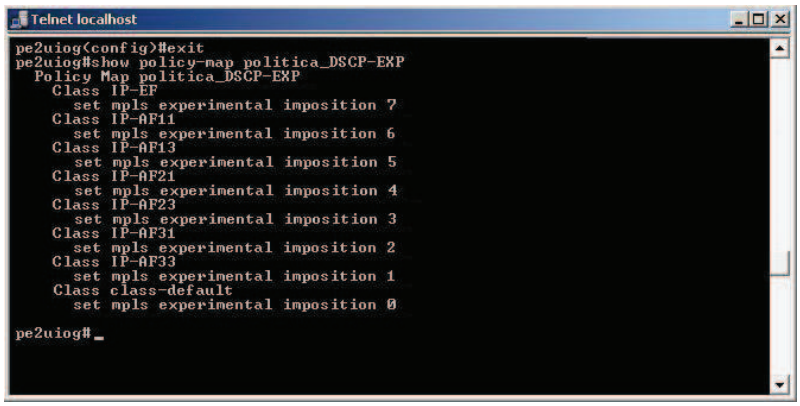

Figura 4.13 Mapa de política para corresponder valores DSCP a valores EXP

La figura 4.14 muestra la configuración del mapa de política en las interfaces con IP para setear el campo EXP durante la imposición de las etiquetas.

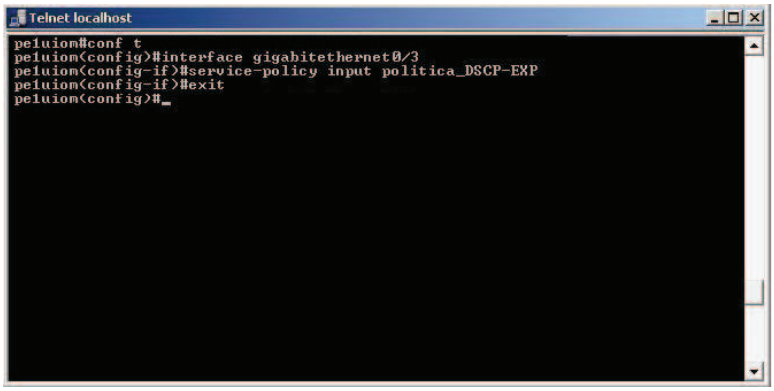

Figura 4.14 Configuración del mapa de política en las interfaces para setear el campo EXP

La figura 4.15 indica el mapa de política creado para manejar la QoS sobre MPLS con el modo de tunelización tubería corta.

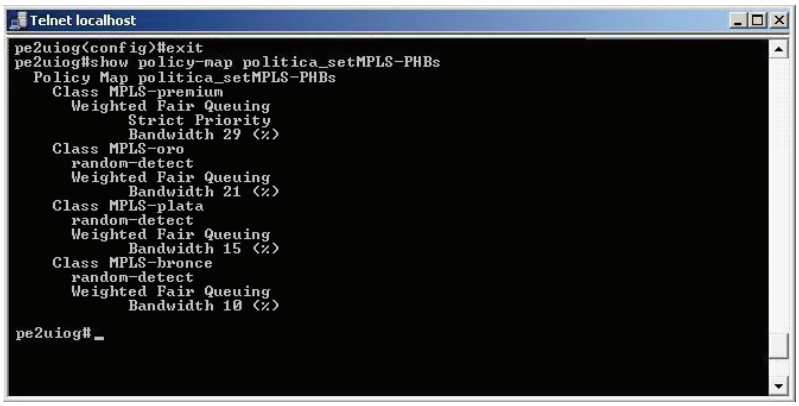

Figura 4.15 Mapa de política para manejar la QoS sobre MPLS

La figura 4.16 muestra la configuración del mapa de política en las interfaces configuradas con MPLS para brindar los PHBs al tráfico de salida por CoS.

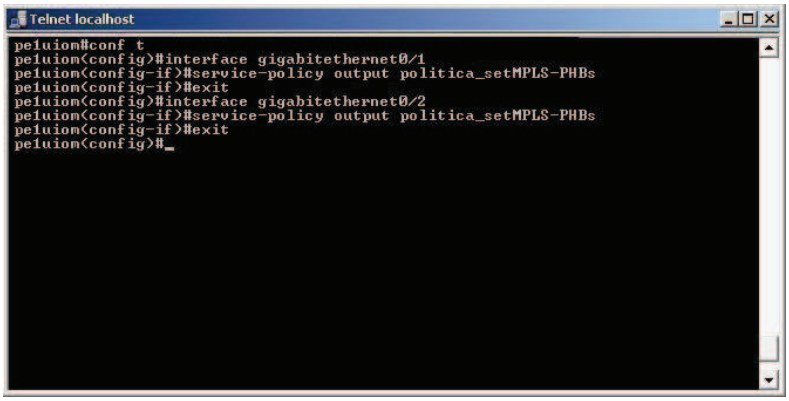

Figura 4.16 Configuración del mapa de política en las interfaces para los PHBs MPLS

La figura 4.17 indica el mapa de política creado para manejar la QoS sobre IP y brindar los PHBs correspondientes a cada CoS.

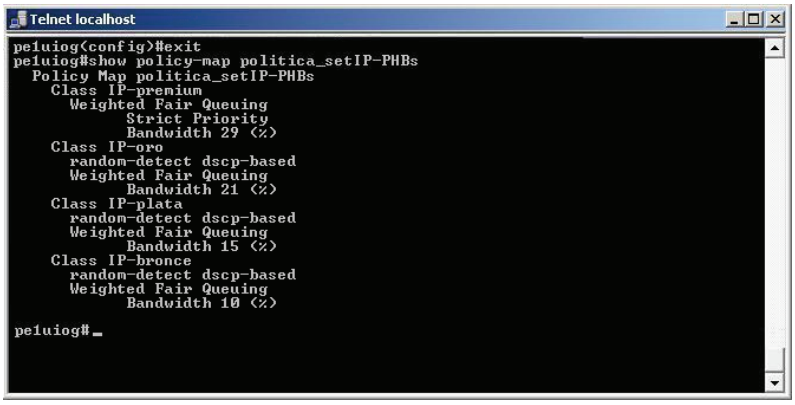

Figura 4.17 Mapa de política para manejar la QoS sobre IP

La figura 4.18 muestra la configuración del mapa de política en las interfaces con IP para brindar los PHBs al tráfico de salida de acuerdo a su CoS.

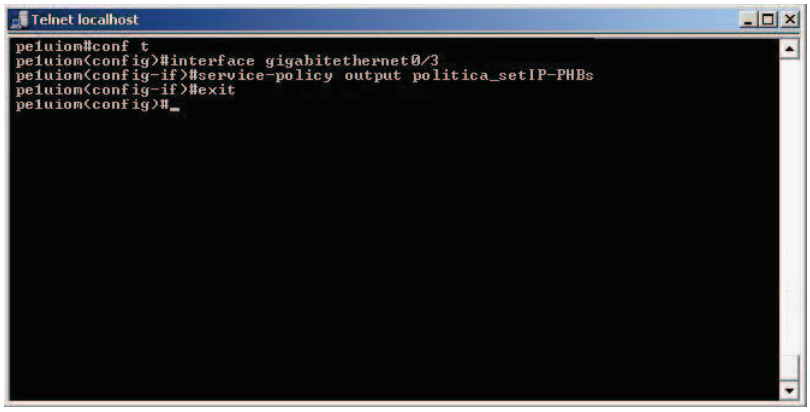

Figura 4.18 Configuración del mapa de política en las interfaces para los PHBs IP

4.3.2.2.2 Configuración de los nodos principales en Dynamips

La figura 4.19 muestra la habilitación de QoS en uno de los nodos principales.

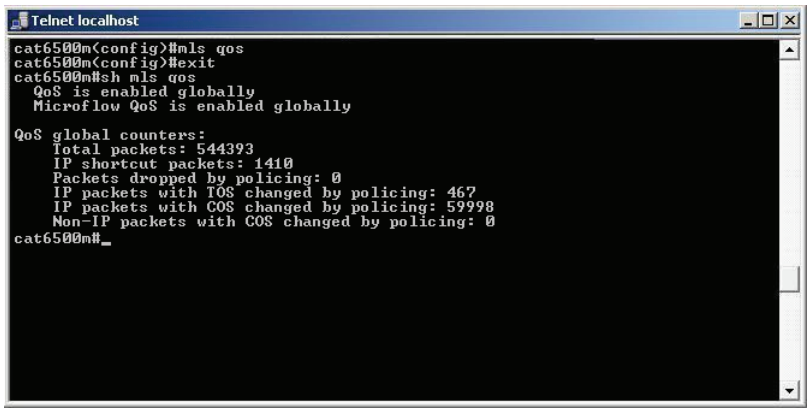

Figura 4.19 Habilitación de QoS en un nodo principal de la capa *core*

La figura 4.20 indica los mapas de clases creados para clasificar los paquetes MPLS en base al campo EXP para agruparlos por CoS, agrupar los paquetes IP de acuerdo al subcampo DSCP que contienen y seleccionar los paquetes IP en base al subcampo DSCP para reunirlos por CoS.

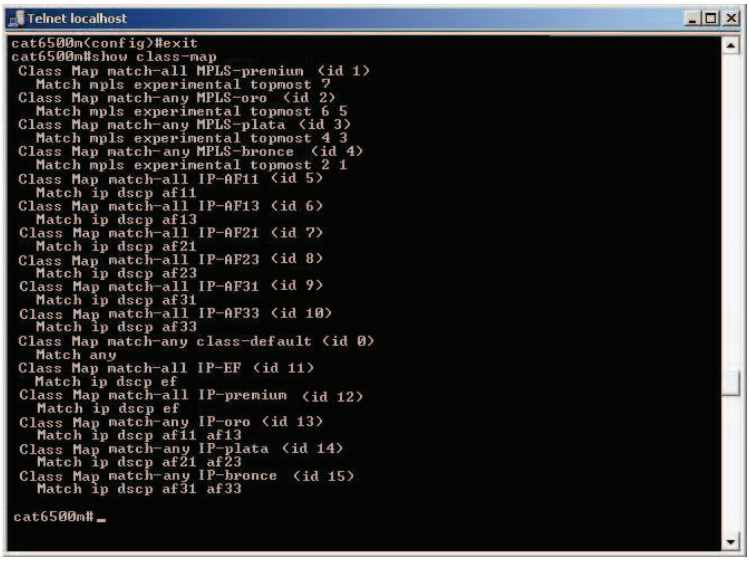

Figura 4.20 Mapas de clases creados para clasificar paquetes por un mismo criterio

La figura 4.21 muestra el mapa de política configurado para manejar la QoS sobre MPLS y brindar los PHBs correspondientes a cada CoS.

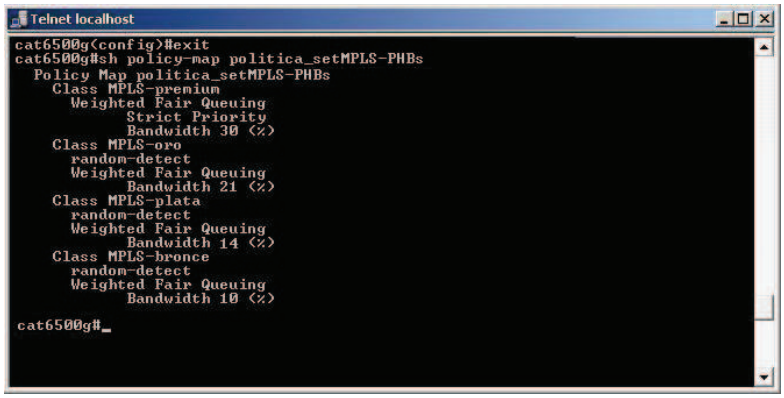

Figura 4.21 Mapa de política para configurar los PHBs MPLS

La figura 4.22 muestra la configuración del mapa de política en las interfaces configuradas con MPLS para brindar los PHBs al tráfico de salida por CoS.

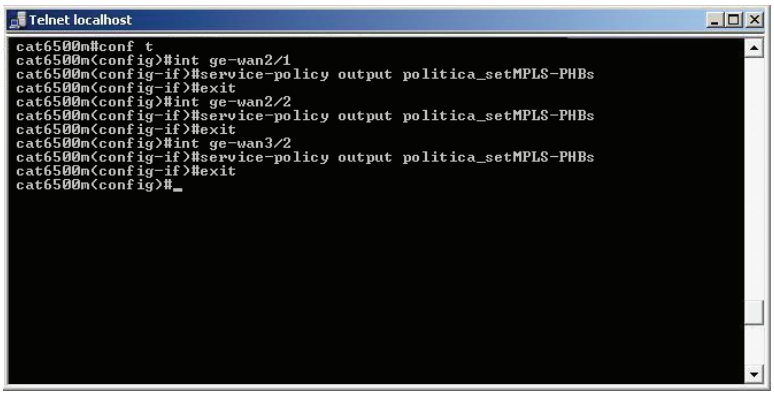

Figura 4.22 Configuración del mapa de política en las interfaces con MPLS

La figura 4.23 indica el mapa de política creado para corresponder los valores DSCP a valores EXP con el método E-LSP.

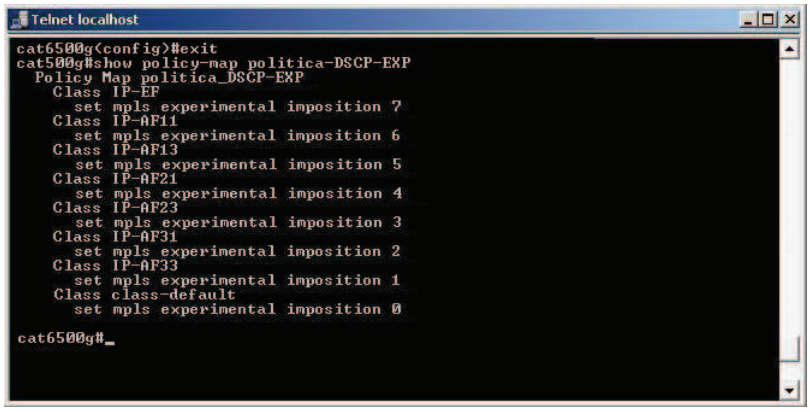

Figura 4.23 Mapa de política para corresponder subcampo DSCP a campo EXP

La figura 4.24 muestra la configuración del mapa de política en las interfaces con IP para setear el campo EXP durante la imposición de las etiquetas.

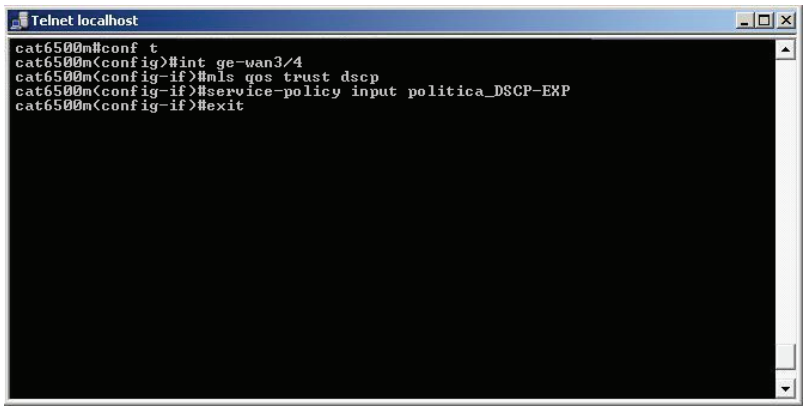

Figura 4.24 Configuración del mapa de política para confiar en valores DSCP y setear campo EXP

La figura 4.25 muestra el mapa de política creado para manejar la QoS sobre IP y brindar los PHBs correspondientes a cada CoS.

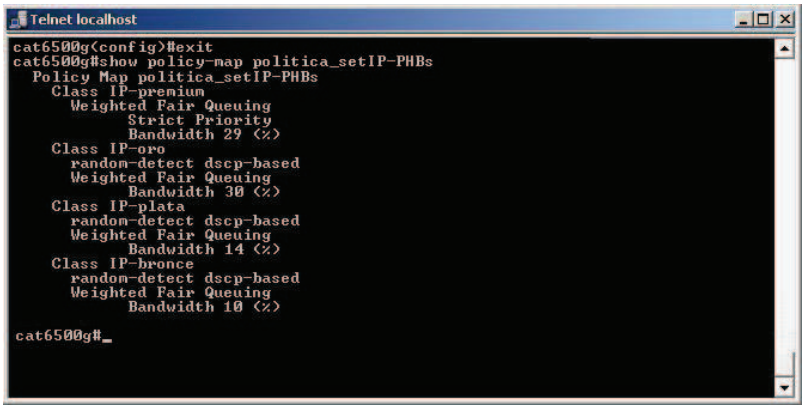

Figura 4.25 Mapa de política para brindar los PHBs sobre IP

La figura 4.26 muestra la configuración del mapa de política en las interfaces con IP para brindar los PHBs al tráfico de salida de acuerdo a su CoS.

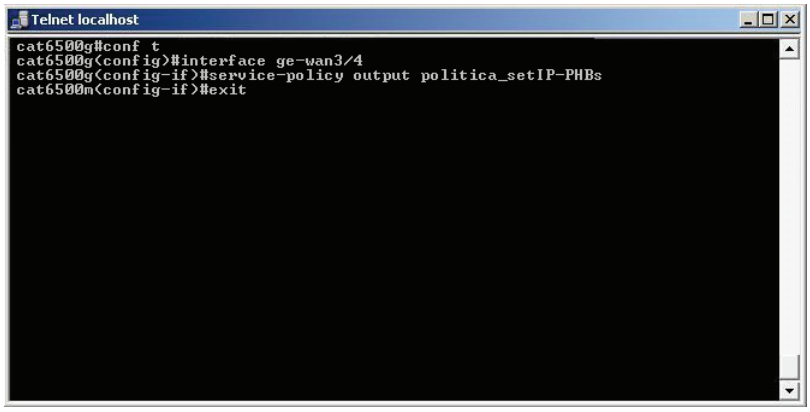

Figura 4.26 Configuración del mapa de política PHBs IP en las interfaces

4.3.3 RESULTADOS OBTENIDOS EN DYNAMIPS[24]

Una vez introducidos los comandos de configuración en el programa Dynamips, se debe verificar que los agregados de tráfico reciban el tratamiento que les corresponde en cada nodo.

El departamento de Proyectos de la empresa Telconet S.A. utiliza el lenguaje de programación Perl para crear *scripts* que proporcionen un generador simple de flujos de tráfico, con el fin de realizar pruebas en laboratorios sobre los modelos de los equipos de su red en el programa Dynamips. Estos *scripts* Perl están programados para generar los diferentes agregados de tráfico que circulan por la red de la empresa, de manera que se puede obtener estadísticas de las políticas configuradas para brindar QoS.

Los equipos marca Cisco tienen la habilidad de mostrar las estadísticas y las configuraciones de las políticas de entrada y salida adjuntadas a una interfaz. Esta habilidad es posible mediante la utilización del comando *show policy-map interface [interface-type interface-number]*.

Utilizando los scripts Perl se generó cantidades confiables y predecibles de diferentes tipos de tráfico en el programa Dynamips para obtener estadísticas de las políticas configuradas en los equipos de la capa *core*, debido a que estos concentran la mayor parte de tráfico y realizan la integración entre las tecnologías

IP y MPLS. La figura 4.27 indica las estadísticas de una de las interfaces de los equipos de la capa *core* de la red de Telconet S.A. en el programa Dynamips.

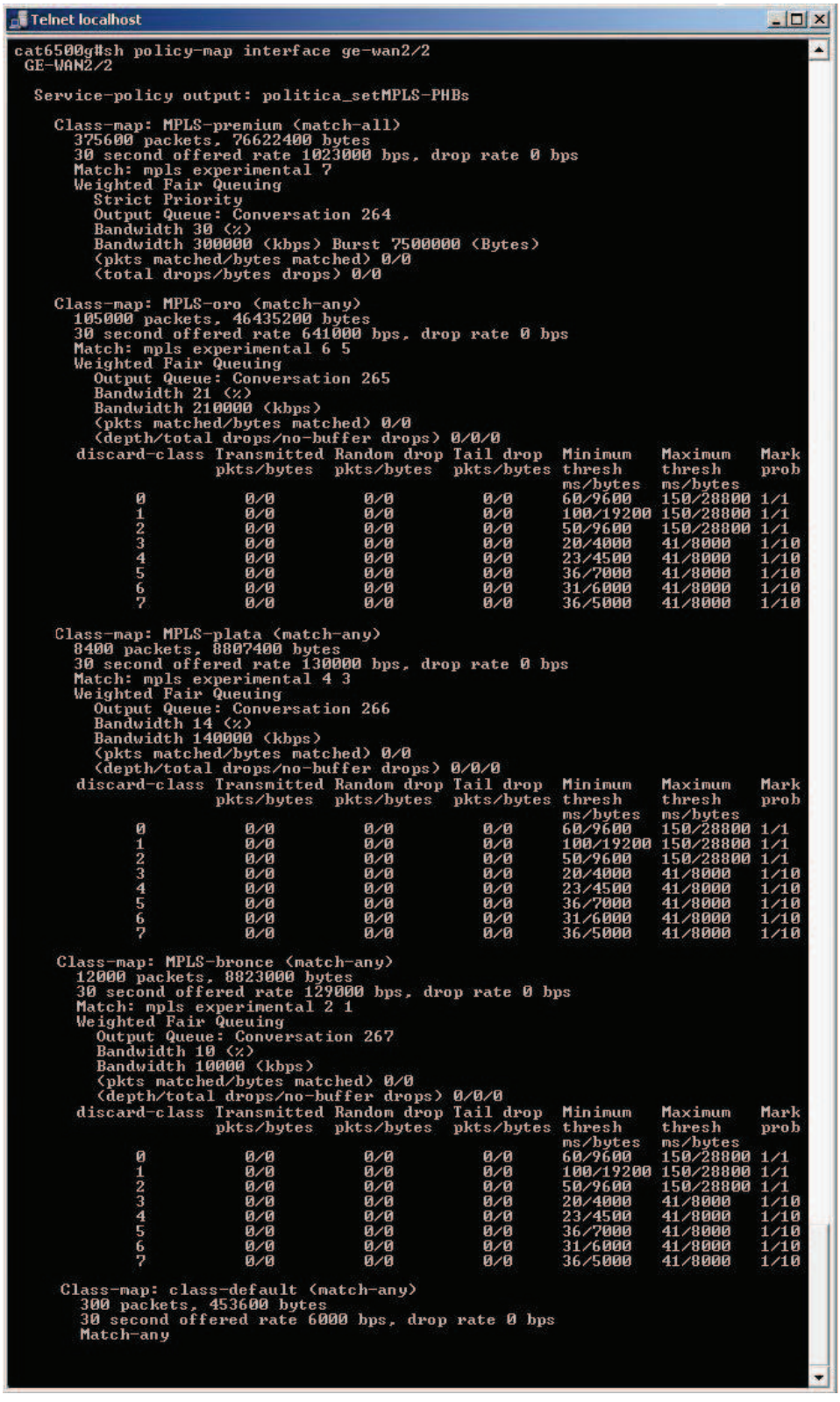

Figura 4.27 Estadísticas de tráfico de una política en un nodo de la capa *core*

A partir de las estadísticas mostradas anteriormente para la política que permite brindar el tratamiento correspondiente a cada paquete MPLS, se puede indicar lo siguiente:

- Las estadísticas de las políticas son actualizadas cada 30 segundos; este valor puede ser modificado utilizando el comando *load interval [seconds]*, donde el valor ingresado deber ser un múltiplo de 30, desde 30 hasta 600 segundos.
- Cada clase muestra: el criterio de selección de los paquetes, la clase prioritaria, el porcentaje de ancho de banda asignado y la cantidad de ancho de banda asignada del enlace en Kbps.
- El número de paquetes y bytes indicados corresponden al número y tamaño de los paquetes que coincidieron con el criterio de selección de la clase configurada. Este contador se incrementa independientemente de si la interfaz está o no congestionada.
- El número de paquetes y bytes coincidentes indicados corresponde al número y tamaño de los paquetes que coincidieron con el criterio de selección de la clase configurada cuando la interfaz estaba congestionada.
- Todas las clases utilizan el mecanismo WRED para evitar la congestión mediante el descarte aleatorio basado en los valores del campo EXP de los paquetes MPLS, a excepción de la clase Premium que utiliza el mecanismo *tail drop* por defecto.

Utilizando el comando indicado anteriormente, se obtuvo estadísticas de las políticas configuradas en las interfaces de los nodos de la capa *core*, donde los parámetros del número de paquetes y bytes son considerados para demostrar que los paquetes están siendo clasificados y recibiendo el tratamiento que les corresponde.

La tabla 4.4 indica las estadísticas de la política para configurar el mapa de correspondencias entre los valores DSCP y los valores EXP del nodo PE1UIOG.

Interfaz	Clase	Número de paquetes	Número de bytes
G0/3	IP-EF	192000	384000000
	IP-AF11	33600	10348800
	IP-AF13	7200	9676800
	IP-AF21	12000	12612000
	IP-AF23	4800	4982400
	IP-EF31	18600	9858000
	IP-EF33	2280	3043800

Tabla 4.4 Estadísticas de la política para el mapa de correspondencias del nodo PE1UIOG

La tabla 4.5 muestra las estadísticas de la política para manejar la QoS sobre MPLS en el nodo PE1UIOG.

Interfaz	Clase	Número de paquetes	Número de bytes
G0/1	MPLS-premium	14000	2856000
	MPLS-oro	11200	3494400
	MPLS-plata	9600	6092400
	MPLS-bronce	6600	6963000
G0/2	MPLS-premium	188400	38433600
	MPLS-oro	37200	18444400
	MPLS-plata	8400	8807400
	MPLS-bronce	12000	8823000

Tabla 4.5 Estadísticas de la política para la QoS sobre MPLS en el nodo PE1UIOG

Las estadísticas de la política para manejar la QoS sobre MPLS en la interfaces G0/1 y G0/2 del nodo PE1UIOG se muestran de forma gráfica en la figura 4.28.

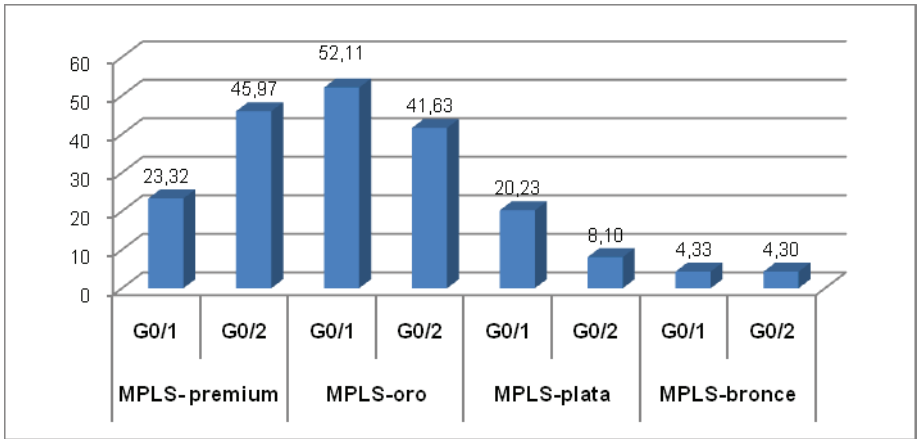

Figura 4.28 Tráfico en las interfaces G0/1 y G0/2 del nodo PE1UIOG para la QoS sobre MPLS

La tabla 4.6 muestra las estadísticas de la política para manejar la QoS sobre IP en el nodo PE1UIOG.

Interfaz	Clase	Número de paquetes	Número de bytes
G0/3	IP-premium	33600	6854400
	IP-oro	12000	3744000
	IP-plata	9000	9378000
	IP-bronce	1800	2410200

Tabla 4.6 Estadísticas de la política para la QoS sobre IP en el nodo PE1UIOG

Las estadísticas de la política para manejar la QoS sobre IP en la interfaz G0/3 del nodo PE1UIOG se muestran de forma gráfica en la figura 4.29.

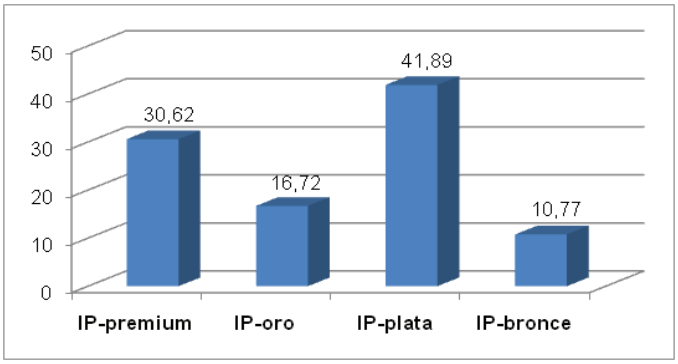

Figura 4.29 Porcentajes de tráfico en la interfaz G0/3 del nodo PE1UIOG para la QoS sobre IP

La tabla 4.7 indica las estadísticas de la política para configurar el mapa de correspondencias entre los valores DSCP y los valores EXP del nodo PE2UIOG.

Interfaz	Clase	Número de paquetes	Número de bytes
G0/3	IP-EF	96000	19584000
	IP-AF11	62400	19219200
	IP-AF13	42100	56582400
	IP-AF21	23400	24593400
	IP-AF23	4200	4359600
	IP-EF31	9000	4806000
	IP-EF33	1800	2403000

Tabla 4.7 Estadísticas de la política para el mapa de correspondencias del nodo PE2UIOG

La tabla 4.8 muestra las estadísticas de la política para manejar la QoS sobre MPLS en el nodo PE2UIOG.

Interfaz	Clase	Número de paquetes	Número de bytes
G0/1	MPLS-premium	187200	38188800
	MPLS-oro	122400	38187000
	MPLS-plata	27000	27797400
	MPLS-bronce	9600	6092400
G0/2	MPLS-premium	188400	38433600
	MPLS-oro	67800	27991200
	MPLS-plata	43780	46187900
	MPLS-bronce	7830	10484370

Tabla 4.8 Estadísticas de la política para la QoS sobre MPLS en el nodo PE2UIOG

Las estadísticas de la política para manejar la QoS sobre MPLS en la interfaces G0/1 y G0/2 del nodo PE2UIOG se muestran de forma gráfica en la figura 4.30.

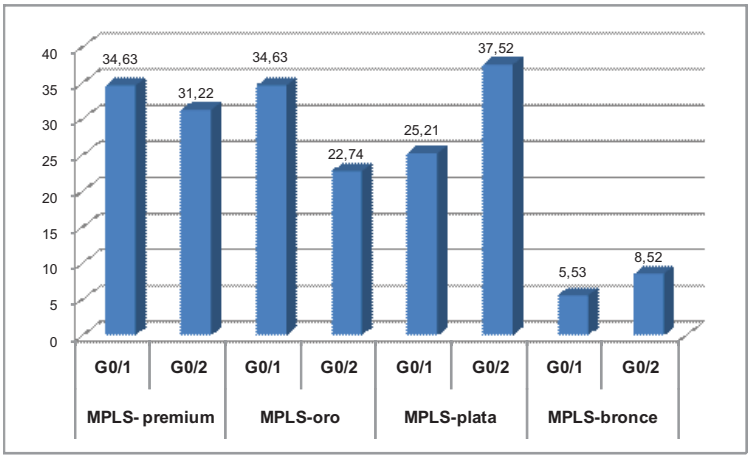

Figura 4.30 Tráfico en las interfaces G0/1 y G0/2 del nodo PE2UIOG para la QoS sobre MPLS

La tabla 4.9 muestra las estadísticas de la política para manejar la QoS sobre IP en el nodo PE2UIOG.

Interfaz	Clase	Número de paquetes	Número de bytes
G0/3	IP-premium	98000	19584000
	IP-oro	81000	25272000
	IP-plata	6600	6877200
	IP-bronce	4200	5623800

Tabla 4.9 Estadísticas de la política para la QoS sobre IP en el nodo PE2UIOG

Las estadísticas de la política para manejar la QoS sobre IP en la interfaz G0/3 del nodo PE2UIOG se muestran de forma gráfica en la figura 4.31.

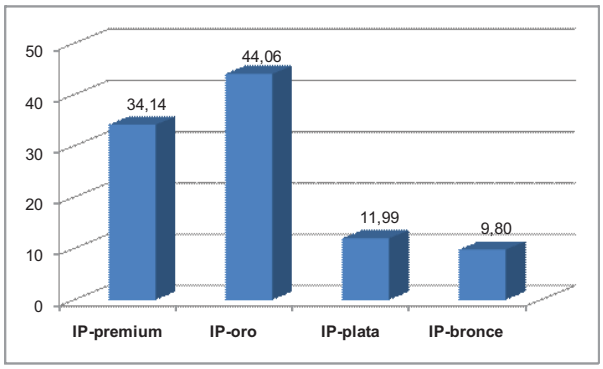

Figura 4.31 Porcentajes de tráfico en la interfaz G0/3 del nodo PE2UIOG para la QoS sobre IP

La tabla 4.10 indica las estadísticas de la política para configurar el mapa de correspondencias entre los valores DSCP y los valores EXP del nodo PE1UIOM.

Interfaz	Clase	Número de paquetes	Número de bytes
G0/3	IP-EF	20350	4070000
	IP-AF11	15600	4804800
	IP-AF13	10200	1062840
	IP-AF21	13100	2620000
	IP-AF23	9670	1007614
	IP-EF31	7800	4165200
	IP-EF33	4780	6214000

Tabla 4.10 Estadísticas de la política para el mapa de correspondencias del nodo PE1UIOM

La tabla 4.11 muestra las estadísticas de la política para manejar la QoS sobre MPLS en el nodo PE1UIOM.

Interfaz	Clase	Número de paquetes	Número de bytes
G0/1	MPLS-premium	258300	52693200
	MPLS-oro	213790	66702480
	MPLS-plata	107800	14531440
	MPLS-bronce	5780	7739420
G0/2	MPLS-premium	188400	38433600
	MPLS-oro	126000	39312000
	MPLS-plata	80690	67078980
	MPLS-bronce	43729	58553131

Tabla 4.11 Estadísticas de la política para la QoS sobre MPLS en el nodo PE1UIOM

Las estadísticas de la política para manejar la QoS sobre MPLS en la interfaces G0/1 y G0/2 del nodo PE1UIOM se muestran de forma gráfica en la figura 4.32.

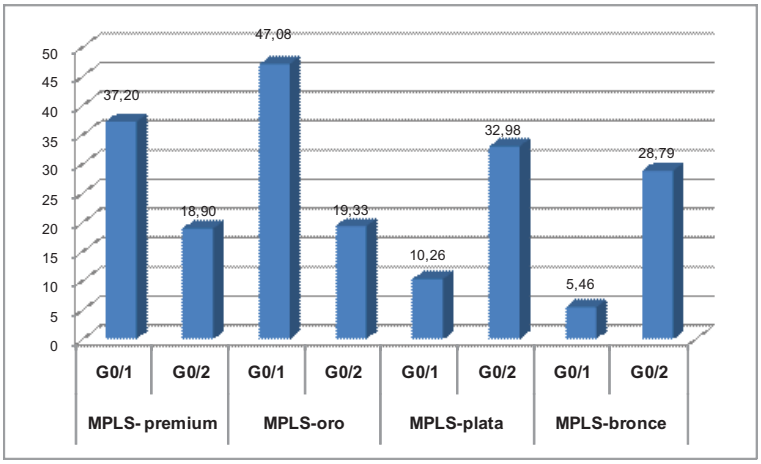

Figura 4.32 Tráfico en las interfaces G0/1 y G0/2 del nodo PE1UIOM para la QoS sobre MPLS

La tabla 4.12 muestra las estadísticas de la política para manejar la QoS sobre IP en el nodo PE1UIOM.

Interfaz	Clase	Número de paquetes	Número de bytes
G0/3	IP-premium	33000	6732000
	IP-oro	12000	3744000
	IP-plata	8400	8752800
	IP-bronce	3000	4017000

Tabla 4.12 Estadísticas de la política para la QoS sobre IP en el nodo PE1UIOM

Las estadísticas de la política para manejar la QoS sobre IP en la interfaz G0/3 del nodo PE1UIOM se muestran de forma gráfica en la figura 4.33.

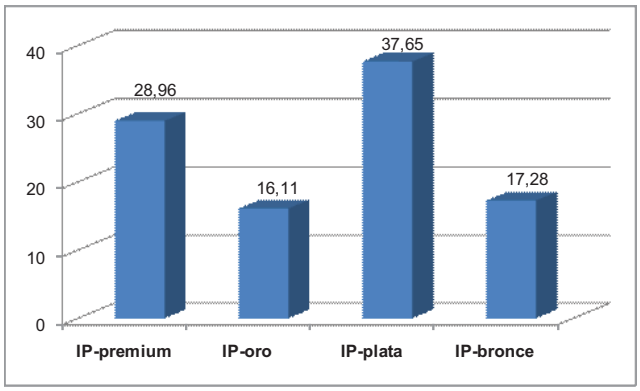

Figura 4.33 Porcentajes de tráfico en la interfaz G0/3 del nodo PE1UIOM para la QoS sobre IP

La tabla 4.13 indica las estadísticas de la política para configurar el mapa de correspondencias entre los valores DSCP y los valores EXP del nodo PE2UIOM.

Interfaz	Clase	Número de paquetes	Número de bytes
G0/3	IP-EF	188400	38433600
	IP-AF11	61200	19094400
	IP-AF13	56000	75488000
	IP-AF21	45009	47484495
	IP-AF23	14670	15286140
	IP-EF31	9000	4806000
	IP-EF33	1300	1740700

Tabla 4.13 Estadísticas de la política para el mapa de correspondencias del nodo PE2UIOM

La tabla 4.14 muestra las estadísticas de la política para manejar la QoS sobre MPLS en el nodo PE2UIOM.

Interfaz	Clase	Número de paquetes	Número de bytes
G0/1	MPLS-premium	200400	40881600
	MPLS-oro	67800	91339440
	MPLS-plata	35408	35456700
	MPLS-bronce	5672	7594808
G0/2	MPLS-premium	45600	9303400
	MPLS-oro	27000	8424000
	MPLS-plata	15730	1639066
	MPLS-bronce	6500	870350

Tabla 4.14 Estadísticas de la política para la QoS sobre MPLS en el nodo PE2UIOM

Las estadísticas de la política para manejar la QoS sobre MPLS en la interfaces G0/1 y G0/2 del nodo PE2UIOM se muestran de forma gráfica en la figura 4.34.

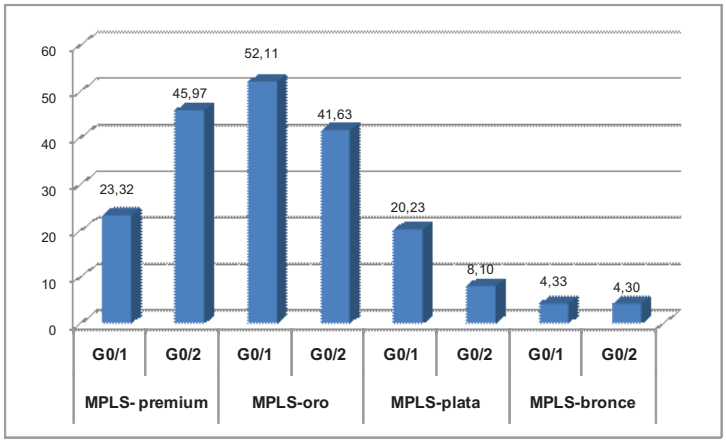

Figura 4.34 Tráfico en las interfaces G0/1 y G0/2 del nodo PE2UIOM para la QoS sobre MPLS

Las estadísticas de la política para manejar la QoS sobre IP en la interfaz G0/3 del nodo PE2UIOM se muestran de forma gráfica en la figura 4.35.

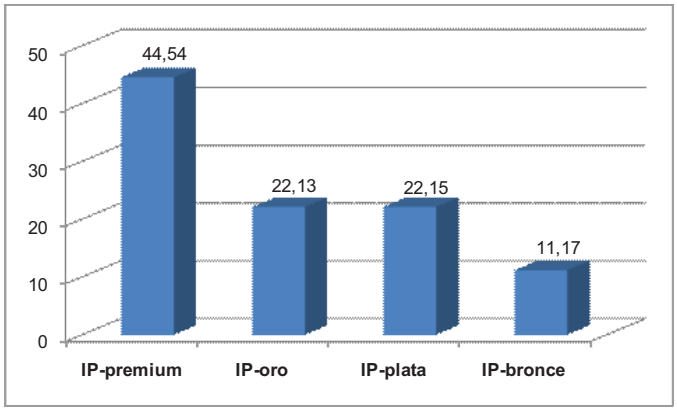

Figura 4.35 Porcentajes de tráfico en la interfaz G0/3 del nodo PE2UIOM para la QoS sobre IP

La tabla 4.15 muestra las estadísticas de la política para manejar la QoS sobre MPLS en el nodo CAT6500G.

Interfaz	Clase	Número de paquetes	Número de bytes
GE-WAN2/1	MPLS-premium	5278	1076712
	MPLS-oro	2130	664560
	MPLS-plata	240	253200
	MPLS-bronce	120	160680
GE-WAN2/2	MPLS-premium	375600	76622400
	MPLS-oro	105000	46435200
	MPLS-plata	8400	8807400
	MPLS-bronce	12000	8823000
GE-WAN2/3	MPLS-premium	110000	22440000
	MPLS-oro	106540	33240480
	MPLS-plata	30950	32652250
	MPLS-bronce	15300	20486700
GE-WAN3/2	MPLS-premium	10450	2131800
	MPLS-oro	9860	3076320
	MPLS-plata	8569	2308731
	MPLS-bronce	5670	2289072
GE-WAN3/3	MPLS-premium	97640	19918560
	MPLS-oro	32600	10171200
	MPLS-plata	12853	13392826
	MPLS-bronce	5630	2456825

Tabla 4.15 Estadísticas de la política para la QoS sobre MPLS en el nodo CAT6500G

Las estadísticas de la política para manejar la QoS sobre MPLS en la interfaces del nodo CAT6500G se muestran de forma gráfica en la figura 4.36.

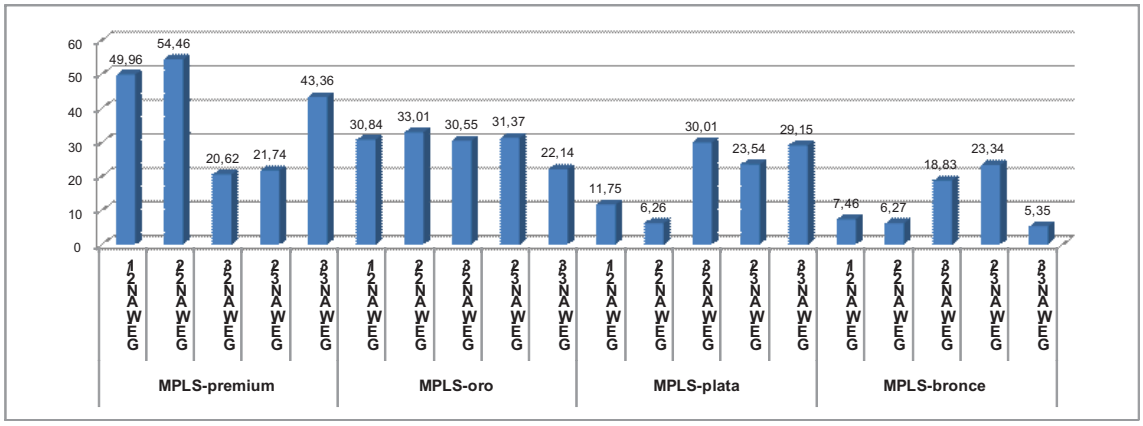

Figura 4.36 Porcentajes de tráfico en las interfaces del nodo CAT6500G para la QoS sobre MPLS

La tabla 4.16 muestra las estadísticas de la política para manejar la QoS sobre MPLS en el nodo CAT6500M.

Interfaz	Clase	Número de paquetes	Número de bytes
GE-WAN2/1	MPLS-premium	8763	1787652
	MPLS-oro	5430	1694160
	MPLS-plata	3270	3407340
	MPLS-bronce	1034	1384526
GE-WAN2/2	MPLS-premium	22421	4573884
	MPLS-oro	17560	5478720
	MPLS-plata	12372	12891624
	MPLS-bronce	6530	8743670
GE-WAN2/3	MPLS-premium	204590	41736360
	MPLS-oro	118300	36909600
	MPLS-plata	68540	53418680
	MPLS-bronce	11873	6340182
GE-WAN3/2	MPLS-premium	98560	20106240
	MPLS-oro	34670	10817040
	MPLS-plata	13457	14022194
	MPLS-bronce	8651	4619634
GE-WAN3/3	MPLS-premium	89563	18270852
	MPLS-oro	23600	7363200
	MPLS-plata	13455	1402011
	MPLS-bronce	4328	2311152

Tabla 4.16 Estadísticas de la política para la QoS sobre MPLS en el nodo CAT6500M

Las estadísticas de la política para manejar la QoS sobre MPLS en la interfaces del nodo CAT6500M se muestran de forma gráfica en la figura 4.37.

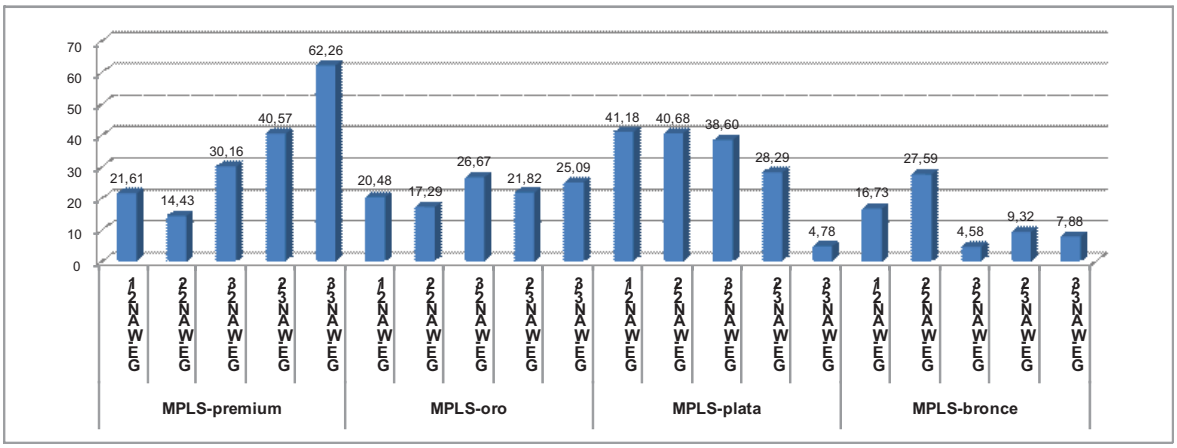

Figura 4.37 Porcentajes de tráfico en las interfaces del nodo CAT6500M para la QoS sobre MPLS

De acuerdo a los resultados mostrados en las tablas, las clases configuradas en las interfaces de los equipos están clasificando los paquetes y brindándoles el tratamiento que deben recibir en cada nodo. Además, las estadísticas obtenidas de los mecanismos de evasión de congestión indicaron que no existe congestión en las interfaces, ya que no hubo presencia de paquetes encolados o descartados durante el tiempo de simulación. Sin embargo, se debe tomar en cuenta que el programa Dynamips no entrega la cantidad real de tráfico que está circulando por la red, evitando detectar los posibles puntos de congestión que puedan presentarse.

REFERENCIAS CAPÍTULO 4

LIBROS Y MANUALES

[1] CISCO SYSTEMS. Datasheet Cisco Catalyst 6500 and 6500-E series switch

[2] CISCO SYSTEMS. Datasheet Cisco 7200VXR series router

[3] CISCO SYSTEMS. Datasheet Cisco Catalyst 3750 series switches

[4] CISCO SYSTEMS. Curriculum CCNA exploration 4.0: Networks fundamentals

ARTÍCULOS E INTERNET

[5] ANÓNIMO. “WS-C6509-E-Cisco Catalyst 6509-E-switch” http://www.hardware.com/store/Cisco/WS-C6509-E

[6] EXPRESS COMPUTER SYSTEMS. “CISCO7206VXR” http://www.7206vxr.com

[7] T3 SYSTEMS. “Cisco WS-C3750G-12S-S-12-Port SFP switch” http://www.t3systemsinc.com/catalog/product_info.php/products_id/95

[8] CISCO SYSTEMS. “Cisco 7600 Series Enhanced 4-port GE OSM” http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SR_OSM_config/pwan.html

[9] CISCO SYSTEMS. “Configuring the 4-Port Gigabit Ethernet WAN OSMs” http://www.cisco.com/en/US/products/hw/routers/ps368/prod_eol_notice0900aecd8073fdf9.html

[10] CISCO SYSTEMS. “Configuring QoS on the Optical Services Modules” http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SR_OSM_config/qos.html#wpxref83687

[11] ANÓNIMO. “CISCO IOS” http://en.wikipedia.org/wiki/Cisco_IOS

[12] CISCO SYSTEMS. “Cisco Modular QoS Command Line Interface” http://www.cisco.com/en/US/technologies/tk543/tk545/technologies_white_paper09186a0080123415.html

[13] CISCO SYSTEMS. “DiffServ tunneling modes for MPLS networks” http://www.cisco.com/en/US/tech/tk436/tk428/technologies _tech_note09186a0

08022ad7e.shtml

[14] CISCO SYSTEMS. “Configuring Multiprotocol Label Switching on the OSMs” http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SXOSM_config/mpls.html

[15] CISCO SYSTEMS. “Configuring QoS” http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_see/configuration/guide/swqos.html

[16] CISCO SYSTEMS. “Cisco Catalyst 3750 QoS Configuration Examples” http://www.cisco.com/en/US/products/hw/switches/ps5023/products_tech_note09186a0080883f9e.shtml

[17] ANÓNIMO. “Calidad de servicio: Servicios Diferenciados” http://www.info-ab.uclm.es/asignaturas/42650/PDFs/practica5.pdf

[18] GEROMETTA, Oscar. “Elementos básicos de QoS” http://librosnetworking.blogspot.com/2008_04_01_archive.html

[19] ANÓNIMO. “NAT (Network Address Traslation)” http://isa.uniovi.es/~sirgo/doctorado/NAT.pdf

[20] ÁLVAREZ, Sebastián; GONZÁLEZ, Agustín. “Estudio y configuración de QoS para protocolos IPv4 e IPv6 en una red de fibra óptica WDM” http://www.scielo.cl/pdf/rfacing/v13n3/art15.pdf

[21] CISCO SYSTEMS. “Cisco IOS Software Selector” http://tools.cisco.com/ITDIT/ISTMAIN/Dispatch?act=featdesc&task=display&featureId=6502

[22] CISCO SYSTEMS. “Cisco Feature Navigator” http://tools.cisco.com/ITDIT/CFN/Dispatch?act=featdesc&task=display&featureId=6791

[23] ANÓNIMO. “Dynamips” http://en.wikipedia.org/wiki/Dynamips

[24] CISCO SYSTEMS. “Understanding packet counters in show policy-map interface output” http://www.cisco.com/en/US/tech/tk543/tk760/technologies_tech_note09186a0080108e2d.shtml

OTROS

[25] ALVARADO, Alexandra. “Manual de trabajo en Dynamips de Telconet S.A.”. Marzo 2009

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La tecnología MPLS es una solución innovadora que está teniendo gran acogida en las empresas de nuestro país como es el caso de Telconet S.A., por sus ventajas de funcionalidad sobre otra infraestructura instalada, el ofrecimiento de nuevas aplicaciones y servicios, una administración inteligente de la red para un mejor rendimiento y el cumplimiento de las exigencias de los usuarios de los servicios.

- MPLS tiene como una de sus principales ventajas el soporte de QoS, lo que permite diseñar y configurar un esquema óptimo que entregue mejores prestaciones y alcance altos grados de confiabilidad con los clientes que solicitan servicios a los ISPs.

- La integración de MPLS y DiffServ mejora las prestaciones de calidad que el tradicional servicio de “mejor esfuerzo” ha ofrecido a la mayoría de ISPs actualmente; se combina el tratamiento diferenciado de los agregados de tráfico entregado por la arquitectura DiffServ y la simplificación de los procesos de enrutamiento proporcionado por la tecnología MPLS.

- La ejecución de un análisis de tráfico permite conocer las aplicaciones y servicios que circulan por la red de un ISP, de manera que se pueda determinar los requerimientos de QoS que los distintos agregados de tráfico exigen y brindar una visión del comportamiento que tienen durante su transmisión por la red.

- El ofrecimiento de QoS al tráfico para la administración de la red disminuye considerablemente el tiempo de respuesta ante fallas en los equipos, ya que

las soluciones se transmiten de forma rápida y eficiente con mejores niveles de servicio que permitan obtener los resultados previstos.

- La determinación de los parámetros comprometidos dentro de los SLAs es un punto fundamental para establecer un esquema de QoS, ya que representa los niveles de servicio que la empresa desea alcanzar para poner a disposición de sus clientes y de los distintos tipos de tráfico que quieran transmitir.

- Los procedimientos de QoS para el control y evasión de congestión mejoran el rendimiento de una red, controlando los parámetros que definen la QoS como son ancho de banda, *jitter*, retardo y tasa de paquetes perdidos, de manera que se evite que una gran cantidad de paquetes sean descartados y disminuyan el nivel de servicio ofrecido a los clientes.

- La implementación de QoS en la red de Telconet S.A. limita la capacidad que las aplicaciones no críticas como P2P puedan utilizar durante su transmisión, evitando que consuman innecesariamente recursos y resultando en un ahorro de costos para la empresa, al no tener que aumentar la capacidad de los enlaces para transmitir el resto de aplicaciones.

- La red de Telconet S.A. se beneficia con una utilización eficiente de sus enlaces al implementar un esquema de QoS, debido a que las aplicaciones no críticas pueden ocupar todo el enlace, mientras las aplicaciones críticas no soliciten ancho de banda. De esta manera, se asegura que las aplicaciones críticas sean las que se transmitan más rápido y tampoco se bloquee las aplicaciones no críticas.

- El establecimiento de un esquema de QoS en la red con tecnología IP/MPLS de Telconet S.A. contribuye a que todos los servicios y aplicaciones que circulan, en especial las de tiempo real, obtengan una correcta asignación de recursos de acuerdo a sus requerimientos y sean servidas incluso durante periodos de congestión.

- La introducción de QoS en la red de Telconet S.A. permite ofrecer diferentes clases de servicios que cubran las diversas necesidades que los clientes puedan tener y asegurar el cumplimiento de los SLAs establecidos, generando un alto grado de satisfacción por parte del cliente.

5.2 RECOMENDACIONES

- Si el CPE no es administrado exclusivamente por el ISP, se recomienda no ubicar el módulo de clasificación de la arquitectura DiffServ en el origen, debido a que los clientes podrían setear el campo DS de forma incorrecta para asignar un tratamiento diferenciado a los agregados de tráfico que no lo necesitan y ocasionar congestión en la red del proveedor.

- Se recomienda realizar un monitoreo constante de los nodos de la red de Telconet S.A. para determinar si existen puntos de congestión y, en ese caso, establecer los procedimientos más adecuados que regulen las tasas de transmisión y consigan una comunicación fiable que ofrezca mejores niveles de QoS.

- Los procedimientos de control y evasión de congestión deben ser seleccionados cuidadosamente, ya que en lugar de mejorar el rendimiento de la red, podrían disminuir su desempeño y causar fenómenos indeseables como el de *starvation*, donde las colas de menor prioridad no son atendidas y existe un gran número de paquetes descartados.

- Entre las características mínimas que se deben tomar en cuenta al momento de adquirir un equipo están las características técnicas que posee para el soporte de QoS, de modo que cuando el ISP quiera diversificar sus servicios ofreciendo niveles de QoS en sus SLAs, no sea necesario adquirir nuevos equipos ó implementar módulos de expansión en los equipos existentes.

- Es importante tomar en cuenta las versiones de IOS instaladas en los equipos marca Cisco para establecer la forma en la que soportarán los comandos de QoS, ya que los manuales de configuración de los equipos Cisco hacen referencia a la versión de IOS requerida para la utilización de determinados comandos.

- La empresa Telconet S.A. tiene proyecciones futuras de alto crecimiento, por lo que se recomienda migrar en su totalidad a la tecnología MPLS desde el CPE en el lado del cliente, para evitar la utilización de esquemas de integración entre tecnologías que saturen de procesamiento a los equipos y disminuyan la eficiencia de los servicios entregados a los clientes.

- Se recomienda manejar un esquema de mejoramiento continuo de los procedimientos de QoS propuestos para la red IP/MPLS de Telconet S.A., con el propósito de invertir de forma más eficiente en los recursos necesarios para solventar el servicio ofrecido a los clientes.