UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

MPLS/VPN y aplicación de QoS en equipo CISCO

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ANDY JAMES CARREÑO BRICEÑO

PROMOCIÓN
2001- I

LIMA – PERÚ
2008

MPLS/VPN y Aplicación de QoS en equipo CISCO

Dedico el presente informe a:

Mi esposa, por su confianza y apoyo incondicional,

a

Mi hija, por ser la inspiración para seguir adelante,

y a

Mis padres, por su ejemplo y enseñanza brindada.

SUMARIO

En el presente informe de suficiencia se trata de explicar como se puede mejorar el rendimiento del mecanismo de envío de paquetes a través de un protocolo de conmutación de etiquetas (MPLS). También se brinda una breve revisión a las redes privadas virtuales y como trabaja ella con la red MPLS. Así mismo, se explica en que consiste la Calidad de Servicio aplicada a los enlaces de clientes que usan la red MPLS como medio de enrutamiento de información.

Se detallará los parámetros que se deben tener en cuenta en la topología de red del cliente, antes de aprovisionar un determinado enlace de datos con calidad de servicio así como los mecanismos usados para implementar dicha calidad, como son mecanismos de colas para manejar la congestión de tráfico en las interfaces de salidas de los router, como evitar la congestión a través del dropeo aleatorio de paquetes, etc. A manera de comprensión de las técnicas y modos de configuración sobre los equipos usados en las redes de datos, se adjunta configuraciones básicas con la cual debe contar cada equipo de red para garantizar una adecuada CoS.

Actualmente, los clientes vienen migrando sus servicios a la plataforma NGN, por lo que también se consideró en éste informe ver algunos conceptos sobre éstas nuevas redes, así como analizar los costos/beneficios que se tiene al realizar la migración de servicios.

En éste documento, los parámetros y/o mecanismos explicados, son desarrollados sobre equipos de Networking marca CISCO, ya que actualmente en el país, las redes de networking están basados en casi un 90% en la utilización de dichos equipos. Por lo anterior, se vió necesario explicar las consideraciones que se realizan en la empresa de telecomunicaciones en la cual me desempeño, para llegar a la elección de un determinado proveedor de equipos red, como son: validación de equipo, escalabilidad del equipo, performance del equipo, pruebas de laboratorio y verificación económica del equipo.

INDICE

PROLOGO

El protocolo de conmutación de etiquetas es usado ampliamente en las redes de datos de las empresas de telecomunicaciones que actualmente vienen brindando servicio. Es así como se se trata de explicar una breve descripción de sus componentes, funcionalidades, ventajas del MPLS; pero lo más resaltante, es la técnica del marcado de paquetes que se viene implementando para la aplicación de la calidad de servicio. El presente informe muestra de manera práctica las consideraciones para aplicar dicha calidad de la forma más eficiente, ya que la información contenida en el presente informe es la que se viene aplicando en los equipos de networking CISCO a nivel mundial.

Con éste informe se espera mostrar que tan práctico es la aplicación de la QoS en los equipos CISCO con los métodos actualmente vigentes.

En el primer capítulo se describe los componentes del MPLS, así como su fincionalidad a través de una red. Otro punto importante, es la definición de VPN's, componentes, características, tipos y enrutamientos entre los equipos que conforman la red mpls.

El segundo capítulo describe las Clases de Servicio, donde se aprecia la habilidad de diferenciar un tráfico determinado de red, asíu como tambien se explica los diferentes servicios que ofrece la CoS sobre la red MPLS. También se pude apreciar los parámetros de la calidad de servicio (QoS) que se presentan cuando se está implementando una red.

En el tercer capítulo se explica los diferentes modelos de QoS, así como los mecanismos a considerar cuando se implementa la calidad de servicio en una red, dependiendo de las exigencias, necesidades y/o recursos que disponga un determinado cliente.

El cuarto capítulo basicamente muestra la forma modular que tienen los equipos CISCO para proceder con la configuración de la calidad de servicio. También se muestra como se clasifica el tráfico para poder consideralos en la técnica del marcado de paquetes. A modo de ilustración, se ha incluido las sintaxis de configuración que se debe considerar en los equipos CISCO, así como ejemplos de configuración de clientes donde se aprecia como se marcan los paquetes de entrada para luego ser manejados a través de políticas de salida, ubicándolos en colas con determinados ancho de banda.

Adicionalmente, se anexa algunas tablas donde figura los sistemas operativos de los principales equipos CISCO que se deben considerar al momento de implementar una red, teniendo en cuenta el ancho de banda que ocupará el tráfico cursante, el hardware que dispone el equipo así como las funcionalidades y/o características que soportará el equipo elegido.

CAPITULO I

1.1. INTRODUCCIÓN

Los orígenes de MPLS se remontan a los numerosos esfuerzos realizados a mediados de los años 90, por combinar la tecnología IP y ATM. El primer gran esfuerzo para lograr una buena posición en el mercado fue el desarrollo de la tecnología IP switching, desarrollado por la compañía Ipsilon. Para competir con ésta propuesta, surgieron las propuestas de nuevos productos, por parte de varias empresas. Tales como: Cisco Systems (Tag Switching), IBM (aggregate route based IP switching), y Cascade (IP Navigator).

A partir de esta actividad, la IETF (Internet Engineering Task Force) estableció un grupo de trabajo para alcanzar un estándar común basado en todas estas tecnologías. El nombre buscado para el grupo de trabajo debía ser neutral, sin referencia a ninguna de las tecnologías mencionadas, lo que dio lugar al termino Multi Protocol Label Switching (MPLS). Es así como a finales de los 90's se vio la introducción de muchos routers que eran tan rápidos como los switch's ATM.

En conclusión, la utilidad del MPLS se presenta para el soporte de aplicaciones de: ingeniería de tráfico, de diferenciación de servicios en distintas clases (CoS) y de establecimiento de redes privadas virtuales (VPNs) sobre una topología "inteligente", muy superior en prestaciones a las soluciones tradicionales de túneles y circuitos virtuales.

MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM. También como un protocolo para hacer túneles (sustituyendo a las técnicas habituales de "tunneling"), o bien como una técnica para acelerar el encaminamiento de paquetes, ya que integra sin discontinuidades los niveles 2 (transporte) y 3 (red), combinando eficazmente las funciones de control del routing con la simplicidad y rapidez de la conmutación de nivel 2.

1.2. Componentes del Multi Protocolo de Conmutación de Etiquetas (MPLS)

MPLS emplea muchas nuevas mejoras en el ruteo IP y envío de los paquetes. Muchas de estas mejoras son similares a la Ingeniería de Tráfico y la calidad de servicio (QoS) empleadas en ATM. Muchos de sus componentes son simplemente extensiones de las tecnologías ya existentes.

El componente de envío de paquetes es responsable del transporte de un paquete basado en una tabla de ruteo. El componente de control es responsable para la construcción y mantenimiento de la tabla de ruteo, y así también trabaja con los componentes de control de otros nodos para discernir sobre las informaciones de rutas obtenidas. Cada uno de estos componentes, será explicado mas adelante.

1.2.1. La etiqueta

La etiqueta que marca a cada paquete, es un campo de unos pocos bits, de longitud fija, que se añade a la cabecera del mismo paquete e identifica una "clase equivalente de envío" (Forwarding Equivalence Class, FEC).

La etiqueta es similar a un identificador de conexión (como el VPI/VCI de ATM o el DLCI de Frame Relay), tiene solamente significado local, por consiguiente, no modifica la información de la cabecera de los paquetes; tan sólo los encapsula, asignando el tráfico a los correspondientes FEC.

1.2.2. Clase de Envío Equivalente (Forwarding Equivalence Class – FEC)

Una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales son diferentes.

1.2.3. Camino de etiquetas conmutadas (Label Switched Path – LSP)

Un LSP es un camino específico de tráfico a través de una red MPLS. Los algoritmos de intercambio de etiquetas permiten la creación de estos “caminos virtuales” denominados LSP, los cuales funcionalmente equivalen a los PVCs de ATM y Frame Relay.

Un LSP es en realidad un conjunto de LSRs por los cuales viaja un conjunto de paquetes pertenecientes a un mismo FEC para llegar a su destino. Puesto que MPLS permite una jerarquía de etiquetas conocida como Pila de Etiquetas, es posible tener

diferentes LSPs a diferentes niveles de etiquetas para que un mismo paquete alcance el destino.

1.2.4. Protocolo de distribución de etiquetas (Label Distribution Protocol – LDP)

Es la técnica más utilizada para distribuir etiquetas. Es un protocolo que opera entre LSRs adyacentes al intercambiar mapeos de etiqueta-FEC. Dos LSRs que tiene una sesión LDP entre ellos son llamados pares LDP. Es un protocolo bidireccional, de tal forma que una sola sesión basta para comunicar dos pares. LDP se caracteriza por proveer un mecanismo de descubrimiento de LSRs que permite a LSRs adyacentes encontrarse y establecer una sesión entre ellos.

Define cuatro clases de mensajes:

- DISCOVERY: Usados para anunciar y mantener la presencia de un LSR en una red.
- SESSION: Usados para establecer, mantener y terminar sesiones entre pares LDP.
- LABEL ADVERTISEMENT: Usados para crear, retirar y liberar anuncios de vínculos de etiquetas.
- NOTIFICATION: Usados para proveer información de advertencia y señal de error.

Corre sobre TCP para proveer una entrega confiable de mensajes (con excepción de los mensajes DISCOVERY).

Esta diseñado para ser fácilmente extensible, usando mensajes especificados como colecciones de objetos codificados como TVL.

1.3. Descripción funcional del Multi Protocolo de Conmutación de Etiquetas (MPLS)

La operación del MPLS se basa en las componentes funcionales de envío y control de paquetes, y que actúan ligadas entre sí.

A continuación, detallaremos la primera función:

1.3.1. Funcionamiento del envío de paquetes en el Multi Protocolo de Conmutación de Etiquetas (MPLS)

La base del MPLS está en la asignación e intercambio de etiquetas que permiten el establecimiento de los caminos LSP por la red. Los LSPs son simplex por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); el tráfico dúplex requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Label-Swiching Router - LSR) a otro, a través del dominio MPLS. Un LSR no es sino un router especializado en el envío de paquetes etiquetados por MPLS.

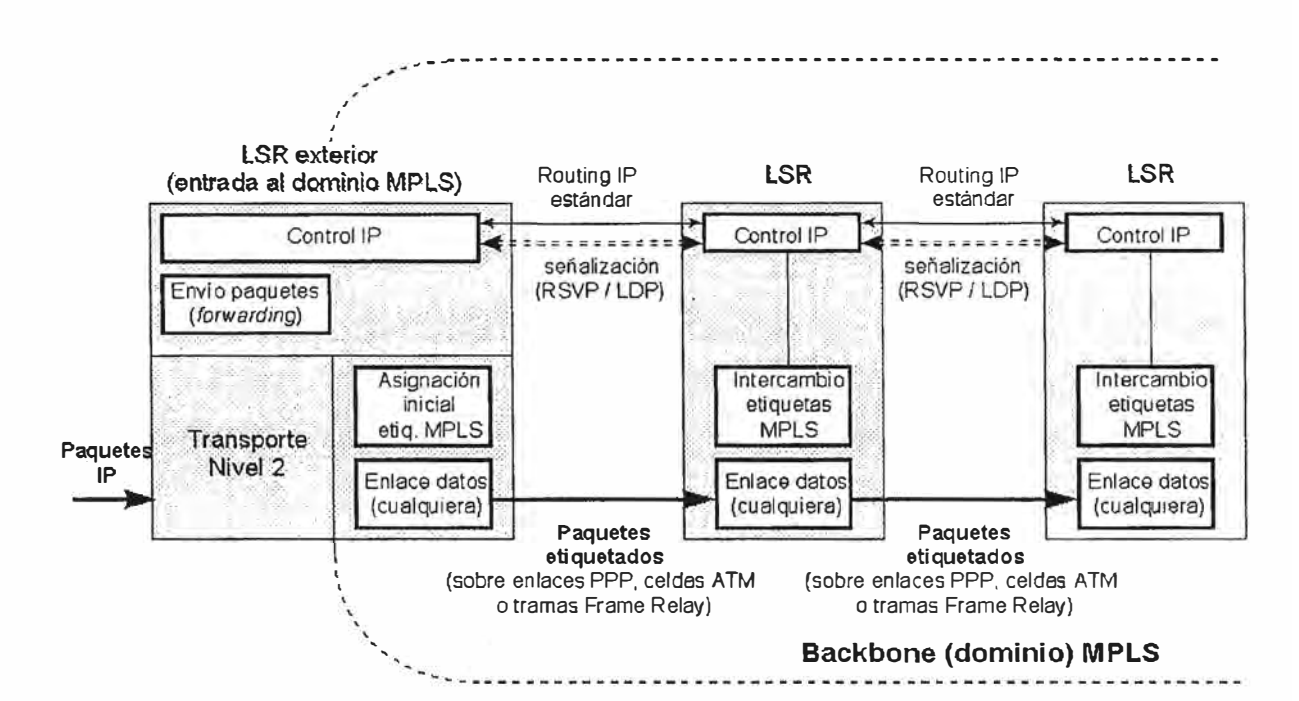


Fig. 1.1 Esquema Funcional del MPLS

Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de **control** (*routing*) y de **envío** (*forwarding*). Del mismo modo, el envío se implementa mediante el **intercambio de etiquetas** en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por el ATM; en lugar de ello, en MPLS o bien se utiliza el protocolo RSVP o bien un nuevo estándar de señalización, el *Label Distribution Protocol*, LDP.

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC.

Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS.

Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por ese interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola).

En la siguiente figura, se muestra un ejemplo del funcionamiento de un LSR del núcleo MPLS. A un paquete que llega al LSR por el interfaz 3 de entrada con la etiqueta 45, el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

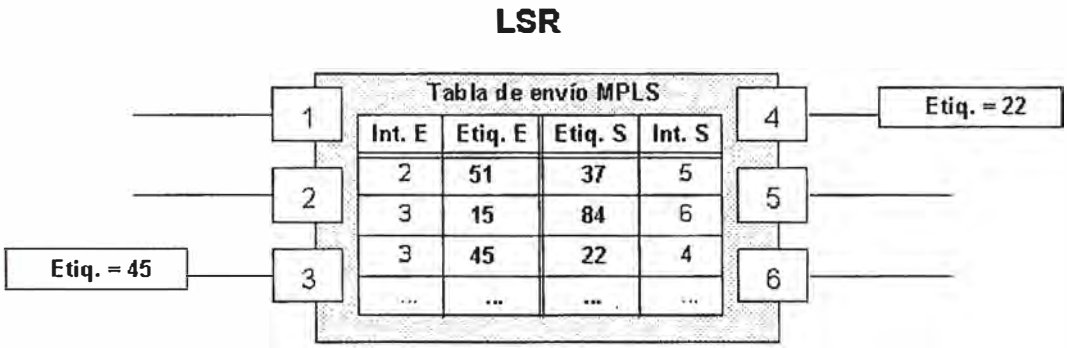


Fig. 1.2 Detalle de la tabla de envío de un LSR

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la siguiente figura, el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al

llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por routing convencional.

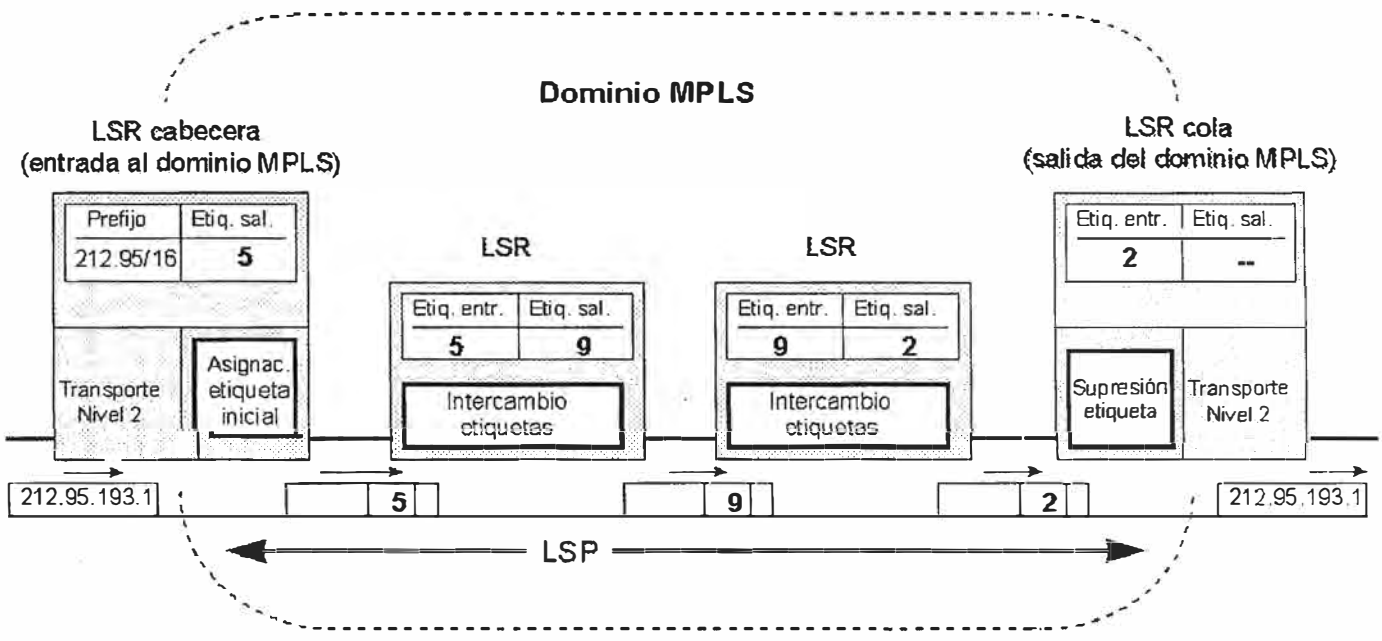


Fig. 1.3 Ejemplo de envío de un paquete por un LSP

La identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3.

Si el protocolo de transporte de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos nativo para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas (p. ej. enlaces PPP o LAN), entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

Cabecera MPLS

La Cabecera MPLS consta de 32 bits, donde cada campo se describe a continuación:

- Etiqueta (label): campo de 20 bits que lleva el valor actual de la etiqueta.
- Campo Experimental (EXP): 3 bits usados para codificar ya sea el ToS de IP o el DSCP usado en Diffserv, para fines de calidad de servicio.
- Bottom of Snack (S): 1 bit de stack para poder apilar etiquetas de forma jerárquica. Es colocado a 1 para la primera entrada en la pila de etiquetas y a 0 para todas las demás entradas.
- Time to Live (TTL): 8 bits para codificar el TTL.

En la siguiente figura se muestra el esquema de los campos de la cabecera genérica MPLS así como la relación con las cabeceras de otros niveles.

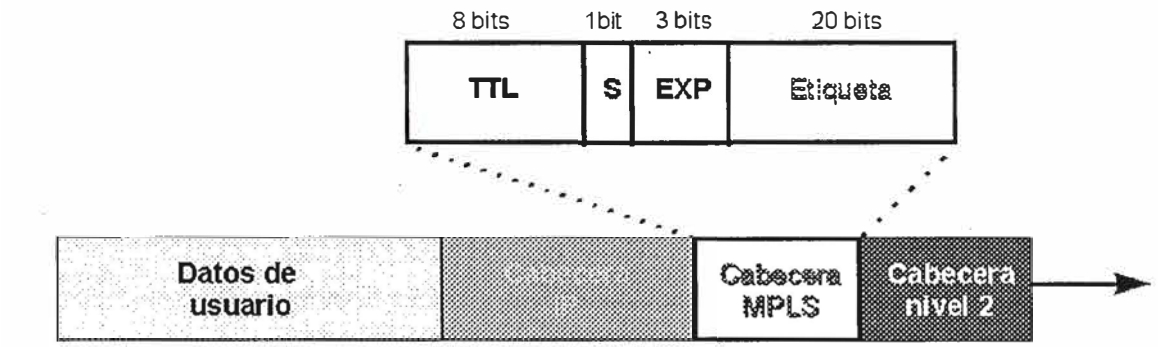


Fig. 1.4 Estructura de la cabecera genérica MPLS

En la realidad, se encapsula una pila de varias etiquetas. Por lo tanto es mejor ver la pila de etiquetas MPLS como un campo de "m" etiquetas: L(m), la cual está formada por una secuencia de entradas de cuatro octetos (anteriormente explicado).

Una vez que se recibe un paquete etiquetado, se revisa el valor de la etiqueta que se encuentra en la cima de la pila y como resultante se puede obtener: el siguiente salto que dará del paquete, y la operación a realizar en la pila antes de enviar el paquete (reemplazar la etiqueta superior, quitarla, o colocar mas entradas).

En la siguiente figura se aprecia la pila de etiquetas entre las cabeceras de capa 2 y 3. Acá se observa que el paquete de capa 3 es seguido por la entrada de la pila de etiquetas cuyo bit S es igual a 1.

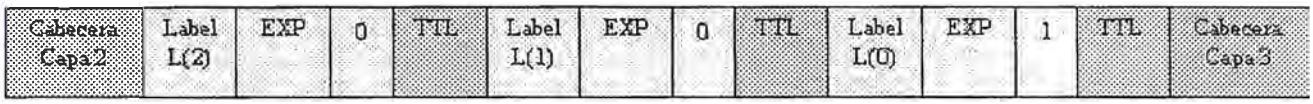


Fig. 1.5 Pila de Etiquetas MPLS

Descripción de la Operación de Reenvío de Paquetes en la Red MPLS

Los siguientes pasos, son los elementos claves de la operación del reenvío de paquetes a través del backbone MPLS:

1er Paso:

- El paquete "B" es enviado de la red no-MPLS "A" hacia el backbone MPLS.

2do Paso:

- El paquete B llega a LSR1 por la interfase if0.
- Al paquete B se le impone una determinada etiqueta de acuerdo al FEC que corresponde a su destino.
- La tabla de reenvió de LSR1 indica que B se reenvía por la interfase if2 y que su siguiente salto es a LSR2.

3er Paso:

- El paquete B llega a LSR2 por la interfase if3.
- LSR2 lee la etiqueta que lleva el paquete.
- LSR4 revisa su tabla de reenvío.
- Se cambia la etiqueta.
- Se reenvía por la interfase if1 hacia LSR4.

4to Paso:

- El paquete B llega a LSR4 por la interfase if2.
- LSR4 lee la etiqueta que lleva el paquete.
- LSR4 revisa su tabla de reenvío.
- Se retira la etiqueta del paquete B, por tratarse del último LSR.
- Se reenvía por la interfase if0 hacia la red C.

5to Paso:

- El paquete B llega a la red destino C sin etiqueta MPLS alguna. De allí en adelante será reenviado en base a su cabecera IP.

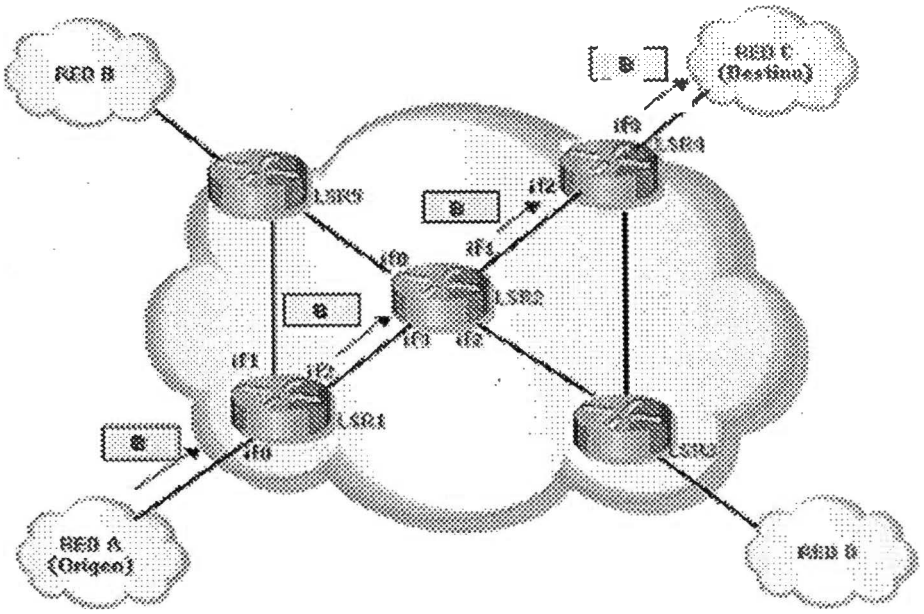


Fig. 1.6 Operación de reenvío de paquetes en la Red MPLS

1.3.2. Control de la información en MPLS

El control de la información tiene dos aspectos fundamentales:

- Cómo se generan las tablas de envío que establecen los LSPs, está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc.
- Cómo se distribuye la información sobre las etiquetas a los LSRs, se refiere a la información de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. La arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo de Servicios Integrados del IETF y Label Distribution Protocol (LDP).

El componente de control de los protocolos de enrutamiento no provee información suficiente para construir las tablas de reenvió. Por tal motivo, un LSR requiere de procedimientos que le permitan:

- Crear vínculos entre etiquetas y FECs.
- Informar a otros LSRs de los vínculos creados.
- Construir y mantener la tabla de reenvío que usara el componente de reenvío.

A continuación se muestra como el componente de control construye una tabla de reenvío MPLS:

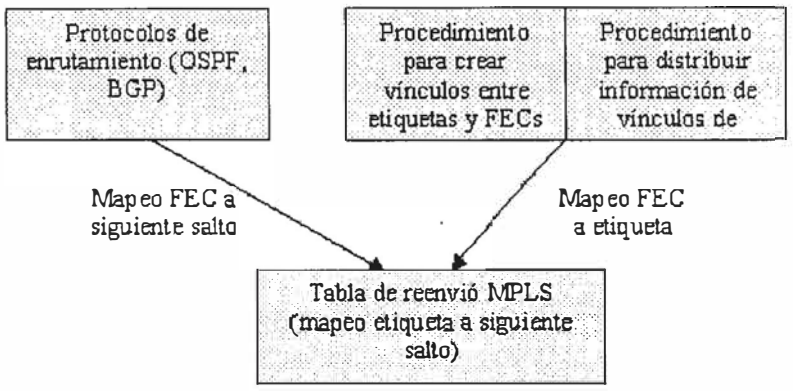


Fig. 1.7 Construcción de una Tabla de Reenvío MPLS

Distribución de Etiquetas

Parte del componente de control consiste en informar a otros LSRs la existencia de los vínculos FEC-etiqueta creados, para que sus tablas de reenvió pueden ser actualizadas y mantenidas. La información de vínculos puede ser intercambiada por un protocolo dedicado como LDP o por protocolos que usan atributos adicionales para realizar un piggyback a la información de vínculos de etiquetas, por ejemplo RSVP, MP-BGP, etc.

1.4. Protocolo de Puerta de Entrada de Frontera (Border Gateway Protocol - BGP)

BGP surge debido al rápido crecimiento de Internet y con la urgente necesidad de contar con un protocolo de enrutamiento altamente escalable, que interconecte sistemas autónomos. Un sistema autónomo, denotado como AS, es un grupo de redes que comparten las mismas políticas de enrutamiento. Cada AS tiene un número de sistema autónomo, un campo de 16 bits asignado por la Internet Numbers Association (IANA). Border Gateway Protocol (BGP) es un protocolo de enrutamiento Inter-sistemas autónomos. Es el reemplazo de EBGP.

Una maquina BGP que envía mensajes BGP es llamada "parlante BGP". Su función principal es intercambiar información de accesibilidad (reachibility) de red con otros AS's. Un BGP parlante anuncia a sus pares (otros parlantes BGP con los cuales se comunica directamente) de los sistemas autónomos vecinos, solo aquellas rutas que el mismo usa. Esta regla refleja el enrutamiento hop-by-hop usado a lo largo de la actual Internet.

BGP funciona sobre un protocolo de transporte confiable. BGP usa TCP como su protocolo de transporte y establece sus conexiones mediante el puerto TCP 179.

1.4.1. Modo de Operación

Al inicio de una sesión, los sistemas BGP intercambian información de enrutamiento enviando una tabla de rutas BGP completa.

A partir de allí solo se intercambian actualizaciones incrementales mediante mensajes de actualización (update). Por lo tanto, un parlante BGP debe retener la versión actual de las tablas BGP de todos los pares por la duración de la conexión. BGP usa mensajes de permanencia de vida (keepalive) para asegurar que una conexión siga activa. Si una conexión encuentra una condición de error, se envía un mensaje de notificación y se cierra la conexión.

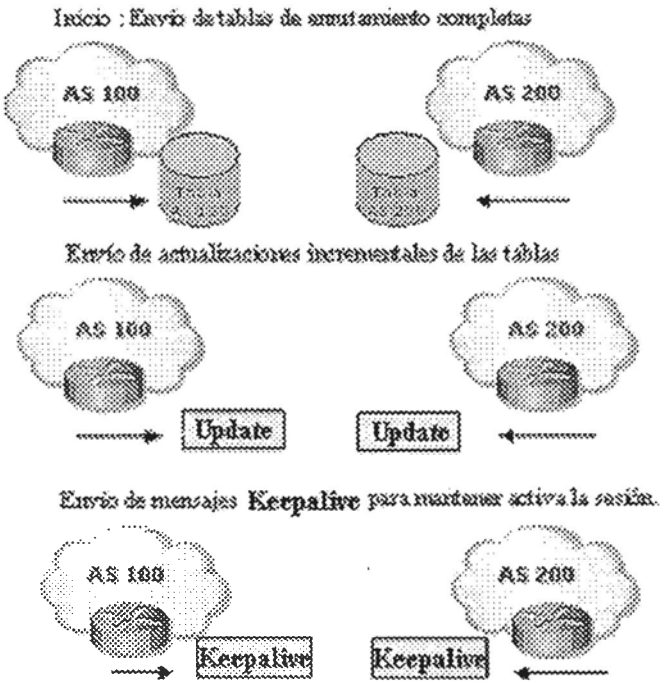


Fig. 1.8 Operación de BGP

Si un AS particular tiene varios parlantes BGP y provee el servicio de tránsito para otros sistemas autónomos, entonces se debe tener cuidado para asegurar un enrutamiento consistente dentro del AS, la cual es provista por el protocolo de enrutamiento interior, forzando a que todos los parlantes BGP dentro del AS mantengan conexiones BGP directas unos con otros. Usando un conjunto de políticas, los parlantes BGP llegan a un acuerdo en que enrutadores de frontera servirán solo como puntos de salida o entrada para un destino particular fuera del AS. Esta información es comunicada a los enrutadores internos AS, vía el protocolo de enrutamiento interior. Es importante asegurar que todos los enrutadores internos han sido actualizados con la información de tránsito antes de que los parlantes BGP anuncien a otros AS que el servicio de tránsito esta siendo provisto.

1.4.2. Sesiones BGP internas y externas (iBGP y eBGP)

A las conexiones entre parlantes BGP de diferentes sistemas autónomos, son llamados como enlaces "externos". Similarmente, un par en un diferente sistema autónomo es referido como un par externo, mientras un par en el mismo AS puede ser descrito como un par interno. Cuando BGP es establecido entre pares internos, es llamado como BGP interno (iBGP), en comparación a BGP externo (eBGP), el cual corre entre pares externos.

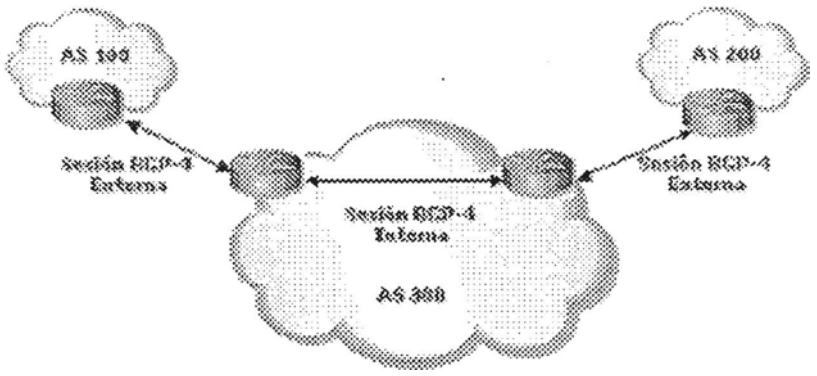


Fig. 1.9 Sesiones iBGP y eBGP

Cuando un parlante BGP recibe el anuncio de una ruta de un par sobre un enlace eBGP, anuncia esta ruta a todos los otros parlantes BGP en el sistema autónomo solo si la ruta es mejor que otras rutas conocidas. Esta información esta contenida en el mensaje update, donde los atributos de rutas son parte de este mensaje.

A continuación se muestra unas cuantas terminologías usadas en BGP:

- AS-PATH: es la lista de números de AS que la ruta atraviesa para llegar al destino red anunciada.
- ORIGIN: define el origen de la información de la ruta. Puede ser IGP, EGP, etc.
- NEXT_HOP: es la dirección IP del enrutador de frontera que es usado como el siguiente salto utilizado para alcanzar un destino.
- UNREACHABLE: notifica al parlante BGP que una ruta previamente anunciada se ha vuelto inalcanzable.
- LOCAL_PREF: indica al AS cual es la ruta de salida preferida para alcanzar una red determinada. La mejor ruta será la de mayor preferencia local.
- COMMUNITY: es un grupo de destinos que comparten alguna propiedad común.

1.5. Ingeniería de Tráfico

Las redes de multiservicio necesitan una forma para controlar la cantidad creciente de tráfico que se debe manejar. Este tráfico es dinámico y difícil de predecir debido a que los flujos están constantemente cambiando y por ende, no necesariamente se adaptan a la topología de red que ha sido establecida. El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red.

La Ingeniería de Tráfico vía MPLS permite que el tráfico sea "mapeado" eficientemente de acuerdo a las topologías de red existentes. Al establecer rutas manualmente a través de una red para acomodar el tráfico, MPLS ofrece un control sobre el tráfico, a diferencia de los algoritmos de enrutamiento tradicionales que no permiten hacer esto.

La Ingeniería de Tráfico vía MPLS mejora la confiabilidad de la red multiservicio en dos maneras. Primero, permite que el Proveedor de Servicio enrute tráfico alrededor de puntos de congestión, para evitar zonas "calientes" en la red y cuellos de botella. Segundo, las rutas MPLS que atraviesan una red pueden ser configuradas para tener redundancia y balanceo de carga. Esto permite asegurar que el tráfico crítico siempre tenga una ruta a través de la red.

La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos). En la siguiente figura, se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

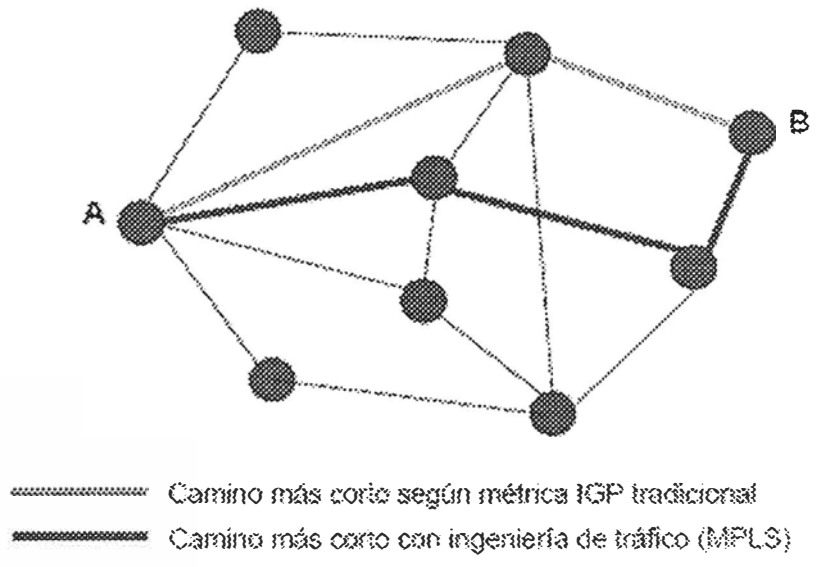


Fig. 1.10 Comparación entre camino mas corto IGP con Ingeniería de Tráfico.

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 routers correspondientes haga aconsejable la utilización del camino alternativo indicado

con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que:

- Permite al administrador de la red, el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.
- Permite hacer "encaminamiento restringido" (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

1.6. Red Privada Virtual (Virtual Private Network - VPN)

Una VPN es una red privada que se construye dentro de una infraestructura de red pública, como la Internet global, que utilizan las mismas políticas de gestión, calidad de servicio y seguridad que son aplicadas a una red privada.

Las VPN's brindan una alternativa para construir una red privada para comunicación entre diversas sedes a través de una red pública o el Internet. Con una VPN, un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre el PC del empleado y un router VPN en la sede.

Las redes WAN tradicionales conectan las diversas sedes vía enlaces punto a punto dedicados. Esto significa que múltiples circuitos independientes tienen que ser asignados, lo cual hace que el despliegue sea no escalable y difícil de mantener. Las VPNs extienden el concepto clásico de WAN, reemplazando los enlaces físicos punto a punto, con enlaces lógicos que comparten una infraestructura común.

Hay dos formas en que las empresas pueden implementar y manejar una VPN. Es posible desplegarla y manejarla con sus propios recursos, o en su defecto se tiene siempre

la opción de utilizar los servicios de un Proveedor que se encargue de gestionar la VPN como un todo, de acuerdo a sus particulares necesidades de negocio.

1.6.1. Tipos de VPN

Una VPN se define como la conectividad de un cliente desplegada en una infraestructura compartida con las mismas normas que una red privada. La infraestructura compartida puede facilitar un proveedor de servicios IP, Frame Relay, un backbone ATM o Internet. Hay tres tipos de VPN según el modo en que las empresas y organizaciones utilizan las VPN:

VPN de Acceso

Las VPN's de acceso remoto, también conocidas como VPDN (Virtual Private Dial up Network), son desplegadas para usuarios remotos individuales conocidos como usuarios móviles. Proporciona acceso remoto a una Intranet o Extranet corporativas sobre una infraestructura compartida con las mismas normas que una red privada. Las VPN de acceso permiten a los usuarios acceder a los recursos corporativos, siempre que lo requieran. Abarcan tecnologías analógicas, de marcación, RDSI (Red Digital de Servicios Integrados), de línea digital de abonado (DSL), IP móvil y de cable para conectar con seguridad a usuarios móviles como teletrabajadores y a sucursales.

Anteriormente, las empresas soportaban estos usuarios vía redes telefónicas (Dial Up) lo cual resultaba inconveniente especialmente cuando la llamada era de larga distancia. Actualmente, un usuario móvil puede hacer una llamada local a su Proveedor de Servicios (ISP) para acceder vía Internet a su red corporativa, desde su PC en dondequiera que se encuentre. En este caso, el software en la PC provee una conexión segura, frecuentemente conocida como un "túnel", hacia la red corporativa.

VPN de Sitio a Sitio

Las VPN's de sitio a sitio son desplegadas para interconectar sedes de una empresa. En otras palabras, la red de una sede es conectada a la red de otra sede, vía una VPN. Con el acceso a Internet de ahora, las líneas dedicadas o los circuitos frame relay pueden ser reemplazados con VPN's de sitio a sitio. Las VPN's de sitio a sitio pueden ser vistas como VPN's de Intranet o de Extranet, dependiendo si las conexiones entre sedes pertenecen o no a la misma Organización:

- VPN de Intranet: Enlaza oficinas centrales corporativas, oficinas remotas y sucursales sobre una infraestructura compartida que utiliza conexiones dedicadas. Las empresas disfrutan de las mismas normas que las de una red privada, entre las cuales se incluyen la seguridad, la calidad del servicio (QoS), la manejabilidad y la fiabilidad. Las redes internas VPN difieren de las redes externas VPN, ya que sólo permiten el acceso a empleados de la empresa. Los servidores de Web de red interna son distintos de los servidores de Web públicos, ya que es necesario que un usuario público cuente con los correspondientes permisos y contraseñas para acceder a la red interna de una organización. Las redes internas están diseñadas para permitir el acceso por usuarios con privilegios de acceso a la LAN interna de la organización. Dentro de una red interna, los servidores de Web se instalan en la red. La tecnología de navegador se utiliza como interfaz común para acceder a la información, por ejemplo datos financieros o datos basados en texto y gráficos que se guardan en esos servidores.
- VPN de Extranet: Enlazan clientes, proveedores, socios o comunidades de interés con una Intranet corporativa sobre una infraestructura dedicada que utiliza conexiones dedicadas. Las empresas disfrutan de las mismas normas que la de una red privada, entre las cuales se incluyen la seguridad, la calidad del servicio (QoS), la manejabilidad y la fiabilidad. Las redes externas VPN difieren de las redes internas VPN, ya que permiten el acceso a usuarios que no pertenecen a la empresa. Las redes externas hacen referencia a aplicaciones y servicios basados en la red interna, y utilizan un acceso extendido y seguro a usuarios o empresas externas. Este acceso generalmente se logra mediante contraseñas, identificaciones de usuarios, y seguridad a nivel de las aplicaciones. Por lo tanto, una red externa es la extensión de dos o más estrategias de red interna, con una interacción segura entre empresas participantes y sus respectivas redes internas.

VPN's basadas en Firewall

Son un tipo particular de implementación de VPN'ss de sitio a sitio, donde el componente de seguridad es resaltado. Se utilizan cuando se requiere medidas de seguridad perimetral más avanzadas, lo que implica mejorar las capacidades técnicas de los firewalls existentes en las redes de las empresas.

1.6.2. Protocolos usados en las VPN's

- PPTP: Point-to-Point Tunneling Protocol, como protocolo de túnel encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet. PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de Internet utilizando PPTP. La técnica de encapsulamiento de PPTP se basa en el protocolo Encapsulación de Ruteo Genérico (Generic Routing Encapsulation - GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.
- IPSec: IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme. Provee mediante dos protocolos, que son Authentication Protocol y Encapsulated Security Payload (ESP):
    - Confidencialidad: los datos transferidos son sólo entendidos por los participantes de la sesión.
    - Integridad: Los datos no son modificados en el trayecto de la comunicación.
    - Autenticidad: Referente a la validación de remitente de los datos.
    - Protección a repeticiones: se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

1.7. MPLS-VPN

MPLS-VPN proporciona un enrutamiento simple con el sitio del cliente y un aprovisionamiento sencillo en la red del proveedor, además permite la creación de topologías difíciles de implementar.

En la arquitectura MPLS-VPN, se tienen 3 tipos de dispositivos:

- PE, enrutador frontera del proveedor con conexión a los clientes.
- P, enrutador interno en la red del proveedor, sin conexión a los clientes.
- CPE, enrutador frontera en el sitio del cliente, conectado a algún PE.

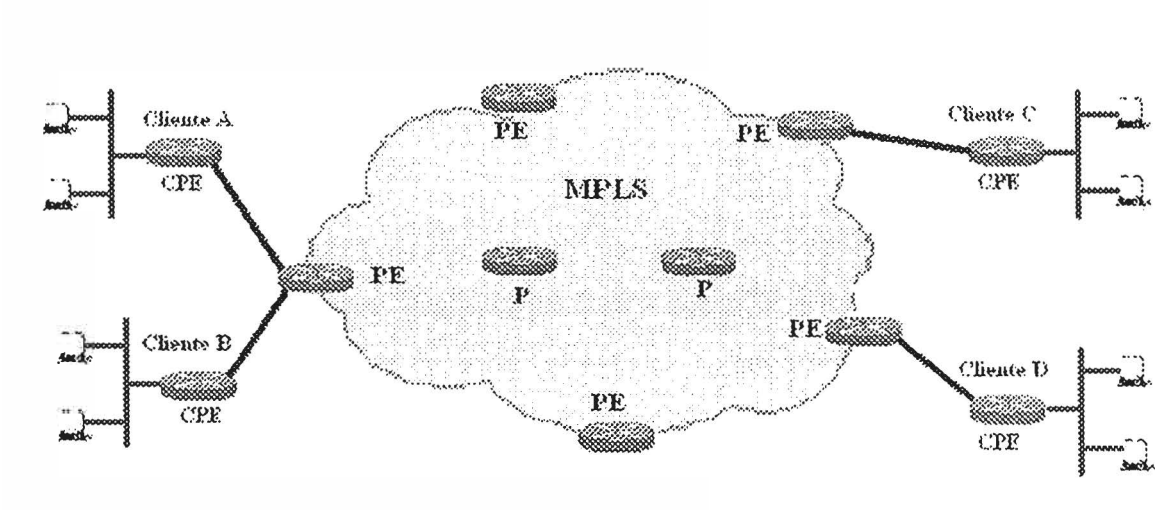


Fig. 1.11 Arquitectura MPLS-VPN

El aprovisionamiento de los recursos de red para cada una de las VPN se realiza con base a etiquetas MPLS y un concepto conocido como router virtual.

1.7.1. Router Virtual

Cada router PE es capaz de administrar en forma aislada la información de enrutamiento de varias VPN mediante la función de Router Virtual.

Bajo este concepto, para cada VPN es creada una tabla de enrutamiento totalmente independiente conocida como VRF (VPN Routing and Forwarding Instance), donde en cada VRF solo aparece la información de los prefijos de red correspondientes a la VPN del cliente.

Esta función permite asignar a los clientes un plan de direccionamiento privado e incluso utilizar el mismo direccionamiento en varias VPN.

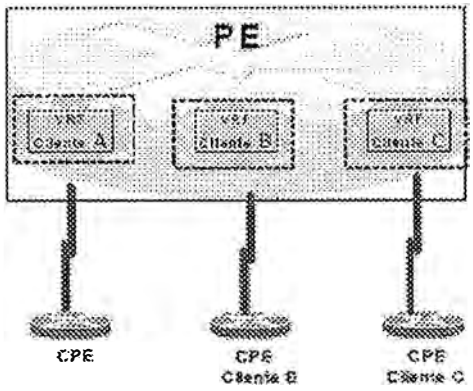


Fig. 1.12 Router Virtual

1.7.2. Asignación de Interface

Cuando se conecta un CPE a un PE la interfaz utilizada en el PE para recibir el enlace desde el CPE debe ser asignada en forma fija a la VRF correspondiente a la VPN del cliente. Para el CPE en el sitio del cliente es transparente esta asignación. Sobre el enlace entre el CPE y el PE se realiza el intercambio de la información de enrutamiento, la cual solo se vera reflejada en la VRF que corresponda a la VPN del cliente conectado.

1.7.3. Enrutamiento entre CPE y PE

El intercambio de información de enrutamiento entre CPE y PE puede realizarse utilizando distintos protocolos, estos pueden ser:

- RIP v2
- OSPF
- EIGRP
- BGP
- Rutas estáticas

Cualquiera de ellos sirve para poblar la tabla de enrutamiento en el CPE y la VRF en el PE con la información de los prefijos de red de todos los sitios del cliente.

1.7.4. Enrutamiento entre PE

Normalmente una MPLS-VPN interconecta múltiples sitios conectados a diferentes PE en la red del proveedor, esta condición obliga a que los PE tengan que intercambiar entre sí información de enrutamiento relacionada a cada una de las VPN.

El intercambio de esta información se logra mediante la integración de varios protocolos de enrutamiento en la red del proveedor. Estos protocolos son:

- Un IGP como OSPF para anunciar las rutas internas
- MPLS-IP Unicast para la creación de la malla LSP interna
- BGP para el establecimiento de sesiones IBGP entre todos los PE de la red
- MP-BGP para el intercambio de la información de enrutamiento de cada una de las VPN.

Además se agregan un par de elementos a la información de enrutamiento que permiten un transporte confiable y aislado de las rutas del cliente, estos elementos son:

- Route Distinguisher (RD)
- Route Target (RT)

Route Distinguisher

La facilidad de manejar el mismo plan de numeración en varias VPN y el utilizar un solo protocolo para el intercambio de la información de enrutamiento (MP-BGP) implicaría una confusión en los procesos de enrutamiento.

Para solucionar este problema es utilizado un distintivo de ruta, RD (Route Distinguisher) el cual es añadido a cada uno de los prefijos de red aumentando la longitud del prefijo de 32 a 96 bytes, obviamente el RD debe ser diferente para cada VRF. MP-BGP tiene las condiciones para transportar información de rutas de esta longitud.

Route Target

El Route Target (RT), es un indicador que se anexa a las rutas correspondientes a una VPN. Este indicador se transporta junto con la información de ruta utilizando MP-BGP y es idéntico para todas las rutas anunciadas desde una VRF.

La información de rutas acompañada por el RT es transportada a través de las sesiones MP-BGP y llega a todos los PE, y entonces aquellos PE que incluyan sitios de la VPN del cliente importarán la información basados en el RT y la incluirán en la VRF correspondiente.

CAPITULO II

2.1 Clases de Servicio (CoS)

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo de Servicios Diferenciados (DiffServ) del IETF. Éste modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico, transferencia de archivos (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de vídeo, video conferencia, voz, etc. Para ello se emplea el campo de Tipo de Servicio (ToS - *Type of Service*), el cual ha sido denominado por DiffServ como el octeto DS. Lo anterior vendría a ser la técnica QoS de marcar los paquetes que se envían a la red. MPLS. Más adelante se verá con detalle el Modelo DiffServ.

MPLS se adapta perfectamente a éste modelo (DiffServ), ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De es te modo, una red MPLS puede transportar distintas clases de tráfico, ya 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 los bits del campo EXP
- entre cada par de LSR exteriores se pueden aprovisionar múltiples LSP's, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo, un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio, los que lógicamente, tendrán distintos precios.

Entonces, la CoS se refiere a la habilidad de una red de proporcionar el servicio diferenciado a un tráfico determinado de red. Las características de las CoS proporcionan redes mejoradas y predecibles, lo cual se logra:

- Proporcionando Ancho de Banda Dedicado
- Mejorando las características de pérdida de paquetes.
- Evitando y Manejando la congestión de la red.
- Dando forma al tráfico de la red (SHAPING)
- Asignando prioridades al tráfico de la red

Las CoS sobre MPLS, ofrece los siguientes servicios:

2.1.1. Tasa de acceso comprometido (CAR - committed access rate)

- **Servicio:** Clasificación de paquetes.
- **Función:** Los paquetes son clasificados en el borde de la red antes de que las etiquetas sean asignadas.
- **Descripción:** CAR es a menudo configurado en interfaces que están en el borde de la red para controlar el tráfico de entrada y salida de la red. CAR usa bits de tipo de servicio (ToS) en la cabecera IP para clasificar paquetes de acuerdo a la tasa de transmisión de entrada y salida. Permite configurar el bit experimental MPLS o el bit IP precedente/DSCP.

2.1.2. Detección temprana aleatoria por peso (WRED – weighted random early detection)

- **Servicio:** Evita la congestión.
- **Función:** Las clases de paquetes son diferenciados por la probabilidad de pérdida de paquetes (drop), basados en el bit experimental MPLS o el bit IP precedente/DSCP.
- **Descripción:** WRED monitorea el tráfico de la red, intentando anticipar y prevenir la congestión de la red. WRED puede, selectivamente, descartar el tráfico de baja prioridad cuando una interface y empieza a congestionarse.

2.1.3. Encolamiento por peso (WFQ - weighted fair queuing)

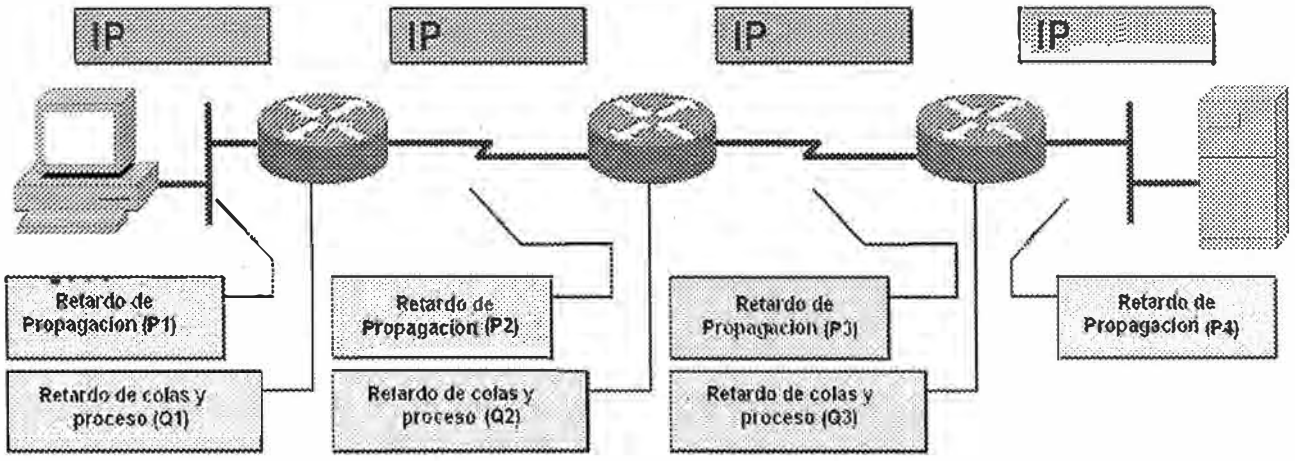
- **Servicio**: Administración de congestión.
- **Función:** las clases de paquetes son diferenciados basados en el ancho de banda y retraso limitado (delay).
- **Descripción:** Es un sistema de planificación automatizada que proporciona el ancho de banda asignado a todo el tráfico de la red, es decir, asegura el ancho de banda asignado a las indiferentes clases de tráfico de la red. WFQ usa los pesos (prioridades) para determinar cuanto ancho de banda tiene asignado cada clase de tráfico.

2.2 Parámetros de QoS

Los principales parámetros de QoS que se presenta cuando se implementa una red son: retardo de extremo a extremo, variación de retardo, pérdida de paquetes y ancho de banda. A continuación se explicará cada uno de estos parámetros:

2.2.1. Retardo de extremo a extremo (end-to-end Delay)

Este parámetro se refiere al período de tiempo que demora el paquete en transmitirse por la red de su origen hasta su destino. Los retardos pueden ser de propagación, serialización, de colas y procesos.



Delay = P1 + Q1 + P2 + Q2 + P3 + Q3 + P4 = X ms

Fig. 2.1 Retardo de extreme a extremo

Los **retardos de propagación** (Propagation Delay), depende del medio de transmisión entre cada dispositivo de la red (cobre, fibra, etc.) y se define como el tiempo que se demora en transmitir un paquete a través del medio de transmisión.

Los retardos **por serialización** (Serialization Delay), se debe al tiempo que se necesita para registrar todo los bits de un paquete y poner una trama en el medio físico (medio de transmisión) para que se transporte.

Los **retardos por procesos** (Processing Delay), se presenta en los dispositivos de la red (router), y se define como el tiempo que demora el router en tomar el paquete de la interface de entrada y colocarlo en la cola de la interface salida del router. Los motivos pueden ser variados (procesamiento del equipo, modelo de equipo, etc.).

Y los **retardos de cola** (Queuing Delay), es el tiempo en que el paquete se demora en la cola de salida del router. Este retardo, depende del número y tamaño de paquetes que se tenga en la cola, del ancho de banda se tenga en la interface y del mecanismo de cola que se este usando.

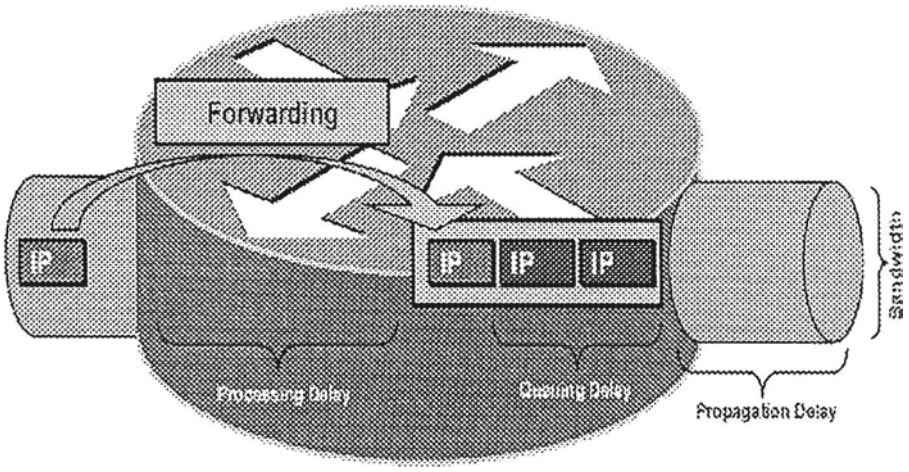


Fig. 2.2 Tipos de Retardo

Para reducir el Delay, se recomienda transmitir (forward) los paquetes mas importantes y comprimir las cabeceras (HEADER) de los paquetes.

2.2.2. Variación de retardo (jitter)

La variación de retardo, se tiene cuando en la red se presenta las variedades de retardos anteriormente mencionados.

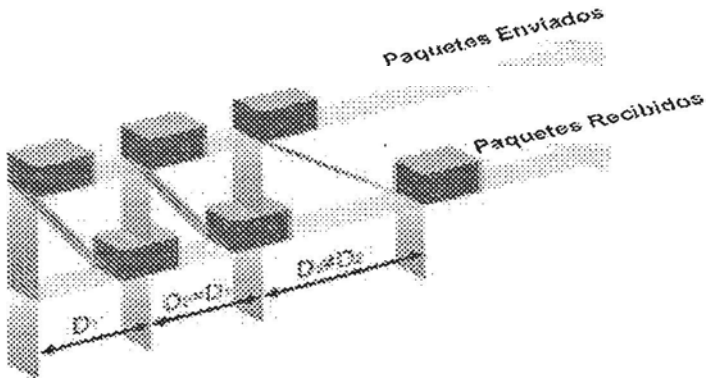


Fig. 2.3 Variación de Retardo

2.2.3. Pérdida de paquetes

Generalmente ocurre, cuando en el router se ha llenado el buffer de una determinada interface (cola de salida). También ocurre en la cola de entrada, cuando el CPU se encuentra congestionado y no puede recibir más paquetes, motivo por el cual el CPU ya no puede asignar un buffer libre para aquellos paquetes que están llegando. También ocurre cuando el equipo detecta una trama con errores (CRC – Cyclic Redundancy Check).

También se le conoce como Trail Drop ya que comienza a eliminar (droppear) paquetes cuando el "buffer space" de un dispositivo se encuentra lleno.

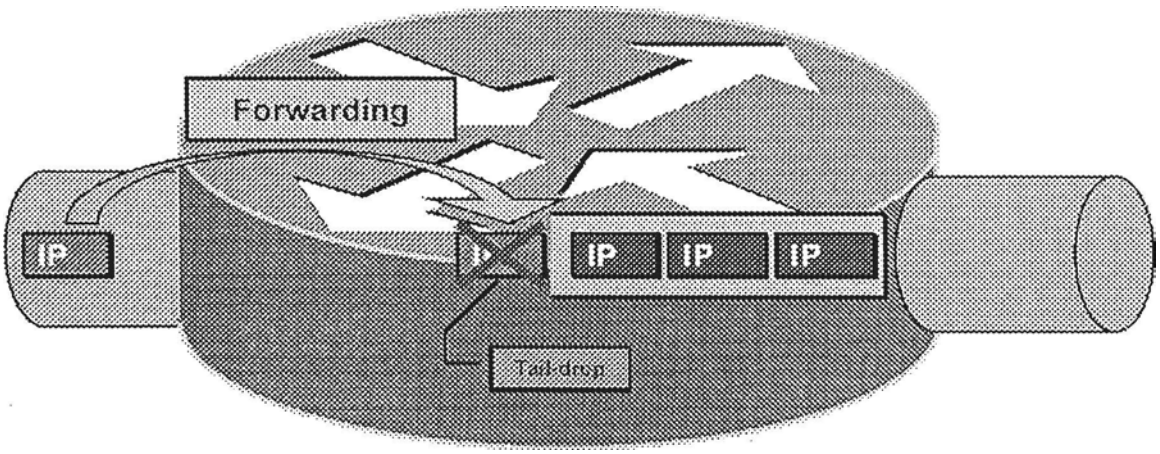


Fig. 2.4 Eliminación de paquetes – Trail Drop

Para prevenir la pérdida de paquetes, se debería garantizar un ancho de banda (BW) suficiente para los paquetes mas sensibles, ó prevenir la congestión eliminando

aleatoriamente (ramdomly dropping) los paquetes menos importantes antes de que ocurra dicha congestión.

2.2.4. Ancho de Banda

Este parámetro se define y según las aplicaciones que tenga el cliente. Actualmente algunas empresas envían archivos muy pesados o emplean aplicaciones multimedia, en el cual se usa voz y vídeo. Para que la transmisión de estos archivos o uso de estas aplicaciones no se vean degradadas, es necesario incrementar el ancho de banda, lo cual a veces puede ser muy costoso.

Existen mecanismos en el cual se puede optimizar el flujo de estos trágicos, uno de ellos es clasificar el tráfico en clases y darle una prioridad según el requerimiento del usuario. Por ejemplo, para la voz es necesario darle una máxima prioridad y para transferencia de archivos a una baja prioridad. Lo anterior se traduce en tomar algo del ancho de banda de aplicaciones menos importantes y brindárselo a las aplicaciones mas importantes.

Otro mecanismo podría ser la compresión de la cabecera de los paquetes (HEADER), usado en redes donde los paquetes cargan cantidades pequeñas, es decir, donde la carga útil de la cabecera es pequeña. Se recomienda usar éste mecanismo cuando la relación entre el campo de información y cabecera es de aprox. 3 a 2. Por ejemplo, este mecanismo se observa en la compresión espacio de cabecera de TCP. Pero aplicar compresión, implica que aumentará el retardo debido a la complejidad de algoritmos de compresión.

CAPITULO III

3.1 Modelos de QoS

3.1.1 Mejor Esfuerzo (Best Effort)

En éste modelo, los router asumen que existe recurso necesario de ancho de banda para transmitir los paquetes, y cuando no es posible transmitir el paquete, éste es descartado. Es el modelo mas sencillo que hay, ya que todos los paquetes son tratados de la misma forma, sin clasificación y/o prioridad. Usa el modelo de cola FIFO (First in – First out).

El Protocolo de Transferencia de Archivo (FTP) se caracteriza por usar éste modelo, es por eso que algunas veces se presenta degradaciones en la comunicación de datos.

Las **ventajas** de Best Effort son:

- No usa configuraciones especiales de QoS, es fácil y rápido de usar.
- Presenta escalabilidad casi ilimitada. La única forma que sea limitada es cuando el ancho de banda es limitado, por lo que todo el tráfico tendría el mismo retraso (delay).

Las **desventajas** de Best Effort son:

- No brinda alguna garantía de que los paquetes lleguen en orden o que lleguen a su destino.
- No existe un tratamiento especial entre los paquetes, o cual puede degradar la comunicación de datos críticos.

3.1.2 Servicios Integrados (IntServ)

Es un servicio que requiere la reserva de recursos en la red para garantizar que los paquetes lleguen a su destino final. El IntServ reservar un ancho de banda determinado para cierto tráfico en la red, por lo que otro tipo de tráfico no puede hacer uso de este

ancho de banda reservado. Si no se llegara a usar este ancho de banda reservado, se perdería su uso para otro tipo de aplicaciones.

En éste modelo, se presenta el protocolo de reservación de recurso (Resource Reservation Protocol RSVP), cuyo rol en la arquitectura QoS es proporcionar el control de la admisión del recurso para la voz sobre red del IP (VOIP). Si los recursos se encuentran disponibles, RSVP acepta una reserva e instala un clasificador del tráfico en la trayectoria de envió del QoS. El clasificador de trafico dice a la trayectoria de envió del QoS como clasificar los paquetes de un flujo en particular y qué tratamiento de envió se le va a brindar.

A continuación, algunas **ventajas** de aplicar IntServ y RSVP:

- El RSVP señala peticiones de los QoS por flujo individual. La red puede entonces proporcionar garantías a estos flujos individuales. El problema con esto es que el IntServ no escala a las redes grandes debido al número grande de flujos actuales de RSVP.
- RSVP informa a los dispositivos de la red, los parámetros del flujo (las direcciones del IP y números de acceso).
- IntServ apoya el control de la admisión, el cual permite que una red rechace la nueva sesión del RSVP de una de las interfaces que ha alcanzado el límite, es decir, cuando todo el ancho de banda reservable se encuentra reservado (ocupado).

A continuación, algunas **desventajas** de aplicar IntServ y RSVP:

- Se tiene que señalar continuamente para saber las operaciones RSVP.
- RSVP no es escalable para las redes grandes, donde por flujo las garantías tendría que ser hechas a los simultáneos de millares de flujos RSVP.

3.1.3 Servicios Diferenciados (DiffServ)

El DiffServ fue diseñado para superar las limitaciones que presenta los dos modelos anteriormente mencionados. Los mecanismos de QoS se usan sin previa señalización. Las políticas de QoS son establecidas independientemente en cada dispositivo intermedio de la red, es decir, las características de QoS tales como ancho de banda y retardo son manejadas sobre una base del salto por salto (hop-by-hop).

Con DiffServ, el tráfico se divide o se clasifica en clases según el requerimiento del cliente. A cada clase se le puede asignar un nivel de servicio. Cuando los paquetes viajan a

través de la red, los dispositivos de la red identifican a que clase pertenecen cada paquete, y son tratados según el nivel de servicio que posean.

El DiffServ solicita un nivel de servicio cuando envía un paquete, la red reconoce el nivel de servicio, y el paquete es tratado según lo requerido.

Las **ventajas** de trabajar con DiffServ son:

- Es altamente escalable.
- Se puede asignar diferente niveles de calidad.

Las **desventajas** de trabajar con DiffServ son:

- No brinda una garantía absoluta de la calidad de servicio.
- Su implementación es compleja a través de la red.

En éste modelo, surge el denominado per-hop behaviors (PHB), que nos es otra cosa que el comportamiento independiente que tiene cada dispositivo de la red, es decir, un dispositivo no sabe como se comporta el anterior o siguiente dispositivo de la red.

La arquitectura DiffServ se basa en la clasificación y posible condicionamiento del tráfico ingresante a la red, el cual se realiza en el borde de la red (network edge). Luego, la clase de tráfico es identificado por un punto de código del DiffServ, denominado DSCP (DiffServ Code Point) o por un bit de marcado en la cabecera IP.

Los valores de DSCP son usados para marcar paquetes o seleccionar un PHB. Dentro de la red, los paquetes son transmitidos de acuerdo al PHB el cual está asociado al DSCP.

Uno de los principios primordiales del DiffServ, es marcar los paquetes al borde de la red, tan cerca como sea posible.

A continuación se verá el formato básico de DSCP y el propósito del campo DSCP en la Cabecera IP (Header IP):

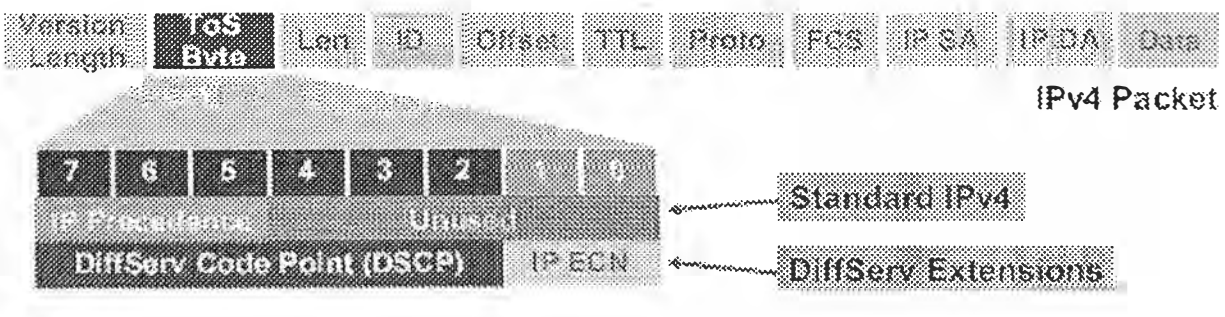


Fig. 3.1 Formato del DSCP

DiffServ usa el campo DiffServ en la cabecera IP para marcar los paquetes de acuerdo a su clasificación dentro de un comportamiento agregado (BA – behavior aggregate). El BA se refiere a un grupo de paquetes con un mismo DSCP que cruzan un enlace en una determinada dirección.

El campo DiffServ ocupa los mismos 8 bits de la cabecera IP, del byte usado previamente por el ToS (Type of Services).

Con respecto a los bits del campo ToS, se tiene lo siguiente:

- La **RFC 791** incluye especificaciones del campo ToS donde los 3 bits de mayor orden son usados para el IP Precedente, y los otros bits son usados para el delay, fiabilidad, etc.
- La **RFC 1812** modifica el significado del campo ToS, y dice que los 5 bits de menor orden deben ser cero, quedando solo el IP Precedente como el uso de los 3 bits más significativos (mayor orden).
- La **RFC 2474** reemplaza el campo ToS con el campo DiffServ, donde los 6 bits más significativos son usados para el DSCP. Los otros 2 bits (IP ECN) son usados para control de flujo, maneja la congestión notificando que se está saturando la cola y que es necesario disminuir el tráfico.

Los valores de DSCP por defecto son:

Default DSCP: "000000" Default PHB: FIFO, Tail drop.

Analizando los diferentes PHB que son usados en DSCP:

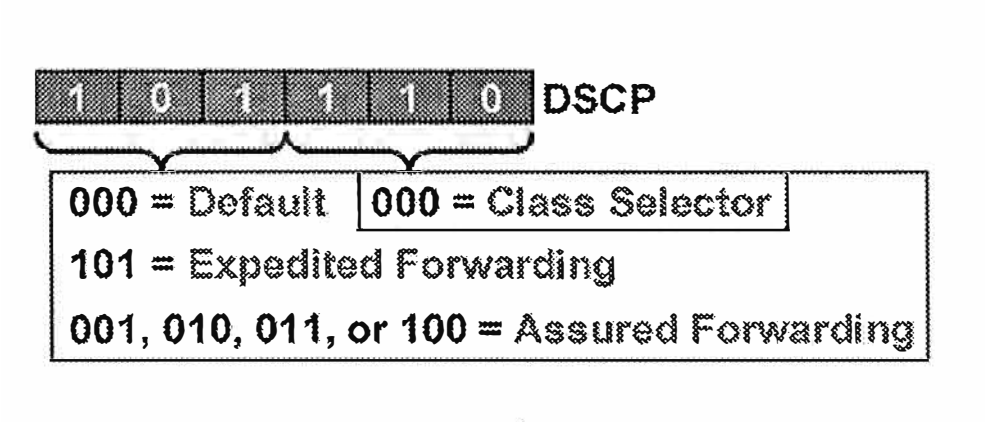


Fig. 3.2 Valores de PHB

- El Default PHB es usado por los servicios Best-Effort, donde los bits del 5 al 7 son DSCP="000".

- Expedited Forwarding (EF) PHB, es usado para servicios con bajo delay, donde los bits del 5 al 7 son: DSCP="101" (usado generalmente para voz: IP Precedente 5).
- El selector de clase (Class Selector – CS), se denomina cuando el DSCP= "xxx 000" (los 3 últimos bits del DSCP, bits del 2 al 4, son cero). El Class Selector PHB fue definido para establecer una compatibilidad de DSCP con el ToS basado en IP precedente.

CS0	000	000
CS1	001	000
CS2	010	000
CS3	011	000
CS4	100	000
CS5	101	000
CS6	110	000
CS7	111	000

Fig. 3.3 Class Selector

- Assured Forwarding (AF) PHB, es usado por servicios de BW garantizados, donde los bits del 5 al 7 son: DSCP="001", "010", "011" ó "100". Los paquetes que requieren AF PHB deben ser marcados con DSCP = "aaadd0", donde "aaa" indica el número de clase; y el "dd" indica la probabilidad de dropeo.

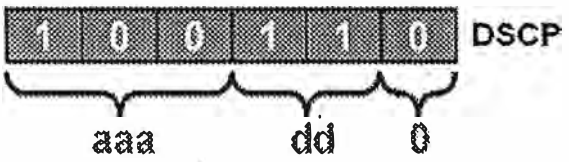


Fig. 3.4 Formato del AF

Según lo mencionado, se tiene 4 clases: AF1, AF2, AF3 y AF4 (según el valor de "aaa")

CLASE	VALOR
AF1	001 dd 0
AF2	010 dd 0
AF3	011 dd 0
AF4	100 dd 0

Fig. 3.5 Clases de AF

Analizando la clase AF1, los valores de Probabilidad de Dropeo ("dd") son:

Probabilidad de Dropeo (dd)	Valor	Valor de AF
Baja	01	AF11
Media	10	AF12
Alta	11	AF13

Fig. 3.6 Análisis de la Probabilidad de Dropeo

Por lo tanto, cada clase AF tiene 3 valores de DSCP.

3.2 Mecanismos para implementar QoS

Los principales mecanismos para implementar QoS en una red, son:

- Clasificación y Marcado.
- Administración de Congestión.
- Evitar Congestión.
- Policing y Shaping.
- Eficiencia de Enlace (Link Efficiency).

3.2.1 Clasificación

Clasificación consiste en identificar un grupo de paquetes que recibirán un servicio particular y dividir el tráfico en clases predefinidas. Esto se logra a partir de capa 2 hacia arriba. Actualmente, se debe tener mas criterio para clasificar que para marcar, y puede variar en diferentes puntos, por ejemplo ACL (listas de acceso), dirección de destino (destination address), dirección de origen (source address) DSCP, etc. La clasificación por DSCP se realiza en el CORE.

Cuando un dispositivo final, tal como un Workstation (estación de trabajo) o un teléfono IP, marca un paquete con CoS o DSCP, un switch o router tiene la opción de aceptar o no el valor de marcado que proviene de aquel dispositivo final.

Si el switch o router elige aceptar el valor marcado, entonces confiará en aquel dispositivo final y no será necesario reclasificar el paquete que venga por la interface del equipo.

Si el switch o router elige no confiar en el dispositivo final, tendrá que reclasificar con un valor de QoS apropiado a los paquetes que vengan por esa interface.

Generalmente los switches y routers están configurados para no confiar en los dispositivos finales, por lo que deben reclasificar los paquetes que provienen por la interface de dicho equipo.

En la siguiente figura, se puede apreciar cuando un dispositivo final (PC o Teléfono IP) envía paquetes al router, El router elige no confiar en el marcado del dispositivo final y reclasifica los paquetes según su prioridad (voz, datos críticos, transacciones) en la interface de entrada:

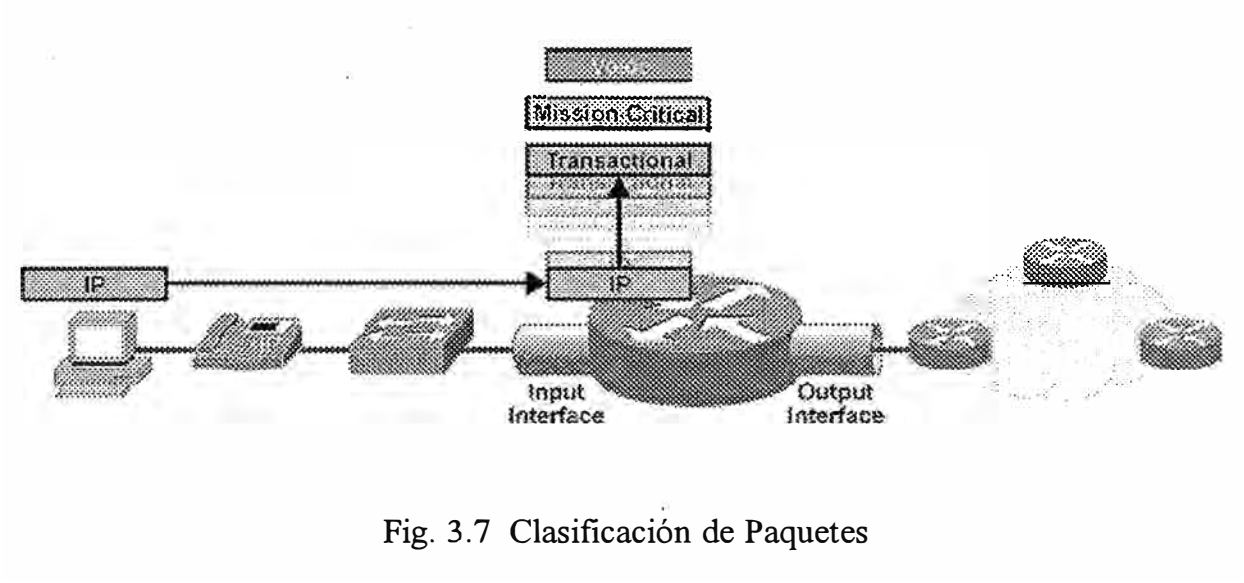


Fig. 3.7 Clasificación de Paquetes

3.2.2 Marcado

El marcado, también conocido como "colorear o pintar el paquete", involucra cada paquete marcado como un miembro de una clase de red de manera que el resto de los dispositivos a través de la red, puedan rápidamente reconocer al paquete y que clase pertenece.

El marcado es realizado lo más cerca posible al borde de la red y generalmente se usa el MQC (Modular QoS CLI), que no es más que usar módulos a través de comandos de líneas.

El marcado se puede hacer en capa 2 o 3 (FR DE, ATM CLP, 802.1 p/q, IP DSCP, IP Precedente, campo experimental MPLS)

- DE (Discard Elegible): bit usado en la trama Frame Relay, que indica que cuando el paquete viene marcado de ésta forma, es de menor prioridad.
- CLP (Cell loss priority): bit usado en celdas ATM el cual indica:

- CLP = 0 Alta prioridad
- CLP = 1 Baja prioridad

Si tenemos paquetes de voz, éstos son marcados con alta prioridad, de manera que generalmente nunca serán dropeados por el mecanismo de "Evitar Congestión" y tendrán automáticamente un orden preferencial en el mecanismo de encolamiento "Administración de Congestión".

Si tenemos paquetes de transferencia de archivos, éstos serán marcados con baja prioridad, por lo que serán dropeados cuando ocurra la congestión y generalmente movidos al final de la cola por el mecanismo de "Administración de Congestión".

En la siguiente figura, podemos observar como los paquetes de Voz, Datos Críticos y de transacciones de datos, son clasificados por el router, para luego ser marcados o coloreados con una respectiva prioridad, lo cual permitirá que los paquetes sean reconocidos con facilidad a que clase pertenecen cuando atraviesen el resto de dispositivos en la red.

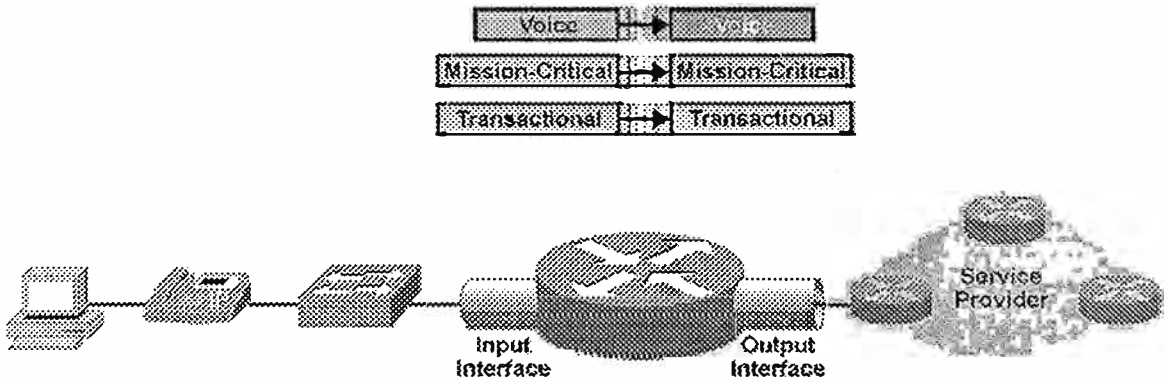


Fig. 3.8 Marcado de Paquetes

Clasificación y Marcado del Tráfico (usando Campo Experimental MPLS)

Cuando un cliente transmite paquetes IP de un sitio a otro, el campo IP Precedente (los 3 primeros bits del campo DSCP en la cabecera de un paquete) especifican la CoS. Basado en el marcado IP Precedente, los paquetes recibirán el trato deseado, así como el BW garantizado o latencia.

Cuando la red del proveedor de servicio es MPLS, el IP Precedence es copiado en el campo experimental MPLS (EXP) en el borde de la red. Ésta tarea es realizada por defecto (default) por el software IOS del equipo CISCO.

El campo EXP permite al proveedor de servicio (service provider) brindar QoS sin tener que sobrescribir un valor en el campo IP precedente del paquete del cliente. El marcado del paquete IP no es cambiado y se mantiene a través de todo el viaje por el resto de la red.

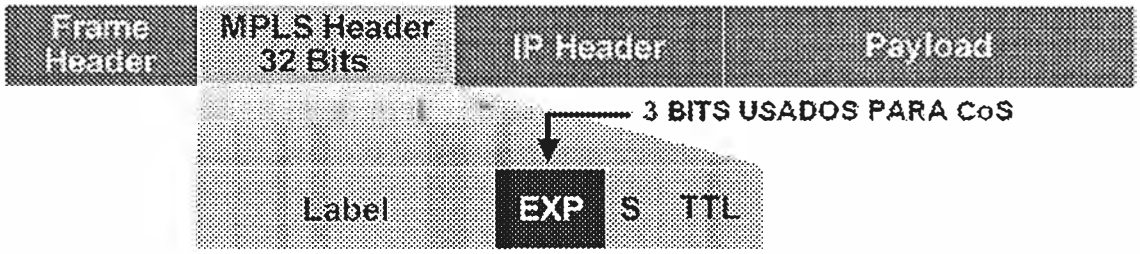


Fig. 3.9 Campo Experimental MPLS (EXP)

Según las combinaciones posibles del campo EXP, puede soportar hasta 8 clases de servicio:

Fig. 3.10 Combinaciones del Campo EXP

3.2.3 Administración de Congestión

Usa el marcado en cada paquete para determinar en que lugar de la cola será posicionado dicho paquete. Las colas con paquetes de mayor prioridad, recibirán un trato preferencial.

La Administración de Congestión es implementada en las interfaces de salidas de los dispositivos de red, usando mecanismos de colas para manejar el flujo de tráfico de salida.

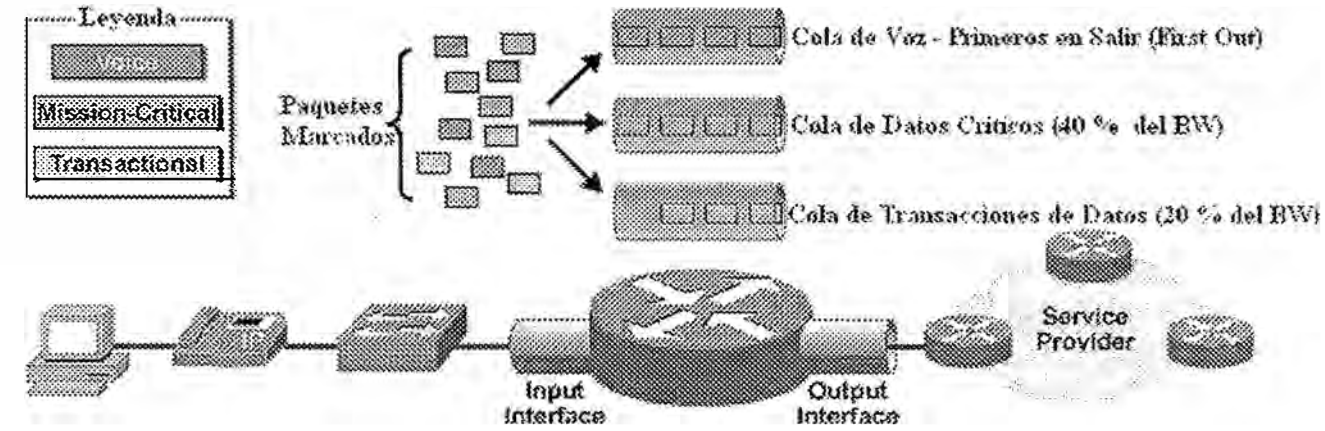


Fig. 3.11 Manejo de la Congestión de Tráfico en un Router

El software CISCO IOS (sistema operativo de los routers y switches CISCO), para la administración de congestión o encolamiento, incluye lo siguiente:

- FIFO, encolamiento por prioridad (PQ – priority queuing), encolamiento personalizado (CQ – custom queunig).
- Encolamiento justo por peso (WFQ – Weighted Fair Queuing)
- Encolamiento justo basado en clases por peso (CBWFQ – Class-Based Weighted Fair Queuing)
- Encolamiento de baja latencia (LLQ – Low-latency queuing)

Actualmente, LLQ es el método de encolamiento más usado. El LLQ es un método híbrido entre PQ y CBWFQ, el cual fue desarrollado específicamente para los requerimientos de tráfico a tiempo real, tal como la VOZ.

3.2.4 Evitar Congestión

Es un mecanismo de monitoreo de carga de tráfico en la red, el cual trata de anticipar y evitar la congestión, evitando así los llamados cuellos de botella. Ésta mecanismo se logra a través del dropeo de paquetes.

El dropeo de paquetes puede hacerse aleatoriamente de las clases seleccionadas, antes de que alcance los límites definidos en cada cola. Éste dropeo que se hace tempranamente, ayuda a prevenir los cuellos de botella en los flujos de tráfico de la red.

El mecanismo de Evitar Congestión, generalmente es implementado en las interfaces de salida de los dispositivos de red, con lo cual se asegura de que la WAN no se vea instantáneamente congestionada por el flujo de tráfico que proviene de la LAN.

El WRED es una de las técnicas principales de CISCO para evitar la congestión. WRED incrementa la probabilidad de evitar la congestión a través del dropeo de paquetes de baja prioridad. WRED no es recomendado en las colas de voz, es por eso que ninguna red debe ser diseñada para dropear los paquetes de voz.

En la siguiente figura se puede observar como los paquetes marcados (no los paquetes de voz, alta prioridad) son dropeados en las colas de manera aleatoria a fin de evitar la congestión en dichas colas, es decir, evitar los cuellos de botella:

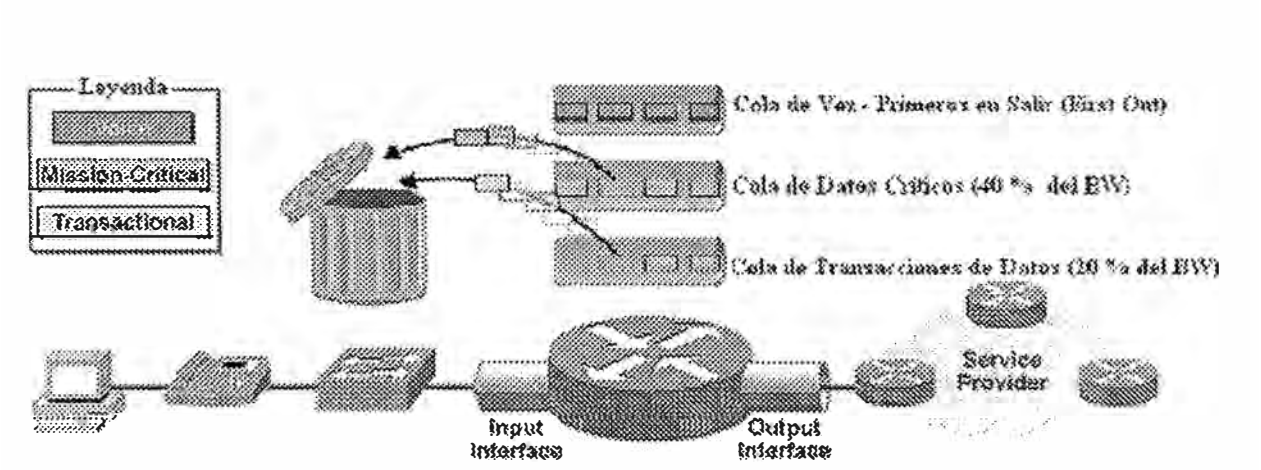


Fig. 3.12 Dropeo de paquetes aleatoriamente para evitar congestión

3.2.5 Policing and Shaping

El Policing o Shaping son mecanismos que a menudo son usados para condicionar el tráfico antes de transmitir el tráfico a una red o recibir el tráfico de una red. Ambas técnicas consisten en clasificar, medir y marcar el tráfico para ver si se dropea o no el paquete.

Policing

El Policing dropea o marca paquetes cuando los límites de BW en una cola son alcanzados. El mecanismo de Policing puede ser configurado para que primero se dropee aquella clase de tráfico que vienen marcado con menor prioridad de QoS.

El Policing puede ser usado en la entrada o salida de una interface. Este mecanismo generalmente se usa para controlar el flujo en un dispositivo de red con enlaces de alta velocidad. En un ambiente TCP, el policing podría causar que el equipo que envía el tráfico baje su flujo de transmisión de paquetes. Este mecanismo usa policing basado en clases y CAR (committed access rate).

En la siguiente figura, se tiene unas clases configuradas para aceptar un cierto límite de BW en sus colas respectivas:

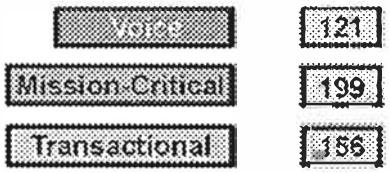


Fig. 3.13 Asignación de ancho de banda por cola

donde la cola de datos críticos está configurado para aceptar como máximo 200Kbps y se encuentra en 199 Kbps, luego viene un paquete IP y llega a alcanzar el límite establecido. A partir de éste momento, todo paquete que llegue será dropeado:

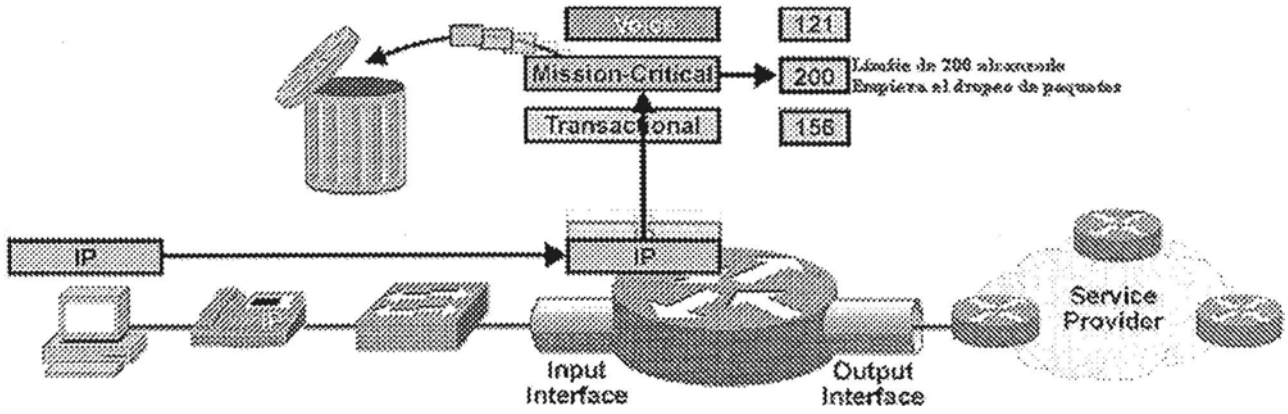
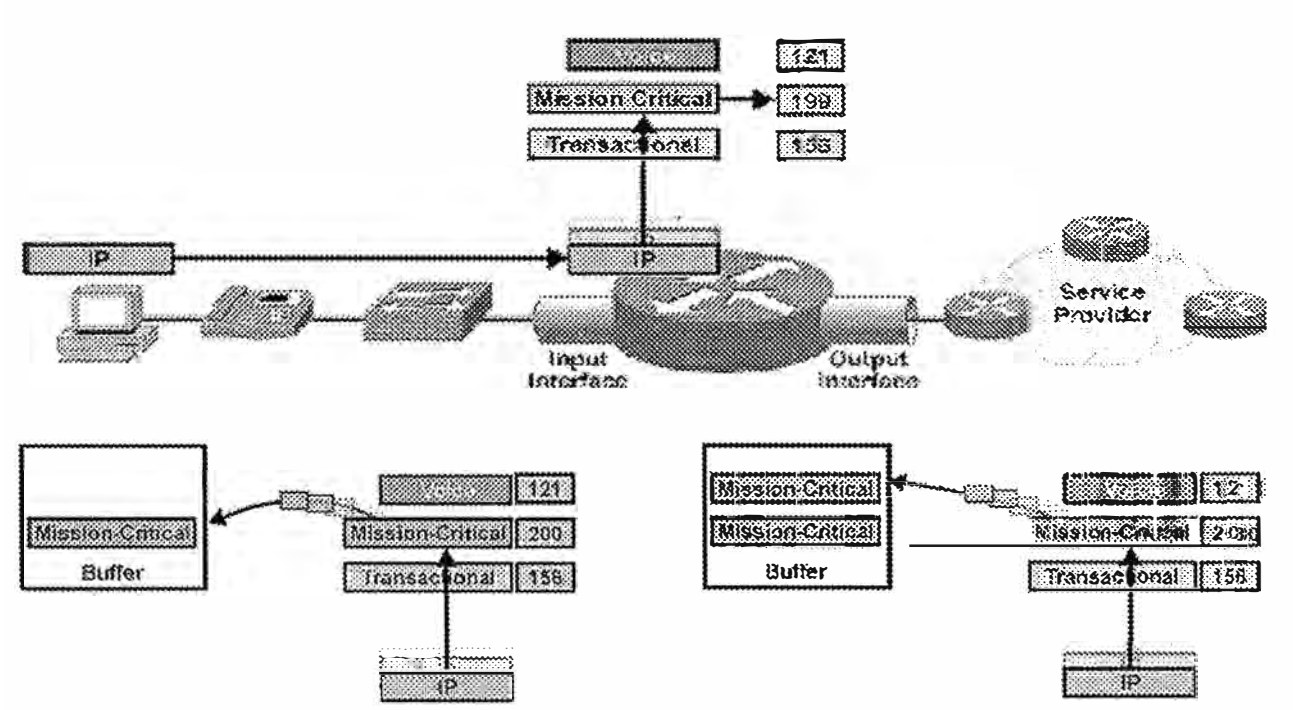


Fig. 3.14 Dropeo de paquetes luego de alcanzar el límite de BW definido

Shaping

Es un mecanismo usado en las salidas de las interfaces, típicamente usado para limitar el flujo de un enlace de alta velocidad a un enlace de baja velocidad, y así asegurar que el enlace de baja velocidad no desborde tráfico. También se usa para manejar el flujo en un punto de la red donde múltiples flujos son agregados. A diferencia del Policing, el Shaping no dropea paquetes tan drásticamente, lo que hace es: una vez alcanzado el límite establecido en las colas, los paquetes que siguen llegando son almacenados en un buffer para luego ser enviados cuando baje el flujo de tráfico, de ésta manera se evita de que se pierdan paquetes. En la siguiente figura, sea las mismas condiciones iniciales (datos críticos configurados a un tope de 200k y se encuentra en 199K), llega un paquete y alcanza el límite establecido en la cola. A partir de acá empieza la buferización de paquetes:



Límite de 200 alcanzado, los paquetes que llegan son enviados a un BUFFER

Fig. 3.15 Almacenamiento de paquetes luego de alcanzar el BW definido

Luego, cuando el tráfico de la cola baja o disminuye de su límite establecido, los paquetes en el buffer son retransmitido a la cola para ser enviados a su siguiente salto:

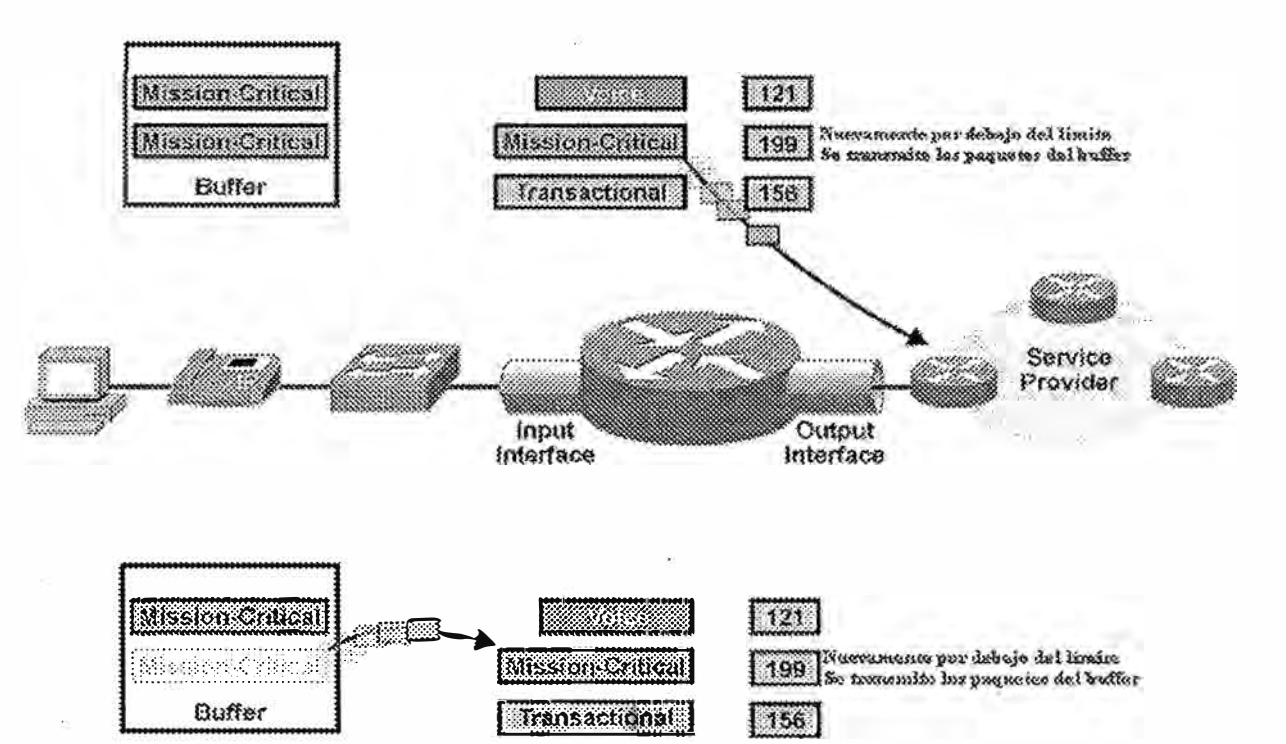


Fig. 3.16 Retransmisión de paquetes almacenados en el buffer

3.2.6 Eficiencia de enlace (Link Efficiency)

Éste mecanismo es usado para mejorar la eficiencia del ancho de banda a través de la compresión y LFI (Link Fragmentation and Interleaving).

Compresión

El software Cisco IOS QoS ofrece mecanismos de eficiencia de enlaces que trabajan en conjunto con las colas y "traffic shaping", para manejar el BW existente de manera mas eficiente y predecible. Uno de estos mecanismos es la compresión del Protocolo de Transporte a Tiempo Real (cRTP – compressed Real-Time Transport Protocol)

Un paquete de voz lleva un payload de 20 bytes, por ejemplo, normalmente lleva 20 bytes de cabecera IP, 8 byte de cabecera UDP (User Datagram Protocol), y 12 bytes de cabecera RTP, lo que hace un total de 40 bytes. Éstos 40 bytes pueden ser comprimidos a 2 o 4 bytes, dependiendo de si el CRC (cyclic redundancy check) es transmitido o no.

La compresión puede dramáticamente mejorar la performancia del enlace. La compresión típicamente se usa en los enlaces WAN de los routers para mejorar la

eficiencia del BW y es una técnica aplicada de host a host, por lo que es necesario habilitarlo en cada enlace (no es end to end).

Éste mecanismo nos permite poner más paquetes en la cola; pero el proceso de compresión también nos puede tomar un tiempo (delay). Se recomienda realizar éste mecanismo cuando la relación de cabecera a carga (header a payload) es de 3:2 ó 2:1

En la siguiente figura se muestra lo anteriormente explicado:

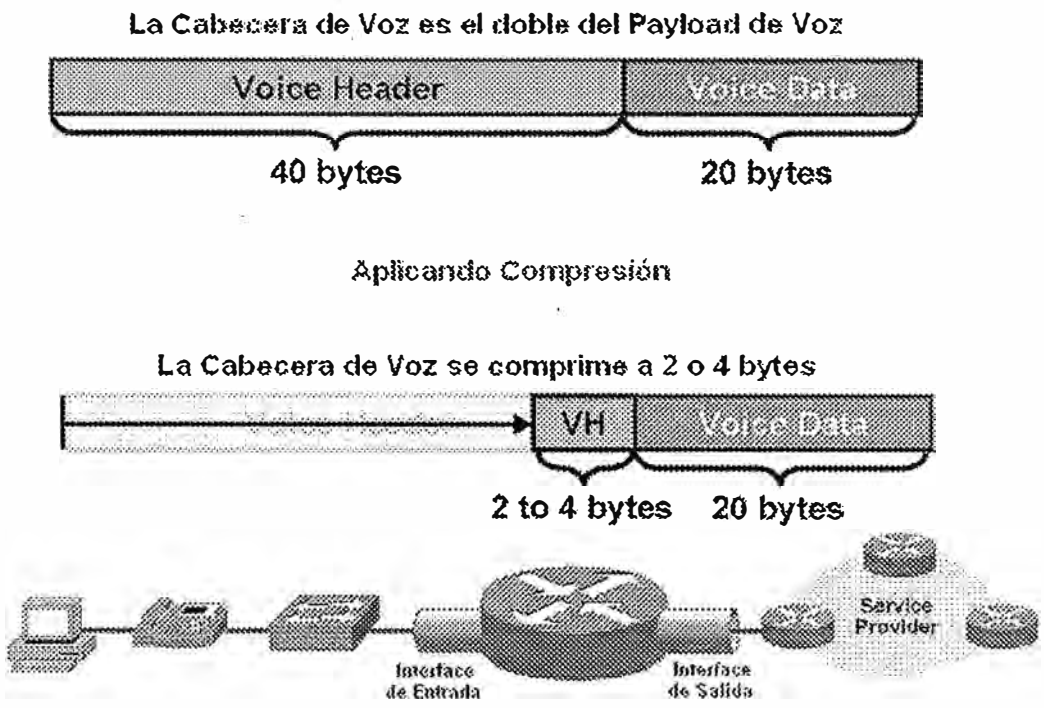


Fig. 3.17 Compresión de la Cabecera de Voz

LFI (Link Fragmentation and Interleaving)

Sin éste mecanismo, los paquetes pequeños de voz pueden ser ubicados detrás de los paquetes grandes de datos, incrementando el delay en el tráfico de voz. Para esto, se fragmenta los paquetes grandes de datos en paquetes mas pequeños, para así poder ser ubicados de manera casi intercalada los paquetes de voz y datos, conservando la premisa de que los paquetes de mayor prioridad generalmente van primero ante los paquetes de menor prioridad.

Éste mecanismo es implementado solo en interfaces seriales.

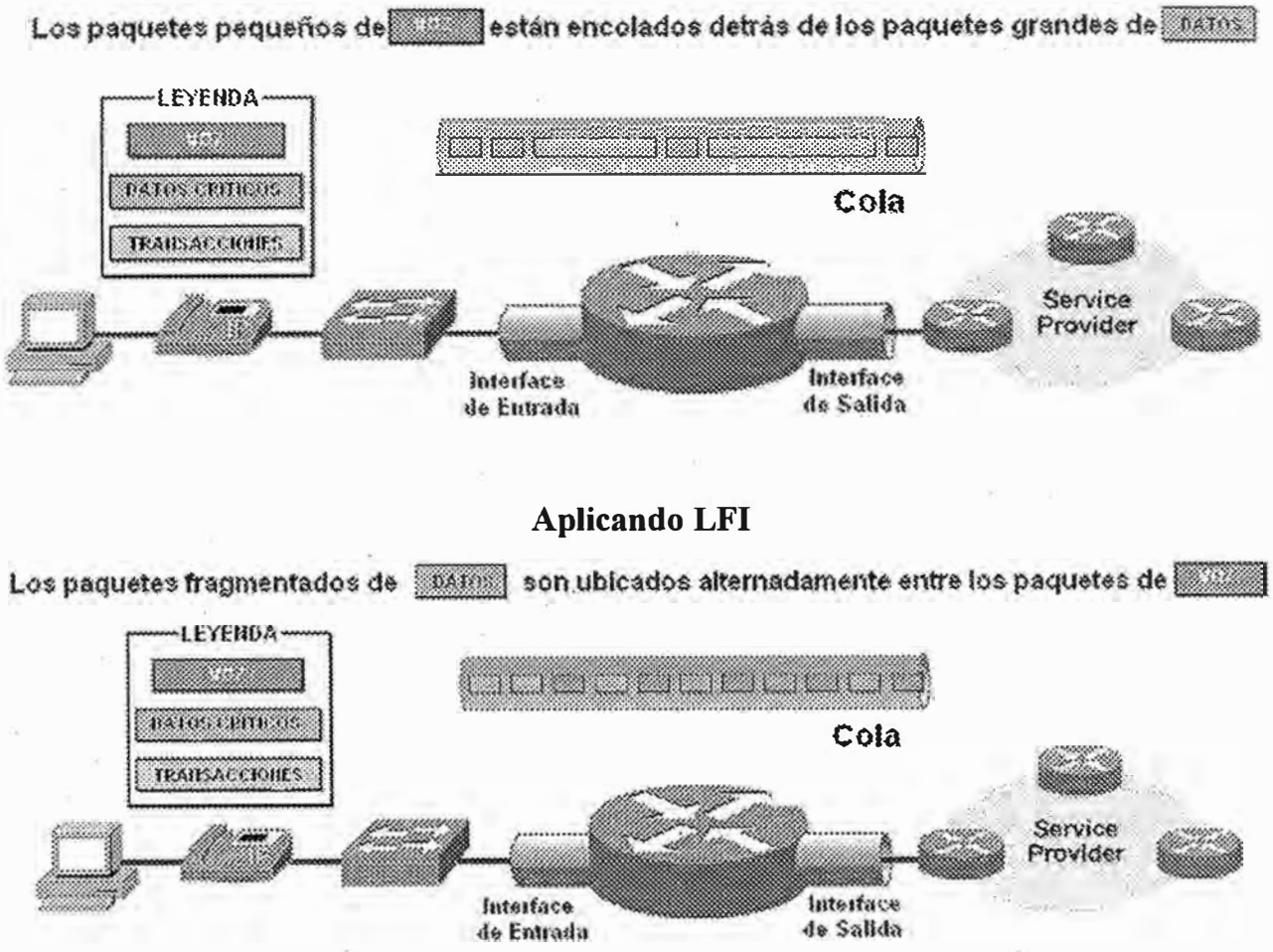


Fig. 3.18 Fragmentación de paquetes y ubicación alternada en la cola de tráfico

CAPITULO IV

4.1 Comandos de Interface de Línea para el QoS Modular (MQC – Modular QoS CLI)

El MQC fue creado para permitir cualquier clasificación a ser usado con cualquier mecanismo de QoS. Un beneficio importante del MQC es la reutilización de configuración. El MQC permite aplicar la misma política de QoS en múltiples interfaces.

Para implementar QoS usando MQC, se recomienda los siguientes pasos:

- Configurar la Clasificación usando el comando **class-map**.
- Configurar políticas de tráfico asociando clases de tráfico con una o mas características de QoS usando el comando **policy-map**.
- Amarrar las políticas de tráfico a la entrada o salida de una interface, subinterface o circuito virtual, usando el comando **service-policy**.

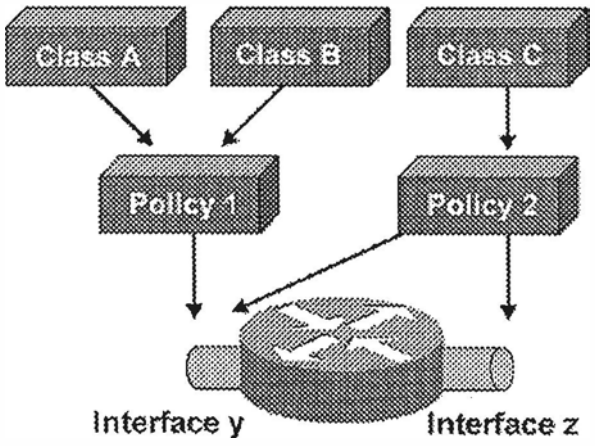


Fig. 4.1 Estructura del MQC

4.1.1 Class Map

Los Class Map son usados para crear plantillas de clasificación que se usarán mas adelante en los Policy Map. Los router pueden ser configurados con un gran número de class map's (actualmente soporta hasta 256).

Un class map es creado usando el comando de configuración global class-map. Cada class map contiene una o más condiciones que determinas si el paquete pertenece a la clase.

Existe 2 formas de procesar las condiciones, cuando hay mas de una condición en un class map:

- **Match all**: Todas las condiciones se deben cumplir para ligar o asociar un paquete a la clase.
- **Match any**: Al menos una condición debe cumplirse para ligar o asociar un paquete a la clase.

Por defecto, el class map está en la condición de **match all**.

Clasificación usando Class Maps

La siguiente figura, ilustra el proceso de determinación si un paquete pertenece a una clase (match) o no (no match).

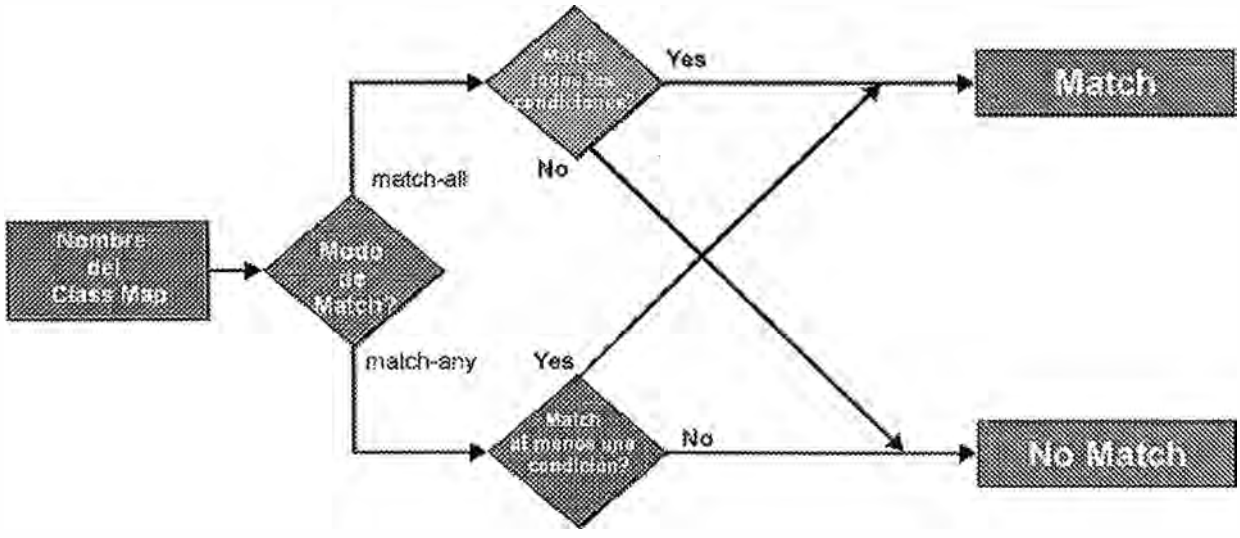


Fig. 4.2 Diagrama de flujo del Class Map

- **Match all** requiere que se cumplan todas la condiciones para dar una respuesta positiva. Si una condición no es conocida, el class map dará "no match" como resultado.
- **Match any** requiere que se cumpla al menos una condición para dar una respuesta positiva. Si ninguna condición es conocida, el class map dará "no match" como resultado.

La sintaxis al usar class-map, es:

router(config)#

class-map [match-all | match-any] *class-map-name*

- Se ingresa al modo de configuración class-map.
- Se especifica la estrategia de matching.

router(config-cmap)#

match *condition*

- Usar al menos una condición para el matching de paquetes.

router(config-cmap)#

match class-map *class-map-name*

- Un class map puede usar otro class map para la clasificación de paquetes.
- El anidado de class map permite la generación de plantillas de class maps para ser usados en otros class maps.

4.1.2 Policy Map

El comando policy-map es usado para crear una política de tráfico. El propósito de una política de tráfico es configurar las características de QoS que deberían estar asociadas con el tráfico que viene siendo clasificado en una clase de tráfico específico.

Pueden estar asociados hasta 256 clases de tráfico con una única política de tráfico. También, múltiples policy maps, pueden estar anidados para influenciar en la secuencia de las acciones de la QoS.

La sintaxis al usar policy map, es:

router(config)#

policy-map *policy-map-name*

- Se ingresa al modo de configuración policy-map
- Los policy-map's son identificados por un nombre.

router(config-pmap)#
class {*class-name* | class-default}

- Se ingresa al modo de configuración por clase usando el nombre del class-map previamente definido.
- Se usa el nombre "class-default" para configurar la política de la clase por defecto.

router(config-pmap)#
class *class-map-name condition*

- Opcionalmente, se puede definir un nuevo class map ingresando la condición después del nombre del nuevo class map.
- Usa la estrategia del "match-any".

4.1.3 Service Policy

Las políticas de servicio (service policy) son usados para adjuntar las políticas de tráfico configurados con un policy map, a una interface determinada. Los service policies pueden ser aplicados a una interface para el ingreso o salida de paquetes.

Usando el comando **service-policy**, se puede asignar un único policy map a múltiples interfaces o asignar múltiples policy maps a una única interface (un máximo de un service policy en cada dirección, es decir, entrada y salida).

La sintaxis del service policy, es:
router(config-map-class)#
service-policy *policy-map-name*

Se adjunta los policy map de servicio específicos para entrada o salida de una interface.

Los routers verifican inmediatamente que los parámetros a usarse en el policy map, sean los correctos. Si existe un error en la configuración del policy map, el router mostrará un mensaje explicando cual es el error con el policy map.

4.2 Consideraciones para aplicar QoS en equipos CISCO sobre una red MPLS

En la red MPLS, se ha considerado 3 tipos de tráfico, los que se muestran a continuación:

- **Prioridad 1 (P1)**: Aplicaciones que no necesita altas exigencias de retardo tales como http, mail, ftp, etc.
- **Prioridad 2 (P2)**: Aplicaciones sensibles al retardo (delay) y/o críticas para el negocio, como por ejemplo: Oracle, SAP, SNA, etc.
- **Prioridad 3 (P5)**: Aplicaciones en tiempo real que exijan una baja variación de delay (jitter), como por ejemplo: Multimedia, VoIP, Video Conferencia, Telefonía IP, etc.

Para el caso de Prioridad 3 (P5), se considera **precedencia 5** o **dscp cs5** en la Calidad de Servicio.

4.3 Clasificación de Tráfico

La clasificación de paquetes se realiza usando los bits de DSCP (6 bits) o los de ToS - Tipo de Servicio (3 bits), estos últimos son mapeados en los primeros por compatibilidad. En la siguiente tabla (Tabla 4.1) se resume el uso de DSCP para la clasificación del tráfico de red en clases de servicios:

Clase de Servicio	Tráfico	IP Precedence (3 Bits)	IP DSCP (6 Bits)	IP ToS (8 Bits)
CoS 3	Voz / Video	5 (101)	40 (101000)	160 (10100000)
CoS 2	Datos Críticos	2 (010)	16 (010000)	64 (01000000)
CoS 1	Datos / Transacciones	1 (001)	8 (001000)	32 (00100000)

Tabla 4.1 Valores de DSCP según la Clase de Servicio

A continuación, se muestra una tabla (Tabla 4.2) donde se detalla la prioridad, ancho de banda y aplicaciones para cada QoS, que se viene usando en las grandes empresas de Telecomunicaciones:

	QoS5	QoS2	QoS1
PRIORIDAD	MAXIMA	MEDIA	NORMAL
TIPO DE DATOS	VOZ Y VIDEO	DATOS CRITICOS	APLICACIONES NO CRITICAS
ANCHO DE BANDA MAXIMO POR PUERTO	50%	75%	75%
APLICACIONES	Aplicaciones en Tiempo Real así como aplicaciones que exigen baja diferencia de delay (jitter)	Aplicaciones sensibles al retardo (delay) y/o críticas para el negocio.	Datos sin altas exigencias de retardo.
	Multimedia, Voz sobre IP, video conferencia.	Oracle, SAP, ERP, etc.	Correo electrónico, chat, FTP, etc.

Tabla 4.2 Porcentaje de BW, prioridad y aplicaciones según el QoS

A continuación se definirán algunas Listas de Accesos necesarias para la aplicación de la QoS:

4.4 Listas de Acceso en Sede Principal y Remota

A continuación, se muestra Tabla 4.3 donde se menciona las listas de acceso que son consideradas en la Sede Principal y Remota:

Comando	Propósito
ip access-list extended qos5MPLS	Creación de la lista de acceso **qos5MPLS**
permit ip < Redes Telefonia IP > any	Tráfico Telefonía IP
permit ip < Loopback de Voz > any	Tráfico VoIP
permit ip < Red VideoConferencia > any	Tráfico VideoConferencia
ip access-list extended qos2MPLS	Creación de la lista de acceso **qos2MPLS**
permit ip < Redes que necesitan reservación de BW > any	Aplicativos de prioridad 2 que necesitan reservación de BW (Tráfico crítico)

Tabla 4.3 Listas de Acceso en los CPE's

4.5 Configuración de las Interfaces VoIP

A continuación se muestra la Tablas 4.4 donde se detalla las configuraciones de las Interfaces de VoIP:

Comando	Propósito
dial-peer voice [# interface] voip	Interface VoIP (Llamadas externas)
destination-pattern [# Teléfono]	[# Teléfono], Número Anexo ó Telefónico destino
session target Ipv4:[# IP destino]	[# IP destino], IP del router destino
codec g729r8 [# bytes]	[# bytes], Tamaño del paquete usado en el paquete de Voz
ip precedence 5	Marcado de paquetes VoIP con precedencia 5 (solo para IOS 12.2.x)
ip qos dscp cs5 media	Marcado de paquetes VoIP con precedencia 5 (solo para IOS 12.2.xT o superior)
ip qos dscp cs5 signalling	Marcado de paquetes de sañalización VoIP con precedencia 5 (solo para IOS 12.2.xT o superior)
no vad	Se habilita la no detección de voz

Comando	Propósito
dial-peer voice [# interface] pots	Interface pots (Llamadas Locales)
destination-pattern [# Teléfono]	[# Teléfono], Número Anexo ó Telefónico destino
port [# Puerto de Voz]	[# Puerto de Voz], con respecto a las interfaces FXS, FXO, E1

Comando	Propósito
dial-peer voice [# interface] voip	Interface VoIP (Llamadas locales)
incoming called-number [# Teléfono]	[# Teléfono], Número Anexo ó Telefónico de los pots (solo se configura una sola vez)
codec g729r8 [# bytes]	[# bytes], Tamaño del paquete usado en el paquete de Voz
ip precedence 5	Marcado de paquetes VoIP con precedencia 5 (solo para IOS 12.2.x)
ip qos dscp cs5 media	Marcado de paquetes VoIP con precedencia 5 (solo para IOS 12.2.xT o superior)
ip qos dscp cs5 signalling	Marcado de paquetes de sañalización VoIP con precedencia 5 (solo para IOS 12.2.xT o superior)
no vad	Se habilita la no detección de voz

Tabla 4.4 Configuración de las Interfaces de Voz sobre IP

4.6 Configuración de Políticas de Calidad

4.6.1 Definición de las clases de tráfico para el marcado de paquetes (Sede Principal y Remotas)

Para el marcado de paquetes, se debe definir las siguientes clases según lo servicios vendidos al cliente, lo cual se puede apreciar en la Tabla 4.5:

Comando	Propósito
class-map match-any P5	**Class Map: P5**, identifica tráfico tipo QoS5
match ip dscp cs5	Reconoce tráfico que venga marcado como QoS5 desde la LAN del cliente.
match access-group name qos5MPLS	Se aplica lista de acceso qos5MPLS para marcar tráfico tipo QoS5
class-map match-any P2	**Class Map: P2**, identifica tráfico tipo QoS2
match ip dscp cs2	Reconoce tráfico que venga marcado como QoS2 desde la LAN del cliente.
match access-group name qos2MPLS	Se aplica lista de acceso qos2MPLS para marcar tráfico tipo QoS2

Tabla 4.5 Clases de tráfico para el marcado de paquetes

4.6.2 Definición de las clases de tráfico para los equipos en Sede Principal y Remotas

Se definen las clases genéricas para la configuración de las clases de tráfico, por ejemplo si se desea configurar solo QoS para VoIP, se considerará solo la configuración relacionado a la VoIP. A continuación se muestra las Tabla 4.6 y Tabla 4.7, donde se observa las clases de tráfico cuando se realiza o no, un marcado de paquete general en la red del cliente:

Caso 1: No se realiza un Marcado de Paquetes General en la Red del Cliente:

Comando	Propósito
class-map match-any qos5MPLS	**Class Map: qos5MPLS**, identifica tráfico hacia la nube MPLS con QoS5
match access-group name qos5MPLS	Identifica al tráfico tipo QoS5, sensible al retardo.
class-map match-any qos2MPLS	**Class Map: qos2MPLS**, identifica tráfico hacia la nube MPLS con QoS2
match access-group name qos2MPLS	Identifica al tráfico tipo QoS2, que necesita reservación de BW.

Tabla 4.6 Clase de tráfico sin marcado de paquete general

Caso 2: Se realiza un Marcado de Paquetes General en la Red del Cliente:

Comando	Propósito
class-map match-any qos5	**Class Map**: **qos5**, identifica tráfico tipo QoS5
match ip dscp cs5	Con marcado de paquetes general en la red del cliente, ya no es necesario hacer referencia a las listas de acceso, sino solamente a la precedencia del paquete
class-map match-any qos2	**Class Map**: **qos2**, identifica tráfico tipo QoS2
match ip dscp cs2	Con marcado de paquetes general en la red del cliente, ya no es necesario hacer referencia a las listas de acceso, sino solamente a la precedencia del paquete
class-map match-any qos1	**Class Map**: **qos1**, identifica tráfico tipo QoS1
match ip dscp cs1	Con marcado de paquetes general en la red del cliente, ya no es necesario hacer referencia a las listas de acceso, sino solamente a la precedencia del paquete

Tabla 4.7 Clases de tráfico con marcado de paquete general

4.6.3 Definición policy-map para el marcado de paquetes en routers de Sede Principal y Remotas

Se muestra la definición de los policy-map para el marcado de paquetes en los CPE's, cuando la interface LAN del cliente maneja varios tipos de tráfico (Tabla 4.8) y cuando la interface LAN del cliente maneja el concepto de VLAN's (Tabla 4.9) donde cada VLAN hace referencia a un solo tipo de tráfico:

Caso 1: Interfaces LAN manejan distintos tráficos LAN del cliente

Comando	Propósito
policy-map SetDscpLan	**Política: SetDscpLan, política de marcado de paquetes**
class P5	Clase P5, identifica el tráfico tipo QoS5
set ip dscp cs5	Marca los paquetes con precedencia cs5
class P2	Clase P2, identifica el tráfico tipo QoS2
set ip dscp cs2	Marca los paquetes con precedencia cs2
class class-default	Clase class-default, identifica cualquier tipo de tráfico como QoS1.
set ip dscp cs1	Marca los paquetes con precedencia cs1

Tabla 4.8 Policy-map con varios tipos de tráfico en la LAN

Caso 2: Interfaces LAN que manejan un solo tipo de tráfico LAN del cliente (aplicación de VALN's)

En éste caso, ya no es necesaria la configuración de listas de acceso para clasificar las redes de acuerdo al QoS establecido. Cada policy-map será aplicado en cada sub-interface lógica de la LAN (mas adelante se verá un ejemplo de configuración).

Comando	Propósito
policy-map SetLanQosX	**Política: SetLanQoSX, política de marcado de paquetes**
class class-default	Clase class-default, identifica cualquier tipo de tráfico.
set ip dscp csX	Marca los paquetes según la precedencia a utilizar, X=1,2 ó 5.

Tabla 4.9 Policy-map cuando se tiene VLAN's

4.6.4 Definición de policy-map para el tráfico hacia la red MPLS

En las siguientes tablas (Tabla 4.10, 4.11 y 4.12) se muestran los policy-map para el tráfico hacia la red MPLS, según el tipo de tráfico con o sin marcado de paquetes previo en la LAN.

Caso 1: Definición de policy-map para tipo de tráfico QoS5

Comando	Propósito
policy-map wan-MPLS	**Política: wan-MPLS**, política que hace referencia al tráfico QoS5
class qos5MPLS	Clase qos5MPLS, identifica el tráfico tipo QoS5
priority [BW5]	[BW5], Bw a priorizar para el tráfico QoS5
police 8000 1500 1500 conform-action set-prec-transmit 5 exceed-action set-prec-transmit 5	Se marcan los paquetes que ingresan a la red MPLS con precedencia 5.
class class-default	Clase class-default, identifica cualquier tipo de tráfico.
fair-queue	

Tabla 4.10 Policy-map para QoS5, sin marcado de paquetes en la LAN

Caso 2: Definición de policy-map para tipo de tráfico QoS5, QoS2 y QoS1

Comando	Propósito
policy-map wan-MPLS	**Política: wan-MPLS**, política que hace referencia al tráfico QoS5, QoS2 y QoS1.
class qos5MPLS	Clase qos5MPLS, identifica el tráfico tipo QoS5
priority [BW5]	[BW5], Bw a priorizar para el tráfico QoS5
police 8000 1500 1500 conform-action set-prec-transmit 5 exceed-action set-prec-transmit 5	Se marcan los paquetes que ingresan a la red MPLS con precedencia 5.
class qos2MPLS	Clase qos2MPLS, identifica el tráfico tipo QoS2
bandwidth [BW2]	[BW2], BW a priorizar para el tráfico QoS2
police 8000 1500 1500 conform-action set-prec-transmit 2 exceed-action set-prec-transmit 2	Se marcan los paquetes que ingresan a la red MPLS con precedencia 2.
class class-default	Clase class-default, identifica cualquier tipo de tráfico.
bandwidth [BW1]	[BW1], asegura el BW1 para cualquier tipo de tráfico.
police 8000 1500 1500 conform-action set-prec-transmit 1. exceed-action set-prec-transmit 1	Se marcan los paquetes que ingresan a la red MPLS con precedencia 1.
	La suma de **BW1 + Bw2 + BW5** debe ser el BW Total vendido al cliente.

Tabla 4.11 Policy-map para QoS5, QoS2 y QoS1, sin marcado de paquetes en la LAN

Caso 3: Definición de policy-map para tipos de tráfico QoS5, QoS2 y QoS1 en una red con Marcado de Paquetes

Comando	Propósito
policy-map wan-MPLS	**Política: wan-MPLS, política que hace referencia al tráfico QoS5, QoS2 y QoS1.**
class qos5	Clase qos5, identifica el tráfico tipo QoS5
priority [BW5]	[BW5], Bw a priorizar para el tráfico QoS5
class qos2	Clase qos2, identifica el tráfico tipo QoS2
bandwidth [BW2]	[BW2], BW a priorizar para el tráfico QoS2
class qos1	Clase qos1, identifica el tráfico tipo QoS1.
bandwidth [BW1]	[BW1], BW a priorizar para el tráfico QoS1
	La suma de BW1 + Bw2 + BW5 debe ser el BW Total vendido al cliente.

Tabla 4.12 Policy-map para QoS5, QoS2 y QoS1, con marcado de paquetes en la LAN

4.6.5 Reservación de BW para VoIP en la Red MPLS

Se considerará como CODEC el G729r8, el cual tiene un tamaño de Voice Payload de 40 bytes. Así mismo dependerá del número de llamadas (canales de voz) que cursará cada sede, para lo cual se considerará los valores de la Tabla 4.13:

Número de Llamadas	BW (Kbps)
1	**22**
2	**44**
3	**66**
N	**22*N**

Taba 4.13 Reservación de BW de acuerdo al número de llamadas

Para el caso de ToIP, la estimación del BW a considerar, se realiza de acuerdo al CODEC y del tamaño del Payload del CODEC (depende de cada cliente, según lo configurado en sus centrales).

4.6.6 Aplicación de Políticas de Marcado de paquetes en los equipos de la Sede Principal y Remotas

Éstas políticas son aplicadas en las interfaces LAN de cada equipo del cliente, según lo mostrado en la Tabla 4.14:

Comando	Propósito
interface Ethernet X/X	Interface Ethernet por donde circula todo el tráfico hacia y desde las sedes remotas
description Interface LAN	
ip addrress [IP ADDRESS] [MASK]	
load-interval 30	
full-duplex	Se recomienda que se encuentre configurado a éste modo de operación (si el equipo lo soporta)
service-policy in SetDscpLan	Comando que aplica el Marcado de Paquetes a todo tráfico que ingrese por la Interface LAN

Tabla 4.14 Aplicación de política de marcado en la LAN

4.6.7 Configuración de Políticas de QoS

En la configuración d políticas de QoS, se presentan 2 casos:

Caso 1: Definición de policy-map (WAN Ethernet, cuando cruza por la Red ATM)

Comando	Propósito
policy-map shape[BW]	Política **shape[BW]**, hace referencia al tráfico de salida desde la sede principal o remota.
class class-default	Clase class-default, identifica a todo el tráfico de salida de la sede.
shape average [BW]	Asegura el BW (max) de salida de la sede.
service-policy wan-MPLS	Política wan-MPLS, el cual define el tratamiento de tráfico de salida, donde las reservas del BW se realizan tomando en cuenta el ancho de banda máximo de dicha sede.

Tabla 4.15 Policy-map cuando se tiene una interface WAN Ethernet y va por la red ATM

Caso 2: Definición de policy-map (WAN Seriales, Red MPLS)

Cuando el acceso es Frame Relay, se tendrán parámetros que definan BW, políticas de QoS y fragmentación (Tabla 4.16):

Comando	Propósito
map-class frame-relay voipfrBW	Clase que define los parámetros del enlace con acceso frame relay
no frame-relay adaptive-shaping	
frame-relay cir CIR	Se define el CIR o el BW del circuito
frame-relay bc BC	
frame-relay be 0	
frame-relay mincir CIR	Se define el CIR mínimo que es igual al BW del enlace
service-policy output wan-MPLS	Se define la política de QoS la cual tomará como BW de referencia al valor configurado en el **CIR**
frame-relay fragment FRAG	Se define la fragmentación de los paquetes IP, con el objetivo que no exista diferencia en el tamaño de paquetes para datos y voz.

Tabla 4.16 Policy-map cuando se tiene una interface Serial

Donde los valores a considerar, según el BW, son mostrados en la Tabla 4.17:

Bandwidth - BW (Kbps)	CIR	BC	FRAG
64	61000	720	90
128	1248000	1280	128
192	188800	1920	240
256	252800	2560	320
512	508800	5120	640
1024	1020000	10200	No aplica
2048	2040000	20480	No aplica

Tabla 4.17 Parámetros en Políticas de QoS cuando se tiene interfaces seriales

4.6.8 Aplicación de las Políticas de QoS

Caso 1: Aplicación de Políticas (WAN Ethernet, cuando cruza por la Red ATM)

A continuación, se aplica la políticas de QoS en la interface WAN del CPE (Tabla 4.18), cuando se conecta a una red ATM

Comando	Propósito
interface Ethernet X/X	Interface Ethernet por donde circula todo el tráfico hacia y desde las sedes remotas
description Interface WAN	
ip address [IP ADDRESS] [MASK]	
load-interval 30	
full-duplex	Se recomienda que se encuentre configurado a éste modo de operación (si el equipo lo soporta)
service-policy output shape[BW]	Comando que aplica la política de QoS al tráfico de salida de la Interface.

Tabla 4.18 Aplicación de Política de QoS de salida en interfaces Ethernet

Caso 2: Aplicación de Políticas (WAN Seriales, Red MPLS)

En éste caso, los equipos del cliente, poseen interfaces seriales, por consiguiente no es necesario que viaje a través de la red ATM, por lo que va directo a una interface serial del equipo PE de la nube MPLS. Para esto, se creará una sub-interface lógica de la interface física serial, donde se configurará la IP Address respectiva, como se muestra en la Tabla 4.19:

Comando	Propósito
interface Serial 0/0	Interface WAN hacia la Red MPLS
description Interface WAN	
bandwidth BW	BW es el ancho de banda del enlace
no ip address	
encapsulation frame-relay IETF	Se define la encapsulación Frame Realy
load-interval 30	
frame-relay traffic-shaping	Parámetros del frame Relay
frame-relay lmi-type ansi	Parámetros del frame Relay

Comando	Propósito
interface Serial 0/0.1 point-to-point	Cuando se usa Frame Relay, se crean circuitos virtuales por donde pasa el tráfico de la sede en mención.
description Sub-Interface Virtual WAN Frame Relay	
ip address [IP ADDRESS] [MASK]	
frame-relay class voipfrBW	Se definen las características del circuito virtual (BW, QoS5 y fragmentación)
frame-relay interface-dlci 110	Cada circuito virtual tiene un identificador llamado DLCI, el cual debe ser diferente para cada servicio adicional que se le provea al cliente. Se debe asociar a una subinterface nueva por cada DLCI nuevo.

Tabla 4.19 Aplicación de Política de QoS de salida en interfaces seriales

4.6.9 Configuración Loopback VoIP

Las Loopback's, no son otras cosa que interfaces lógicas creadas para que siempre se encuentren activas. Antiguamente se empleaba la IP de la interface WAN como IP para el tráfico de voz; pero cuando cae la WAN, también caería la voz, lo que se puede evitar creando la interface lógica (loopback) y la voz cursaría por un enlace backup u otro operador.

Comando	Propósito
interface Loopback X	Interface lógica creada para que circule todo el tráfico de VoIP hacia y desde las sedes del cliente.
description Interface VoIP	
ip address [IP ADDRESS] [MASK]	
h323-gateway voip bind srcaddr [IP Address]	En caso que se utilizen interfaces loopback's para el manejo de la VoIP, se debe aplicar el comando h323-gateway voip bind srcaddr [IP Address] para asociar las llamadas de VoIP con el [IP Address] de la interface Loopback.

Tabla 4.20 Configuración de la Interface Loopback de Voz

4.7 Configuración en Equipos PE de la Red MPLS

Los clientes, según el equipo que posean, se pueden conectar a la Nube MPLS en forma directa (el equipo deberá contar con interfaces seriales) ó se pueden conectar a través de Equipos de Acceso ATM como Catalyst o Router (equipo con interface Ethernet o FastEthernet).

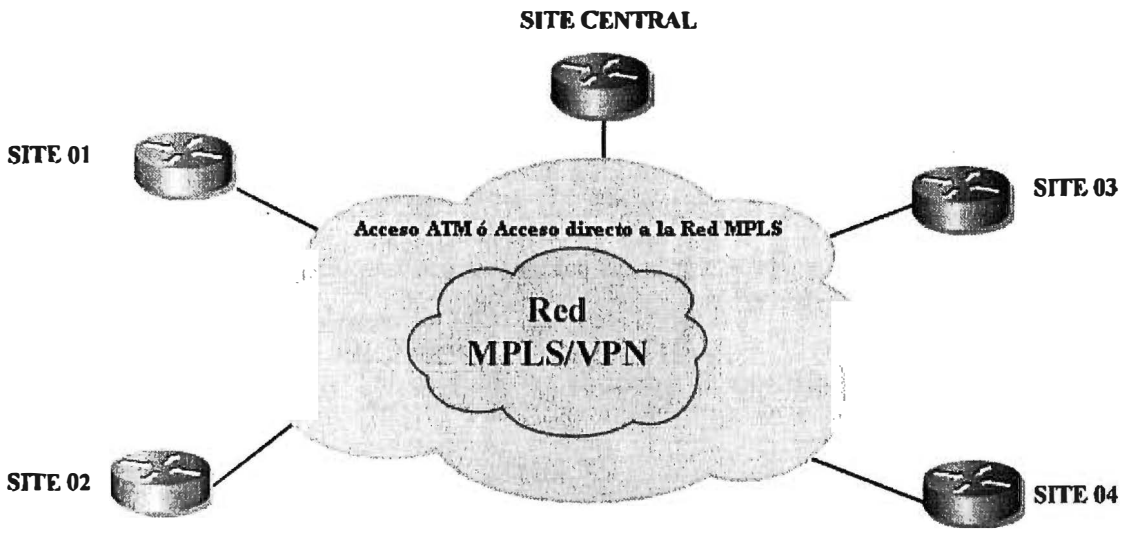


Fig. 4.3 Topología de Acceso desde el punto de vista del cliente

Cuando un equipo posee interfaces ethernet como WAN, el acceso lo hará a través de un equipo de POP (Point of Presence) que generalmente son Catalyst y luego pasarán por los equipos BPX donde se configurarán PVC's (atravesando la red ATM) hasta llegar a una Sub Interface ATM en el Router PE.

A continuación se muestra una topología de acceso a través de la red ATM, donde el ancho de banda no solamente se encuentra restringido con las políticas de calidad, sino también con los PVC's creados entre los BPX (existen varios parámetros que definen el ancho de banda del túnel virtual):

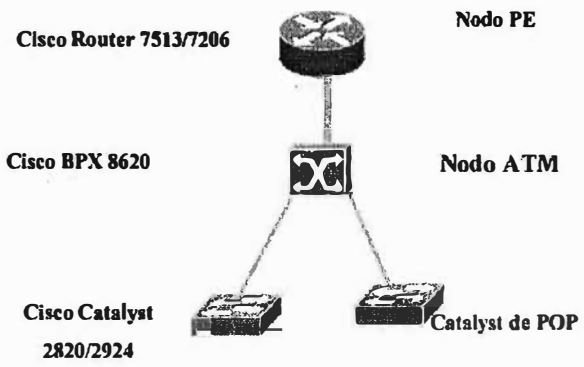


Fig. 4.4 Acceso ATM para llegar a la Nube MPLS

En la frontera de la Red MPLS, se cuenta con equipos PE (Provider Edge) que son los equipos frontera de la Nube MPLS de un determinado proveedor. Es en éstos equipos donde se configurarán políticas de calidad de acuerdo a los paquetes marcados enviados desde los equipos de los clientes (SITE).

A continuación en la Tabla 4.21, se muestra la configuración a considerar en los equipos PE:

Comando	Propósito
access-list 100 permit udp any any range 16384 32768	Se crea la lista de acceso 100, donde se permite el flujo de tráfico de paquetes con Protocolo de Control de Transmisión (TCP) y Protocolo de Datagrama de Usuario (UDP) ; pero que coincidan con ciertos puertos dados.
access-list 100 permit tcp any any eq 1720	
access-list 100 permit tcp any eq 1720 any	

class-map match-any voip	Se crea la política de clase para la Voz, cuando se considera interfaces seriales.
match ip precedence 5	Se clasifica el tráfico marcado con precedencia 5
match access-group 100	Se clasifica el tráfico que cumpla con la lista de acceso 100
class-map match-any qos5	Se crea la política de clase de servicio 3
match ip dscp cs5	Clasifica el tráfico definido como dscp 40
class-map match-any qos2	Se crea la política de clase de servicio 2
match ip dscp cs2	Clasifica el tráfico definido como dscp 16
class-map match-any qos1	Se crea la política de clase de servicio 1
match ip dscp cs1	Clasifica el tráfico definido como dscp 8

policy-map PolicerBWT_BW3_BW2_BW1	Se crea el policy-map asociado a un ancho de banda
class qos5	Hace referencia a la clase de servicio 3 para la asignación de recursos.
police BW3 peak1 peak2 conform-action transmit exceed-action drop	Limita el ancho de banda de la clase especificada (BW3 bps, peak1: Normal Burst bytes, peak2: Maximo Burst bytes)
class qos2	Hace referencia a la clase de servicio 2 para la asignación de recursos.
police BW2 peak1 peak2 conform-action transmit exceed-action set-dscp-transmit cs1	Limita el ancho de banda de la clase especificada (BW2 bps, peak1: Normal Burst bytes, peak2: Maximo Burst bytes)
class qos1	Hace referencia a la clase de servicio 1 para la asignación de recursos.
police BW1 peak1 peak2 conform-action transmit exceed-action transmit	Limita el ancho de banda de la clase especificada (BW1 bps, peak1: Normal Burst bytes, peak2: Maximo Burst bytes)

policy-map QoSBWT_BW3_BW2_BW1	Se crea el policy-map asociado a un ancho de banda
class qos5	Hace referencia a la clase de servicio 3 para la asignación de recursos.
priority BW3	Reserva la prioridad del BW limitado por el policer
police BW3 peak1 peak2 conform-action transmit exceed-action drop	Limita el ancho de banda de la clase especificada (BW3 bps, peak1: Normal Burst bytes, peak2: Maximo Burst bytes)
class qos2	Hace referencia a la clase de servicio 2 para la asignación de recursos.
bandwidth BW2	Reserva el BW mínimo para ésta clase de servicio.
police BW2 peak1 peak2 conform-action transmit exceed-action set-dscp-transmit cs1	Limita el ancho de banda de la clase especificada (BW2 bps, peak1: Normal Burst bytes, peak2: Maximo Burst bytes)
class qos1	Hace referencia a la clase de servicio 1 para la asignación de recursos.
bandwidth BW1	Reserva el BW para el tráfico con prioridad 1 (cs1)
class class-default	Se selecciona la clase default
fair-queue	

ip vrf XXXXX	Configuración de una VPN para el ruteo de redes del cliente, con su respectivo nombre
description Nombre_del_Cliente	
rd 12252:1049	Se especifica el Route Distinguer de la VPN

interface ATM5/0/0.173 point-to-point	Creación de la Sub-Interface lógica única para cada cliente
description Nombre_del_cliente	
ip vrf forwarding XXXXX	Se asocia los parámetros de la tabla de forwarding (de nombre XXXXX) en la interface lógica.
ip address [IP ADDRRES] [MASK]	
atm route-bridged ip	Se establece ruteo IP de los paquetes encapsulados sobre RFC 1483, a nivel ATM
pvc YYYYY VPI/VCI	Se define el nombre del PVC (YYYYY) así como el valor de VPI y VCI.
vbr-rt [PCR] [Average]	Se ingresa la tasa de bit variable (**V**ariable Bit **R**ate) de tiempo real, con los valores de tasa pico de celdas (PCR - Peak Cell Rate) en Kbps y de tasa promedio de celdas (Average) en Kbps, respectivamente.
encapsulation aal5snap	Selección del encapsulamiento ATM para el contenedor virtual (VC)
service-policy in PolicerBWT_BW3_BW2_BW1	Aplicación de la política de entrada y salida en la sub-interface lógica, donde BW3 es el ancho de banda correspondiente al CoS3, BW2 es el correspondiente al CoS2, el BW1 al CoS1; y el BWT es la suma de los anchos de banda de todos los CoS (BW1+BW2+BW3)
service-policy out QoSBWT_BW3_BW2_BW1	

Tabla 4.21 Configuración en los equipos PE

4.8 Ejemplos de configuración

a) Configuración del equipo de la Sede Principal de un cliente, donde la WAN se conecta a través de una Interface FastEthernet (cruza por la red ATM)

```
class-map match-any qos5
 match ip dscp cs5
class-map match-any qos2
 match ip dscp cs2
class-map match-any qos1
 match ip dscp cs1

class-map match-any P5
 match ip dscp cs5
 match access-group name qos5MPLS
class-map match-any P2
 match ip dscp cs2
 match access-group name qos2MPLS

policy-map SetDscpLan
 class P5
  set ip dscp cs5
 class P2
  set ip dscp cs2
 class class-default
  set ip dscp cs1

policy-map wan-MPLS
 class qos5
  priority 192
   police 192000 36000 72000 conform-action transmit
exceed-action drop
 class qos2
   police 1536000 288000 576000 conform-action transmit
exceed-action set-dscp-transmit cs1
 class qos1
  bandwidth 64
 class class-default
  fair-queue

policy-map Shape1792
 class class-default
  shape average 1792000
  service-policy wan-MPLS

interface Loopback0
 description loopback de Administracion
 ip address 10.232.8.122 255.255.255.255

interface Loopback1
 description IP para VoIP
 ip address 10.9.31.151 255.255.255.255
 h323-gateway voip bind srcaddr 10.9.31.151
!
interface FastEthernet0/0
 description Enlace-Wan
 ip address 10.10.4.82 255.255.255.252
 load-interval 30
 speed 10
 full-duplex
 fair-queue
 service-policy output Shape1792

interface FastEthernet0/1
 description Enlace-Lan-cliente
 ip address 10.0.0.253 255.255.255.0
 load-interval 30
 duplex auto
 speed auto
 no cdp enable
 service-policy input SetDscpLan

ip route 0.0.0.0 0.0.0.0 10.0.0.3
ip route 10.9.31.148 255.255.255.255 10.10.4.81
ip route 10.9.31.149 255.255.255.255 10.10.4.81
ip route 10.9.31.150 255.255.255.255 10.10.4.81
ip route 10.10.4.88 255.255.255.252 10.10.4.81
ip route 10.192.16.0 255.255.252.0 10.10.4.81
ip route 10.232.8.119 255.255.255.255 10.10.4.81
ip route 10.232.8.120 255.255.255.255 10.10.4.81
ip route 10.232.8.121 255.255.255.255 10.10.4.81
ip route 192.168.1.0 255.255.255.0 10.10.4.81
ip route 192.168.2.0 255.255.255.0 10.10.4.81
ip route 192.168.3.0 255.255.255.0 10.10.4.81

ip access-list extended qos5MPLS
 permit ip host 10.9.31.151 any

ip access-list extended qos2MPLS
 permit ip any host 192.168.1.20
 permit ip host 10.0.0.2 any
 permit ip any host 192.168.3.1
 permit ip any host 192.168.2.1

dial-peer voice 1 pots
 destination-pattern 100
 port 1/0/0
!
dial-peer voice 2 pots
 destination-pattern 101
 port 1/0/1
!
dial-peer voice 2000 voip
 incoming called-number 10.
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad

dial-peer voice 2006 voip
 destination-pattern 4001
 session target ipv4:10.9.31.148
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
!
dial-peer voice 2007 voip
 destination-pattern 4002
 session target ipv4:10.9.31.148
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad

dial-peer voice 2008 voip
 destination-pattern 300
 session target ipv4:10.9.17.175
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
!
dial-peer voice 2009 voip3014002
 session target ipv4:10.9.17.175
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
```

b) Configuración de un equipo de la Sede Remota para el mismo cliente, donde la WAN se conecta a través de una Interface FastEthernet (cruza por la red ATM):

```
class-map match-any qos5
 match ip dscp cs5

class-map match-any qos2
 match ip dscp cs2

class-map match-any qos1
 match ip dscp cs1

class-map match-any P5
 match ip dscp cs5
 match access-group name qos5MPLS

class-map match-any P2
 match ip dscp cs2
 match access-group name qos2MPLS

policy-map SetDscpLan
 class P5
  set ip dscp cs5
 class P2
  set ip dscp cs2
 class class-default
  set ip dscp cs1

policy-map wan-MPLS
 class qos5
  priority 96
   police 96000 18000 36000 conform-action transmit
exceed-action drop
 class qos2
  bandwidth 768
   police 768000 144000 288000 conform-action transmit
exceed-action set-dscp-transmit cs1
 class qos1
  bandwidth 64
 class class-default
  fair-queue

policy-map Shape928
 class class-default
  shape average 928000
  service-policy wan-MPLS

interface Loopback0
 description loopback de Administracion
 ip address 10.232.8.119 255.255.255.255
!
interface Loopback1
 description IP para VoIP
 ip address 10.9.31.148 255.255.255.255
 h323-gateway voip bind srcaddr 10.9.31.148

interface FastEthernet0/0
 description WAN
 ip address 10.10.4.86 255.255.255.252
 load-interval 30
 speed 10
 full-duplex
 fair-queue
 service-policy output Shape928

interface FastEthernet0/1
 ip address 192.168.1.253 255.255.255.0
 load-interval 30
 duplex auto
 speed auto
 service-policy input SetDscpLan

ip route 0.0.0.0 0.0.0.0 10.10.4.85

ip access-list extended qos5MPLS
 permit ip host 10.9.31.148 any

ip access-list extended qos2MPLS
 permit ip host 192.168.1.20 any
 permit ip any host 10.0.0.2
 permit ip any host 192.168.3.1
 permit ip any host 192.168.2.1

dial-peer voice 1 pots
 destination-pattern 4001
 port 1/0/0
!
dial-peer voice 2 pots
 destination-pattern 4002
 port 1/0/1

dial-peer voice 11 voip
 incoming called-number 400.
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad

dial-peer voice 13 voip
 destination-pattern 100
 session target ipv4:10.9.31.151
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
!
dial-peer voice 14 voip
 destination-pattern 101
 session target ipv4:10.9.31.151
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad

dial-peer voice 15 voip
 destination-pattern 300
 session target ipv4:10.9.17.175
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
!
dial-peer voice 16 voip
 destination-pattern 301
 session target ipv4:10.9.17.175
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
```

c) Configuración de un equipo de la Sede Remota para el mismo cliente, donde la WAN se conecta a través de una Interface Serial (no cruza por la red ATM):

```
class-map match-any qos5
 match ip dscp cs5

class-map match-any P5
 match ip dscp cs5
 match access-group name qos5MPLSS

policy-map SetDscpLan
 class P5
  set ip dscp cs5
 class class-default
  set ip dscp cs1

policy-map wan-MPLS
 class qos5
  priority 88
 class class-default
  fair-queue

interface Loopback1
 description Administracion
 ip address 10.233.4.231 255.255.255.255
!
interface Loopback2
 description Voz IP
 ip address 10.9.17.175 255.255.255.255
 h323-gateway voip bind srcaddr 10.9.17.175

interface FastEthernet0/1
 description LAN
 ip address 10.48.63.177 255.255.255.248 secondary
 ip address 10.48.72.137 255.255.255.224
 no ip redirects
 load-interval 30
 speed 100
 full-duplex
 service-policy input SetDscpLan

interface Serial0/1/0
 description CID 37277 Enlace WAN
 bandwidth 128
 no ip address
 encapsulation frame-relay IETF
 load-interval 30
 serial restart-delay 0
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
!
interface Serial0/1/0.1 point-to-point
 description CID 37277 Subinterface Virtual WAN Frame
Relay
 bandwidth 128
 ip address 10.225.17.110 255.255.255.252
 frame-relay class voipfr128
 frame-relay interface-dlci 110

ip route 0.0.0.0 0.0.0.0 10.225.17.109

ip access-list extended qos5MPLS
 permit ip host 10.9.17.175 any
 permit ip 10.48.63.176 0.0.0.7 any

map-class frame-relay voipfr128
 frame-relay cir 124800
 frame-relay bc 1280
 frame-relay be 0
 frame-relay mincir 124800
 frame-relay fragment 128
 service-policy output wan-MPLS

dial-peer voice 1 pots
 destination-pattern 300
 port 1/0/0
!
dial-peer voice 2 pots
 destination-pattern 301
 port 1/0/1

dial-peer voice 20 voip
 incoming called-number 30.
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad

dial-peer voice 30 voip
 destination-pattern 100
 session target ipv4:10.9.31.151
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
!
dial-peer voice 40 voip
 destination-pattern 101
 session target ipv4:10.9.31.151
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad

dial-peer voice 30 voip
 destination-pattern 4001
 session target ipv4:10.9.31.148
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
!
dial-peer voice 40 voip
 destination-pattern 4002
 session target ipv4:10.9.31.148
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
```

d) Configuración en el equipo PE de la Red MPLS que brinda acceso a la Sede Principal

RMPLSLIMA:

```
ip vrf 01039
 description Tubos y Perfiles Metalicos S.A.
 rd 12252:1039
 export map Loopback
 route-target export 12252:1000001039
 route-target import 12252:1000001039
 route-target import 12252:1100000001

class-map match-any qos5
 match ip dscp cs5

class-map match-any qos2
 match ip dscp cs2

class-map match-any qos1
 match ip dscp cs1

policy-map Policer1792_192_1536_64
 class qos5
  police 192000 36000 72000 conform-action transmit
exceed-action drop
 class qos2
  police 1536000 288000 576000 conform-action transmit
exceed-action set-dscp-transmit cs1
 class qos1
  police 64000 12000 24000 conform-action transmit exceed-
action transmit

policy-map Policer928_96_768_64
 class qos5
  police 96000 18000 36000 conform-action transmit exceed-
action drop
 class qos2
  police 768000 144000 288000 conform-action transmit
exceed-action set-dscp-transmit cs1
 class qos1
  police 64000 12000 24000 conform-action transmit exceed-
action transmit

policy-map QoS1792_192_1536_64
 class qos5
  priority 192
  police 192000 36000 72000 conform-action transmit
exceed-action drop
 class qos2
  bandwidth 1536
  police 1536000 288000 576000 conform-action transmit
exceed-action set-dscp-transmit cs1
 class qos1
  bandwidth 64
 class class-default
  fair-queue

policy-map QoS928_96_768_64
 class qos5
  priority 96
  police 96000 18000 36000 conform-action transmit exceed-
action drop
 class qos2
  bandwidth 768
  police 768000 144000 288000 conform-action transmit
exceed-action set-dscp-transmit cs1
 class qos1
  bandwidth 64
 class class-default
  fair-queue

interface ATM6/0.155 point-to-point
 description Enlace hacia la Sede Principal
 ip vrf forwarding 01039
 ip address 10.10.4.81 255.255.255.252
 atm route-bridged ip
 pvc CID40063 15/155
  vbr-rt 2311 2311
  tx-ring-limit 10
  encapsulation aal5snap
  max-reserved-bandwidth 78
  service-policy input Policer1792_192_1536_64
  service-policy output QoS1792_192_1536_64

interface ATM6/0.156 point-to-point
 description Enlace hacia la Sede Remota 1
 ip vrf forwarding 01039
 ip address 10.10.4.85 255.255.255.252
 atm route-bridged ip
 pvc CID40064 15/156
  vbr-rt 1197 1197
  tx-ring-limit 10
  encapsulation aal5snap
  max-reserved-bandwidth 78
  service-policy in Policer928_96_768_64
  service-policy out QoS928_96_768_64

ip route vrf 01039 0.0.0.0 0.0.0.0 10.10.4.82
ip route vrf 01039 10.9.31.148 255.255.255.255 10.10.4.86
ip route vrf 01039 10.232.8.119 255.255.255.255 10.10.4.86
ip route vrf 01039 192.168.1.0 255.255.255.0 10.10.4.86

router bgp 12252
 address-family ipv4 vrf 01039
 redistribute connected
 redistribute static
 default-information originate
 no auto-summary
 no synchronization
 exit-address-family
```

RMPLSSATELITAL:

```
ip vrf 01039
 description Tubos y Perfiles Metalicos S.A.
 rd 12252:1039
 export map Loopback
 route-target export 12252:1000001039
 route-target import 12252:1000001039
 route-target import 12252:1100000001

class-map match-any voip
 match ip precedence 5
 match access-group 100

policy-map voip_04
 class voip
  priority 88

interface Serial0/3/0
 description CID 37277 Enlace WAN
 bandwidth 128
 no ip address
 encapsulation frame-relay IETF
 load-interval 30
 serial restart-delay 0
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
 frame-relay intf-type dce
!
interface Serial0/3/0.1 point-to-point
 description CID 37277 Subinterface Virtual WAN Frame
Relay
 bandwidth 128
 ip address 10.225.17.109 255.255.255.252
 frame-relay class voipfr128_04
 frame-relay interface-dlci 110

ip route vrf 01039 10.9.17.175 255.255.255.255
10.225.17.110
ip route vrf 01039 10.48.63.176 255.255.255.248
10.225.17.110
ip route vrf 01039 10.48.72.128 255.255.255.224
10.225.17.110
ip route vrf 01039 10.233.4.231 255.255.255.255
10.225.17.110

router bgp 12252
 address-family ipv4 vrf 01039
 redistribute connected
 redistribute static
 default-information originate
 no auto-summary
 no synchronization
 exit-address-family

map-class frame-relay voipfr128_04
 frame-relay cir 124800
 frame-relay bc 1280
 frame-relay be 0
 frame-relay mincir 124800
 frame-relay fragment 160
 service-policy output voip_04

access-list 100 permit udp any any range 16384 32768
access-list 100 permit tcp any any eq 1720
access-list 100 permit tcp any eq 1720 any
```

Lo anteriormente mostrado, es un ejemplo de la configuración que puede tener la Sede Principal y un equipo de la Sede Remota cuando cruza la red ATM o usa interfaces seriales, de un determinado cliente, así como la configuración mínima que se consideraría en los equipos PE de la Nube MPLS para que exista comunicación entre las sedes del cliente.

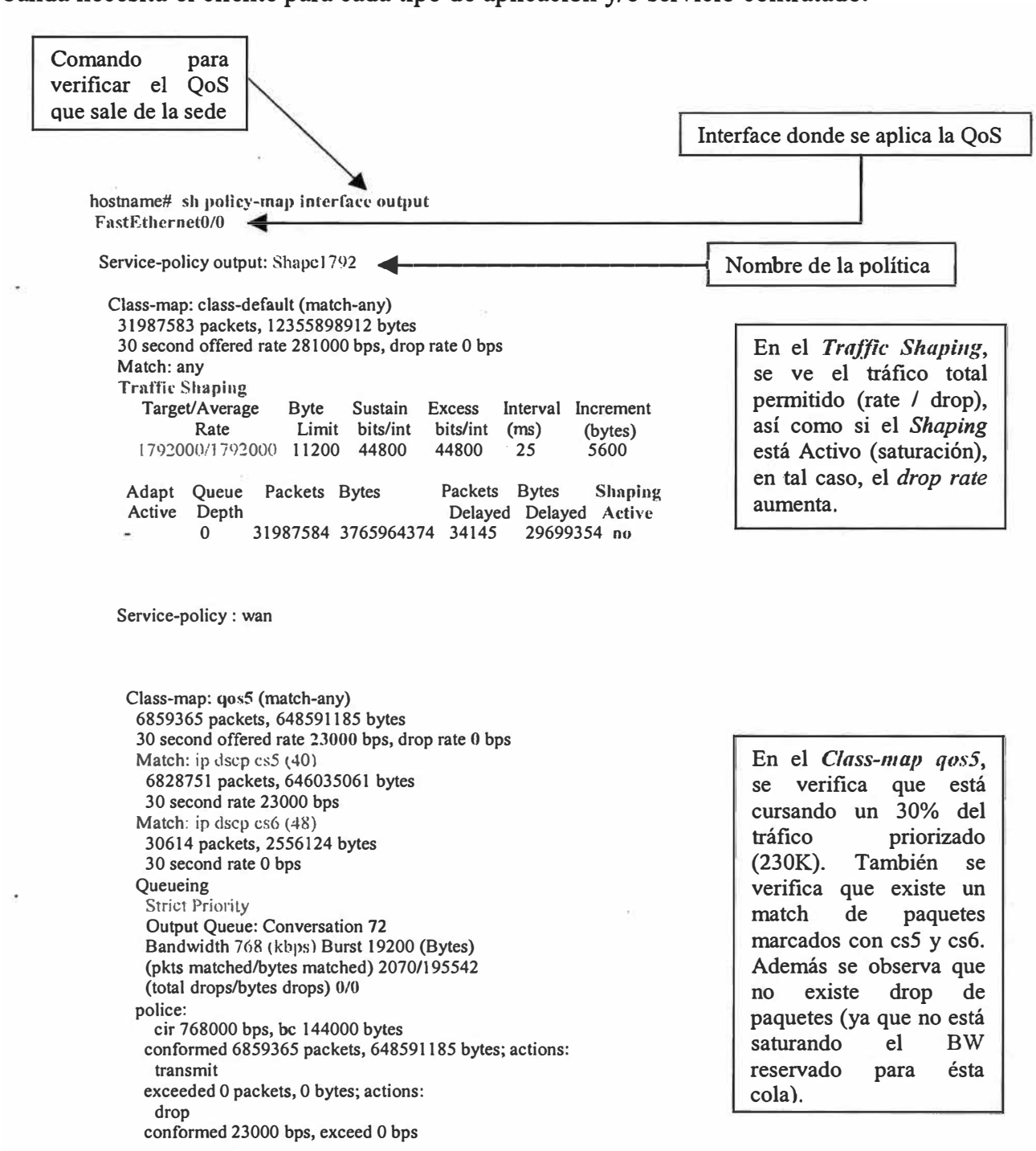
A continuación, se muestra la configuración de la política de marcado para una sede de un cliente, el cual tiene configurado VLAN's, para lo cual ya no es necesario la configuración de listas de acceso (para definir que rangos de IP's de la LAN pertenecen a QoS5, QoS2 o QoS1). Con respecto a la política de congestión, la configuración es la misma que la considerada en el caso anterior:

```
policy-map SetLanQoS5
 class class-default
  set ip dscp cs5

policy-map SetLanQoS1
 class class-default
  set ip dscp cs1


interface GigabitEthernet0/1
 description Enlace RED LAN
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 duplex full
 speed 10
 no cdp enable
!
interface GigabitEthernet0/1.1
 description VLAN DATOS
 encapsulation dot1Q 1
 ip address 172.28.32.1 255.255.248.0
 no ip redirects
 no ip proxy-arp
 service-policy input SetLanQoS1

interface GigabitEthernet0/1.2
 description VLAN VOZ
 encapsulation dot1Q 2
 ip address 172.17.32.1 255.255.248.0
 no ip redirects
 no ip proxy-arp
 service-policy input SetLanQoS5
```

e) Detalles del tráfico cursado visto de manera cuantitativa

En los siguientes datos extraídos del router de un cliente que ha contratado un servicio con los siguientes BW de trafico CoS3 = 768 Kbps, CoS2 = 768 Kbps y CoS1 = 256 Kbps, se puede ver la cantidad de paquetes transferidos así como si ocurre eliminación (drop) de paquetes, para cada clase de servicio.

El comando usado es útil para el análisis del tráfico que cursa un determinado cliente, ya que con el, se puede visualizar, de manera cuantitativa, cuanto de ancho de banda necesita el cliente para cada tipo de aplicación y/o servicio contratado.



```
    Class-map: qos2 (match-any)
      18658814 packets, 9244107182 bytes
      30 second offered rate 244000 bps, drop rate 0 bps
      Match: ip dscp cs2 (16)
        18658814 packets, 9244107182 bytes
        30 second rate 244000 bps
      Queueing
        Output Queue: Conversation 73
        Bandwidth 768 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 19822/13615599
    (depth/total drops/no-buffer drops) 0/0/0
      police:
          cir 768000 bps, bc 144000 bytes
        conformed 18658814 packets, 9244107182 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          set-dscp-transmit cs1
        conformed 244000 bps, exceed 0 bps


    Class-map: qos1 (match-any)
      6088425 packets, 2432756522 bytes
      30 second offered rate 8000 bps, drop rate 0 bps
      Match: ip dscp cs1 (8)
        6088426 packets, 2432756522 bytes
        30 second rate 8000 bps
      Queueing
        Output Queue: Conversation 74
        Bandwidth 256 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 12157/15881315
    (depth/total drops/no-buffer drops) 0/0/0


    Class-map: class-default (match-any)
      380979 packets, 30444077 bytes
      30 second offered rate 2000 bps, drop rate 0 bps
      Match: any
      Queueing
        Flow Based Fair Queueing
        Maximum Number of Hashed Queues 64
    (total queued/total drops/no-buffer drops) 0/0/0
 FastEthernet0/1
hostname#
```

En el ***Class-map qos2***, se verifica que está cursando un 32% del tráfico priorizado (244K). También se verifica que existe un match de paquetes marcados con cs2. Al igual que el Class-map cs5, no existe drop de paquetes.

En el ***Class-map qos1***, solo está pasando 8K de tráfico. Asi mismo, tampoco hay drop de paquetes.

4.9 Seleccionando Equipos CISCO en la implementación de redes MPLS

El proceso de selección de equipos, se basa en varias consideraciones, las cuales son primordiales antes de tomar una decisión sobre que proveedor de equipos se va a elegir para implementar una determinada red. En el caso particular, de la experiencia profesional obtenida de la empresa de telecomunicaciones donde me desempeño, el proveedor CISCO superó a los demás proveedores, en la evaluación de las siguientes consideraciones:

a) Validación de Equipamiento:

Al momento de iniciar el diseño de una RED, lo primero que se debe tener en cuenta son las prestaciones de servicio que se va a ofrecer, por ende se debe inicialmente hacer un análisis de todos los requerimientos, a fin de poder solicitar a los proveedores las propuestas técnicas de los equipos y realizar un cuadro comparativo de los mismos, con el propósito de obtener el equipamiento que se adecue a la mejor manera de nuestras necesidades.

Mucho dependerá de la función que desarrolle un determinado equipo de un proveedor en nuestra red, por ejemplo, si solo se requiere para:

- Medio de Transporte
  - Cisco
  - Nortel
  - Alcatel
  - NEC
  - ZTE
- IP
  - Cisco
  - Juniper
  - Huawei
- Red Metro
  - Huawei
  - Cisco
  - Juniper
  - Siemens

- QoS
    - Juniper
    - Cisco
    - Huawei

b) Escalabilidad del Equipo:

La escalabilidad es la capacidad de mejorar recursos para ofrecer una mejora lineal en la capacidad de servicio.

Debe formar parte del proceso de diseño porque no es una característica separada que se pueda agregar después. Al igual que con otras funciones de aplicación, las decisiones que se tomen durante las primeras fases de diseño y codificación determinarán en gran medida la escalabilidad de la aplicación.

En resumen, es la capacidad de crecimiento que tiene el equipo, es decir cuantas rutas, vlan's, vpn's, interfaces, etc, soportará el equipo sin llegar a saturarse. En tal sentido, en el mercado se cuenta con varios modelos y configuraciones de equipos, los cuales permiten trabajar con los requerimientos recomendados para las aplicaciones que uno posee.

c) Performance del Equipo:

La performance permite verificar si el equipo llega a las características establecidas anteriormente mediante la escalabilidad de los equipos

d) Pruebas de Laboratorio:

Las pruebas de laboratorio permiten verificar la robustez del equipo, realizando una validación real con pruebas de tráfico. De esta manera podremos verificar si el equipo es lo óptimo para la red.

e) Verificación económica:

Una vez que se haya escogido el material a cotizar, se analizará el cuadro comparativo y se evaluará la proposición económica.

La gama de empresas que existen en el mercado permiten que el criterio de elección, no se limite solo a la capacidad del equipo sino también al factor económico.

CAPITULO V

5.1. Tecnología NGN

El servicio de VoIP (Protocolo de Voz sobre Internet – Voice over Internet Protocol) se ha venido desarrollando exitosamente durante todos estos años, el cual ofrecía un servicio masivo implementado sobre redes IP. Éstos servicios implementados, compitió y ganó la batalla sobre las redes tradicionales de conmutación de circuitos y centrales de conmutación. Paralelamente al éxito de la VoIP, los organismos de estandarización internacionales, aceptaron una nueva tecnología, introduciendo un nuevo concepto, el de las Redes NGN.

5.1.1. Definición de NGN

En el año 2000, el ETSI (European Telecommunications Standards Institute) mediante su grupo de trabajo NGN Starter Group introducía la primera definición de una Red NGN:

"NGN - Next Generation Network - es un concepto para la definición y despliegue de redes, que, debido a su separación formal en diferentes niveles y a la utilización de interfaces estándares, permite ofrecer a los operadores y proveedores de servicios una plataforma que puede evolucionar paso a paso en la creación, despliegue y administración de nuevos servicios"

En el año 2004, una de las grandes empresas de telecomunicaciones en América Latina, desarrolla ésta tecnología, el cual entre sus beneficios más importantes destaca el poder escalar las soluciones de acuerdo al ritmo de los negocios, integrando sucursales, nuevos proveedores y clientes, en forma discreta y sin que ello implique un incremento de los costos de operación o de infraestructura. Asimismo, se podrá a través de una sola conexión IP dar conectividad a las aplicaciones de su empresa desde todas sus sucursales,

ya sea para Voz, Datos o Video, sin preocuparse de tener un nodo central de comunicaciones que contenga toda la información. La red NGN permite el desarrollo de una mayor variedad de servicios de valor agregado para el usuario final, por ejemplo se pueden implementar soluciones de mensajería unificada integrando a todas las sucursales (en las soluciones tradicionales, sería necesario replicar la solución en cada sucursal) sin que esto implique tener que comprar servidores independientes para cada oficina. También puede implementar herramientas de atención telefónica como FaxServer que dan servicios a todos las sucursales de una empresa, sin que esto se traduzca en una mayor adquisición de infraestructura.

En general, no existe una definición universalmente aceptada para el término NGN. Todas coinciden en que será la red de telecomunicaciones del futuro, aunque difieren ligeramente en las características y funcionalidades que presenta. Quizá una de las definiciones más acertada es la desarrollada por el SG13 UIT-T (Unión Internacional de las Telecomunicaciones - Sector de Estandarización de las Telecomunicaciones), en su Recomendación Y2001. En ella se define la NGN a partir de las características más relevantes que la distinguen de las redes de telecomunicaciones tradicionales. Entre otras se pueden resaltar las siguientes:

- Es una red de paquetes. En particular IP no será el principal, sino el único protocolo de nivel tres para la NGN. El paquete IP será la unidad de transporte de datos fundamental para todo tipo de medio. Lo anterior no excluye el hecho de que el paquete IP en sí mismo podrá ser encapsulado en diversas tecnologías de nivel 2 y 1, como Ethernet, ATM, MPLS, xDSL, DWDM, RPR, SDHng, etc.
- La NGN debe hacer uso de tecnologías de transporte con capacidades de calidad de servicio y de banda ancha, para ofrecer diferentes niveles de QoS según los requerimientos de los diversos tipos de tráfico.
- La NGN permite la migración desde las redes actuales, verticalmente separadas y específicas para diferentes servicios, hacia una única red capaz de ofrecer y transportar todos los servicios. Esto implica que los sistemas de gestión y facturación también estarán integrados, con los correspondientes ahorros en costos y recursos.
- Soporta movilidad generalizada la cuál permitirá ofrecer servicios permanentes y móviles a los clientes.

Se espera que la migración a las redes NGN, que ya se inició entre 2004 y 2005, continúe hasta el 2010 e incluso hasta el 2015.

5.1.2. Costo/beneficio enla migración hacia redes NGN

Durante los últimos años, las tecnologías de Redes de Nueva Generación (NGN) han sido promocionadas extensamente como la opción adecuada para las redes de telecomunicaciones del futuro. Diferentes estudios sobre el costo/beneficio que involucra migrar hacia redes NGN, demostraban los ahorros de gastos de capital y de explotación , los cuales, junto con la promesa de nuevos servicios generadores de ingresos, hicieron que la transición a la transmisión por paquetes fuera una proposición interesante. Sin embargo, la revolución de la voz "empaquetada" ha sido lenta en materializarse.

La visión original respecto a las redes NGN estaba motivada en gran medida por la convergencia de redes de circuitos y redes de paquetes en una única red NGN multi-servicio. Se consideraba que esta red NGN aportaría una atractiva serie de beneficios para los proveedores de servicios. Entre las promesas originales de las redes NGN estaban las siguientes:

- Invirtiendo en tecnología NGN "evolucionable", pueden congelarse todas las inversiones ya existentes en tecnología TDM (Time Division Multiplex Multiplexión por División de Tiempo), por ejemplo, para una expansión de la capacidad.
- Puede utilizarse NGN para sustituir tecnología TDM anticuada.
- NGN ofrece considerables ahorros operacionales y de explotación, ya que pueden integrarse múltiples redes en una única red multi-servicio. Además, las redes de paquetes son menos jerárquicas, son más escalables y fáciles de aprovisionar.

Pero, la realidad de NGN en la actualidad, es que los proveedores de servicios adoptaron una actitud muy cautelosa a la hora de invertir en tecnologías NGN. Los operadores han tenido especial cuidado en asegurarse que las decisiones de compra actuales permitan desplegar nuevos servicios generadores de ingresos a corto plazo.

El largo ciclo de vida de los sistemas de infraestructura de telecomunicaciones requiere que los equipos y los sistemas instalados hoy, no queden obsoletos antes de obtener de ellos todo su valor invertido.

La migración a tecnología de conmutación de nueva generación está determinada por factores económicos: principalmente por la necesidad de controlar o reducir costos en los servicios existentes, junto a la necesidad de aumentar o mantener los ingresos mediante nuevos servicios.

La calidad de voz extremo a extremo, desempeña un papel crucial en el plan de migración global. Se requiere una planificación cuidadosa, ya que una introducción incontrolada de tecnología de nueva generación podue traer consigo niveles de servicio inaceptables para los usuarios finales.

Es por eso, que los operadores adoptaron como la estrategia de migración más sensata, desplegar una red de nueva generación, en la que de forma controlada, y para los primeros usuarios en adoptar la Banda Ancha, se ofrecería no sólo servicios de voz, sino una gama variada de nuevos servicios que aportarían fuentes de ingresos adicionales.

NGN no es sino un modelo de arquitectura de redes de referencia que debe permitir desarrollar toda la gama de servicios IP multimedia de nueva generación (comunicaciones VoIP nueva generación, videocomunicación, mensajerías integradas multimedia, domótica, etc) así como la evolución, migración en términos mas o menos de sustitución o emulación de los actuales servicios de telecomunicación.

Éste modelo de referencia puede resumirse en el siguiente decálogo de puntos:

- Arquitectura de red horizontal basada en una división transparente de los planos de transporte, control y aplicación.
- El plano de transporte estará basado en tecnología de conmutación de paquetes IP/MPLS.
- Interfaces abiertos y protocolos estándares.
- Migración de las redes actuales a NGN.
- Soporte de servicios de diferente naturaleza: real time/ non real time, streaming, servicios multimedia (voz, video, texto).
- Calidad de servicios garantizada extremo a extremo.
- Seguridad.
- Movilidad generalizada.

En estos años, NGN se puede establecer y simplificar, en 2 marcos de actuación, que son:

- En mercados en expansión, en crecimiento en servicios básicos de telecomunicación, donde se "simulan" o "emulan" redes y servicios tradicionalmente de circuitos, optimizando el escenario técnico-económico, mediante el uso de NGN-SoftSwitches, transporte IP e interfaces de banda estrecha / banda ancha para el soporte de servicios de voz.
- En mercados consolidados en términos de servicios fijos – móviles donde la búsqueda de eficiencias entre ambos mundos y la banda ancha y los nuevos servicios IP multimedia hacen que NGN adquiera un papel fundamental como eje del desarrollo de la convergencia.

Actualmente, cuando un cliente que tiene sus servicios de voz ya implementada en una determinada infraestructura de red y requiere migrar sus servicios a la nueva red NGN, lo que hacen las empresas de telecomunicacines, es redireccionar los servicios a la plataforma softswitch, y en la mayoría de los casos, se reusa los equipos de última milla y de acceso. Las empresas de telecomunicaciones vienen invertiendo en equipos de la plataforma softswitch, que sean compatibles con los equipos ya existentes en su red.

Para el cliente, el costo de aquirir cualquier servicio, el cual va a pasar por la red NGN, es el mismo, es decir, **la migración hacia la red NGN es trasparente para el cliente**.

Las empresas son las beneficiarias en el tema de la migración hacia las redes NGN, ya que estaban pasando por una escacez de recursos por la alta demanda de servicios contratados presentada en los últimos años, y no era inteligente seguir invirtiendo en diferentes tipos de hardware para seguir brindando los servicios exigidos por la evolución de la tecnología. Ahora, con la migración a la red NGN, es possible pasar varios servicios (VoIP, ToIP, telefonía digital y analogical, virtual fax server, etc) por una sola sóla plataforma (softswitch), la cual está integrada con las infraestructuras de redes ya existentes.

5.2. Softswitch

Es un dispositivo que provee control de llamada y servicios inteligentes para redes de conmutación de paquetes. Un Softswitch sirve como plataforma de integración para aplicaciones e intercambio de servicios. Se considera la pieza central en las primeras implementaciones de las NGN. Este dispositivo, combinación de hardware y software,

provee control de llamada y servicios inteligentes para redes de conmutación de paquetes, y puede conmutar el tráfico de voz, datos y video de una manera eficiente. Los componentes principales del softswitch se denominan: Media Gateway (Pasarela de Medios), Media Gateway Controller (Controlador de Pasarela de Medios) y Signalling Gateway (Pasarela de Señalización). Aunque muchas veces estos componentes se encuentran integrados pueden estar separados, lo que requiere el uso de protocolos de comunicación entre los mismos.

5.2.1. Características de la tecnología de softswitch

Una característica clave del softswitch es su capacidad de brindar, a través de la red IP, un sistema telefónico tradicional, confiable y de alta calidad. Sus interfaces de programación permiten a los fabricantes de software crear rápidamente nuevos servicios basados en IP, que funcionen para ambas redes: la telefónica tradicional y la IP. Es así como se pueden ofrecer servicios de voz avanzados, así como nuevas aplicaciones multimedia.

Separar los servicios y el control de llamadas, de la red de transporte actual es una característica esencial de las redes de telecomunicaciones basadas en softswitch. También se tienen las siguientes características:

- Controlan los servicios de conexión asociados a los Media Gateway y los puntos terminales que utilizan IP como protocolo nativo.
- Encaminan las llamadas en función de la señalización y de la información almacenada en la base de datos de clientes.
- Poseen la capacidad para transferir el control de una llamada a otro elemento de red.
- Poseen interfaces que permiten realizar funciones de gestión, como las que se conectan a los sistemas de facturación para la gestión de contabilidad.
- Pueden coexistir con las redes tradicionales así como proveer los servicios de la tecnología de conmutación de paquetes.
- Soportan los servicios de voz, fax, vídeo, datos y posibilidades para los nuevos servicios que serán ofrecidos en el futuro.

Los softswitch se pueden encontrar centralizados o distribuidos por la red. En los casos de redes muy extensas se realiza una división en varias zonas, y se ubica un

softswitch en cada una de ellas. En todos los casos, por seguridad, se emplea redundancia en los centros de conmutación, por lo que el número mínimo de softswitchs a ubicar en una red o zona es dos.

5.2.2. Arquitectura funcional

La arquitectura funcional de un softswitch puede estar integrada por uno o varios de sus componentes: Media Gateway (MG), Media Gateway Controller (MGC) y Signaling Gateway (SG o SMG). Las funcionalidades básicas de estos componentes son:

- **Media Gateway**. Pueden ser de Acceso (AMG) o Troncal (TMG). El **AMG** realiza labores de compresión y descompresión de señales de voz, por lo que requiere potencia de procesamiento. Ofrecen conectividad desde cualquier tipo de acceso como xDSL (Digital Subscriber Line), PABX (Private Automatic Branch eXchange) u otros. Los **TMG** se despliegan en el borde de la red de paquetes, cerca del ingreso de los troncos de portadora. Desde el punto de vista económico, evita las cargas recurrentes de líneas dedicadas debido a la convergencia de este tráfico en un único gateway.
- **Media Gateway Controller**. Es el elemento más importante del softswitch, cuya función es la de localizar, asignar, contabilizar y gestionar los recursos de llamada de las NGN. Ofrece un control centralizado de la mayoría de los servicios. Las redes grandes normalmente demandan una cantidad significativa de memoria y procesamiento para el MGC. Mientras el MG debe realizar un procesamiento en tiempo real de las señales de voz, el MGC debe iniciar y terminar las llamadas, monitorizar los recursos de la red, contabilizar los registros, manejar la seguridad (autenticación y autorización) y tareas administrativas críticas. A menudo, éste elemento es referido como el **Call Agent**, el cual es referido como el centro operativo del softswitch. Éstre componente se comunica con las otras partes del softswitch y componentes externos usando diferentes protocolos.
- **Signaling Gateway**. Termina las conexiones SS7 (Sistema de Señalización número 7), emula un terminal para la red SS7 y convierte los mensajes SS7 en un formato compatible con IP (puede ser H.245 o SIP (Session Initiation Protocol)). La comunicación entre el SG y el MGC se realiza generalmente sobre SCTP (Stream Control Transmission Protocol). Encima del SCTP, el par SG/MGC puede utilizar

uno de los protocolos xUA (User Agent). Es el responsable para ejecutar el establecimiento y desconexión de la llamada. Se puede decir, que es el puente entre la red de señalización SS7 y los nodos manejados por el softswitch en la red IP.

En general, la combinación de MG, MGC y SG debe operar de la siguiente manera: el SG traduce la información de señalización SS7, incluyendo el inicio de llamada desde la PSTN al MGC. El MGC debe notificar la encuesta o solicitud de llamada al dispositivo IP apropiado (teléfono o PC) o al MG (utilizando H.248/MEGACO), y proporciona información para establecer la llamada. Una vez que la comunicación se establece, el MG proporciona compresión/descompresión de salida y conversión de medio durante toda la duración de la llamada.

5.3. La Rgulación de las Redes de Nueva Generaión (NGN)

En el aspecto del marco regulatorio, actualmente una de las principales preocupaciones de los operadores es que la regulación no signifique una traba en el proceso de transformación de sus redes.

El Marco Regulatorio, tiene entre sus principios y objetivos, garantizar la competencia efectiva, y promover al mismo tiempo, una inversión eficiente en materia de infraestructuras fomentando a su vez la innovación. Y es, sobre esta situación, desde la que parte y se puede definir la regulación adecuada para el acceso de las nuevas redes.

El regulador a la hora de llevar a cabo su actividad, debe atender a las necesidades de los usuarios y de los agentes, aunque sin olvidarse de establecer un marco cierto y favorable a las inversiones. Sin embargo, la mejora de las redes y los procesos de innovación, pueden verse claramente afectados en caso de que se impongan de manera prematura medidas dirigidas a proteger, hipotéticas situaciones de fallos en el mercado, sin que éstas se hayan llegado a producir.

La imposición de cualquier obligación o norma adoptada, de forma precipitada o anticipada a que aparezca su necesidad en el mercado, puede tener como consecuencia que se paralicen o retrasen en gran medida las perspectivas de inversión que puedan tener los operadores vigentes.

CONCLUSIONES

1. MPLS soporta la configuración de QoS garantizada, donde los paquetes son marcados para un tratamiento diferenciado, permitiendo de ésta manera brindar servicios como voz o vídeo, los cuales demandan un nivel de delay muy bajo.
2. MPLS reduce considerablemente los niveles de procesamiento en los enrutadores, debido al reenvío simplificado de los paquetes a través de etiquetas.
3. MPLS brinda un apropiado nivel de seguridad con el uso de VPN's.
4. MPLS soporta cualquier tipo de trafico en una red IP, independientemente del tipo de protocolo de enrutamiento usado.
5. Cuando se aplica políticas de calidad de servicio (QoS) sobre el ancho de banda contratado de un determinado cliente, se está configurando el servicio asegurando un ancho de banda mínimo para cada tipo de tráfico y al mismo tiempo se está definiendo una política de encolamiento diferencial de paquetes en función de la Clase de Servicio, en caso se presente un evento de congestión.
6. La arquitectura Diffserv presenta mejores condiciones en la implementación de redes de gran volumen de trafico, a diferencia de la arquitectura InterServ.
7. El uso de VPN implica cifrar los datos antes de ser enviados a través de la red y descifrarlos antes de ser entregados al destino final.
8. Las VPN representan una gran solución a las empresas en cuanto a seguridad, confidencialidad e integridad de los datos, debido a que reduce significativamente los costos de la transferencia de datos de un lugar a otro.
9. Es necesario establecer correctamente los parámetros de acceso y políticas de seguridad a implementar una VPN, ya que la omisión de ellos, podría traer consecuencias serias.

10. La selección del proveedor que uno utilizará para implementar una determinada red, depende de varios factores de evaluación como: validación de equipamiento, escalabilidad del equipo, performance del equipo, pruebas de laboratorio y verificación económica. Para el presente informe, se ha mostrado como se aplica QoS sobre equipos CISCO, ya que si bien es cierto que en el mercado existe una gama de marcas de equipos, el proveedor CISCO ha superado a muchas de ellas en la evaluación de los factores anteriormente mencionados y explicados en el capitulo IV. Es por eso, que actualmente se viene usando éstos equipos en casi un 90% de las redes de networking del país.

ANEXO A

Tabla de IOS recomendado de algunos equipos CISCO

TABLA A.1 Tabla de IOS recomendado de algunos equipos CISCO, para servicios de solo DATOS

Router Platform	IOS Type	IOS Name	Memory (Mb)	Flash (Mb)	BW Range (sin NAT)	BW Range (con NAT)	Port WAN Configuration	Features
806	IP PLUS	c806-sy6-mz.123-21.bin	20	8	Until 512K	Until 512K	Half Duplex	Datos, QoS
831	IP/FW/PLUS 3DES	c831-k9o3sy6-mz.124-8c.bln	64	12	Until 1.5M	Until 1.5M	Full Duplex	FW + VPN + BGP + BGP,EIGRP,OSPF
1605	IP	c1600-y-mz.120-28d.bln	8	4	Until 1M	Until 1M	Half Duplex	Datos
	IP PLUS	c1600-sy-mz.121-27b.bin	12	4	Until 512K	Until 512K	Half Duplex	Datos + QoS + BGP + FR Fragment (FRF.12)
	IP PLUS IPSEC 56	c1600-k8sy-mz.122-37.bin	16	6	Until 128K	Until 128K	Half Duplex	Datos + QoS + VPN
1751	IP	c1700-y-mz.123-20.bin	32	8	Until 1M	Until 1M	Full Duplex	Datos
1841	IP BASE	c1841-ipbasek9-mz.124-8c.bin	128	32	Until 13M	Until 3.5M	Full Duplex	Datos, QoS
	ENTERPRISE BASE	c1841-entbasek9-mz.124-8c.bin	128	32	Until 13M	Until 3.5M	Full Duplex	Datos + QoS + DLSW+ IPX
2610-2614	IP PLUS	c2600-is-mz.122-37.bin	48	16	Until 2M	Until 2M	Full Duplex	Datos, QoS
	IP/FW/IDS PLUS IPSEC 56	c2600-ik8o3s-mz.122-37.bin	48	16	Until 2M	Until 2M	Full Duplex	Datos + VPN + FW
2610XM-2611XM	IP	c2600-i-mz.123-20.bln	32	8	Until 2M	Until 2M	Full Duplex	Datos
	IP PLUS	c2600-is-mz.122-37.bin	48	16	Until 2M	Until 2M	Full Duplex	Datos, QoS
	IP/FW/IDS PLUS IPSEC 56	c2600-ik8o3s-mz.122-37.bln	48	16	Until 2M	Until 2M	Full Duplex	Datos + VPN + 3DES
2801	ENTERPRISE SERVICES	c2801-entservicesk9-mz.124-8c.bin	128	64	Until 18M	Until 4M	Full Duplex	Datos + QOS + DLSW+ IPX + BGP
2811	ENTERPRISE SERVICES	c2800nm-entservicesk9-mz.124-8c.bin	256	64	Until 15M	Until 3M	Full Duplex	Datos + DLSW+ DatosX + BGP
3640	IP PLUS	c3640-is-mz.123-20.bin	96	32	Until 10M	Until 10M	Full Duplex	Datos, QoS
3640	IP/FW/IDS PLUS IPSEC 56	c3640-ik8o3s-mz.122-37.bin	64	16	Until 10M	Until 10M	Full Duplex	Datos + VPN + FW
7201 - 7200VXR	IP IPSEC 56	c7200-is56i-mz.121-27b.bln	64	16	No aplica	No aplica	Full Duplex	ATM, QoS, VoIP, E2

TABLA A.2 Tabla de IOS recomendado de algunos equipos CISCO, para servicios de DATOS, sin VoIP y con ToIP

Router Platform	IOS Type	IOS Name	Memory (Mb)	Flash (Mb)	BW Utilization Range	Port WAN Configuration	Features
806	IP PLUS	c806-sy6-mz.123-21.bin	20	8	Until 512K	Half Duplex	Datos, QoS
831	IP/FW/PLUS 3DES	c831-k9o3sy6-mz.124-8c.bin	64	12	Until 1.5M	Full Duplex	Datos + QoS + FW + VPN + BGP + BGP,EIGRP,OSPF
1605	IP PLUS	c1600-sy-mz.121-27b.bin	12	4	Until 512K	Half Duplex	Datos + QoS + BGP + FR Fragment (FRF.12)
	IP PLUS IPSEC 56	c1600-k8sy-mz.122-37.bin	16	6	Until 128K	Half Duplex	Datos + QoS + VPN
1751	IP VOICE	c1700-ipvoice-mz.123-20.bin	64	16	Until 1M	Full Duplex	Datos, QoS
	IP/VOICE PLUS	c1700-sv3y-mz.123-20.bin	48	16	Until 1M	Full Duplex	IP VOICE + BGP
1841	ENTERPRISE BASE	c1841-entbasek9-mz.124-8c.bin	128	32	Until 4M	Full Duplex	Datos + QoS + DLSW+ IPX
2610-2614	IP PLUS	c2600-ls-mz.122-37.bin	48	16	Until 2M	Full Duplex	Datos, QoS
	ENTERPRISE PLUS	c2600-js-mz.122-37.bin	48	16	Until 2M	Full Duplex	Datos + DLSW+ IPX
	IP/FW/IDS	c2600-io3-mz.123-20.bin	32	16	Until 2M	Full Duplex	Datos + FW
2610XM-2611XM	IP VOICE	c2600-ipvoice-mz.123-20.bin	96	32	Until 2M	Full Duplex	Datos, QoS
	IP PLUS	c2600-ls-mz.122-37.bin	48	16	Until 2M	Full Duplex	Datos, QoS
	IP/FW/IDS PLUS IPSEC 56	c2600-ik8o3s-mz.122-37.bin	48	16	Until 2M	Full Duplex	Datos + VPN + 3DES
2801	IP VOICE	c2801-ipvoicek9-mz.124-8c.bin	128	64	Until 5M	Full Duplex	QoS, VoIP, E1
	ENTERPRISE SERVICES	c2801-entservicesk9-mz.124-8c.bin	128	64	Until 5M	Full Duplex	Datos + QOS + DLSW+ IPX + BGP
2811	IP VOICE	c2800nm-ipvoicek9-mz.124-8c.bin	256	64	Until 4.5M	Full Duplex	Datos + DLSW+ Datos
	ENTERPRISE SERVICES	c2800nm-entservicesk9-mz.124-8c.bin	256	64	Until 4.5M	Full Duplex	Datos + DLSW+ DatosX + BGP
3620	IP PLUS	c3620-is-mz.123-20.bin	64	16	Until 3M	Full Duplex	Datos, QoS
	IP PLUS	c3620-is-mz.122-37.bin	48	16	Until 3M	Full Duplex	Datos, QoS
	IP/FW/IDS PLUS IPSEC 56	c3620-ik8o3s-mz.122-37.bin	64	16	Until 3M	Full Duplex	Datos + VPN + FW
3640	IP PLUS	c3640-is-mz.123-20.bin	96	32	Until 10M	Full Duplex	Datos, QoS
	IP/FW/IDS PLUS IPSEC 56	c3640-ik8o3s-mz.122-37.bin	64	16	Until 10M	Full Duplex	Datos + VPN + FW
7200 - 7200VXR	IP IPSEC 56	c7200-is56i-mz.121-27b.bin	64	16	No aplica	Full Duplex	ATM, QoS, VoIP, E1

TABLA A.3 Tabla de IOS recomendado de algunos equipos CISCO, para servicios de DATOS, con VoIP y sin ToIP.

Router Platform	IOS Type	IOS Name	Memory (Mb)	Flash (Mb)	BW Utilization Range	Port WAN Configuration	Features
1751	IP VOICE	c1700-ipvoice-mz.123-20.bin	64	16	Until 1M	Full Duplex	QoS, VoIP, FXO, FXS
	IP/VOICE PLUS	c1700-sv3y-mz.123-20.bin	48	16	Until 1M	Full Duplex	QoS, VoIP, FXO, FXS+BGP
2610-2613	IP/H323 PLUS BASIC	c2600-is3x-mz.123-20.bin	64	16	Until 2M	Full Duplex	QoS, VoIP, FXO, FXS
2610-2613	IP PLUS	c2600-is-mz.122-37.bin	48	16	Until 2M	Full Duplex	QoS, VoIP, FXO, FXS
2610XM-2611XM	IP VOICE	c2600-ipvoice-mz.123-20.bin	96	32	Until 2M	Full Duplex	QoS, VoIP, FXO, FXS
	IP PLUS	c2600-is-mz.123-20.bin	64	32	Until 2M	Full Duplex	QoS, VoIP, FXO, FXS
2620-2621	IP PLUS	c2600-is-mz.123-20.bin	64	32	Until 2M	Full Duplex	QoS, VoIP, FXO, FXS
2620XM-2621XM	IP VOICE	c2600-ipvoice-mz.123-20.bin	96	32	Until 4M	Full Duplex	QoS, VoIP, FXO, FXS
	IP PLUS	c2600-is-mz.123-20.bin	64	32	Until 4M	Full Duplex	QoS, VoIP, FXO, FXS
2801	IP VOICE	c2801-ipvoicek9-mz.124-8c.bin	128	64	Until 5M	Full Duplex	QoS, VoIP, E1
	ENTERPRISE SERVICES	c2801-entservicesk9-mz.124-8c.bin	128	64	Until 5M	Full Duplex	Datos + QOS + DLSW+ IPX + BGP
2811	IP VOICE	c2800nm-ipvoicek9-mz.124-8c.bin	256	64	Until 4.5M	Full Duplex	Datos + DLSW+ Datos
	ENTERPRISE SERVICES	c2800nm-entservicesk9-mz.124-8c.bin	256	64	Until 4.5M	Full Duplex	Datos + DLSW+ DatosX + BGP
2851	IP VOICE	c2800nm-ipvoicek9-mz.124-8c.bin	256	64	Until 14.5M	Full Duplex	Datos + DLSW+ Datos
	ENTERPRISE SERVICES	c2800nm-entservicesk9-mz.124-8c.bin	256	64	Until 14.5M	Full Duplex	Datos + DLSW+ DatosX + BGP
3640	IP PLUS	c3640-is-mz.123-20.bin	96	32	Until 10M	Full Duplex	Datos, QoS
	IP/FW/IDS PLUS IPSEC 56	c3640-ik8o3s-mz.122-37.bin	64	16	Until 10M	Full Duplex	Datos + VPN + FW
3660	IP PLUS	c3660-is-mz.123-20.bin	96	32	Until 10M	Full Duplex	Datos, QoS
	IP/FW/IDS PLUS IPSEC 56	c3660-ik8o3s-mz.122-37.bin	64	16	Until 10M	Full Duplex	Datos + VPN + FW
AS5350	IP PLUS	c5350-is-mz.123-13b.bin	128	32	Until 20M	Full Duplex	QoS, VoIP, E1
AS5400HPX	IP PLUS	c5400-is-mz.123-5f.bin	256	32	Until 20M	Full Duplex	QoS, VoIP, E1
7200 - 7200VXR	IP IPSEC 56	c7200-is56i-mz.121-27b.bin	64	16	16.5M - NPE400	Full Duplex	ATM, QoS, VoIP, E1

TABLA A.4 Tabla de IOS recomendado de algunos equipos CISCO, para servicios de DATOS, con VoIP y con ToIP.

Router Platform	IOS Type	IOS Name	Memory (Mb)	Flash (Mb)	BW Utilization Range	Port WAN Configuration	Features
1751	IP VOICE	c1700-ipvoice-mz.123-20.bin	64	16	Until 1M	Full Duplex	QoS, VoIP, FXO, FXS
	IP/VOICE PLUS	c1700-sv3y-mz.123-20.bin	48	16	Until 1M	Full Duplex	QoS, VoIP, FXO, FXS + BGP
2610-2613	IP/H323 PLUS BASIC	c2600-is3x-mz.123-20.bin	64	16	Until 2M	Full Duplex	QoS, VoIP, FXO, FXS
	IP PLUS	c2600-is-mz.121-27b.bin	40	8	Until 2M	Full Duplex	QoS, VoIP, FXO, FXS
2610XM-2611XM	IP VOICE	c2600-ipvoice-mz.123-20.bin	96	32	Until 2M	Full Duplex	QoS, VoIP, FXO, FXS
	IP PLUS	c2600-is-mz.121-27b.bin	40	8	Until 2M	Full Duplex	QoS, VoIP, FXO, FXS
2801	IP VOICE	c2801-ipvoicek9-mz.124-8c.bin	128	64	Until 5M	Full Duplex	QoS, VoIP, E1
	ENTERPRISE SERVICES	c2801-entservicesk9-mz.124-8c.bin	128	64	Until 5M	Full Duplex	Datos + QOS + DLSW+ IPX + BGP
2811	IP VOICE	c2800nm-ipvoicek9-mz.124-8c.bin	256	64	Until 4.5M	Full Duplex	Datos + DLSW+ Datos
	ENTERPRISE SERVICES	c2800nm-entservicesk9-mz.124-8c.bin	256	64	Until 4.5M	Full Duplex	Datos + DLSW+ DatosX + BGP
2851	IP VOICE	c2800nm-ipvoicek9-mz.124-8c.bin	256	64	Until 14.5M	Full Duplex	Datos + DLSW+ Datos
	ENTERPRISE SERVICES	c2800nm-entservicesk9-mz.124-8c.bin	256	64	Until 14.5M	Full Duplex	Datos + DLSW+ DatosX + BGP
3640	IP PLUS	c3640-is-mz.123-20.bin	96	32	Until 10M	Full Duplex	ATM, QoS, VoIP,ToIP, E1
	IP/FW/IDS PLUS IPSEC 56	c3640-ik8o3s-mz.122-37.bin	64	16	Until 10M	Full Duplex	Datos + VPN + FW
	ENTERPRISE PLUS/H323 MCM	c3640-jsx-mz.123-20.bin	96	32	Until 10M	Full Duplex	QoS, VoIP,ToIP, E1,DLSW + BGP + IPX
3660	IP PLUS	c3660-is-mz.123-20.bin	96	32	Until 10M	Full Duplex	ATM, QoS, VoIP,ToIP, E1
	IP/FW/IDS PLUS IPSEC 56	c3660-ik8o3s-mz.122-37.bin	64	16	Until 10M	Full Duplex	Datos + VPN + FW
	ENTERPRISE PLUS/H323 MCM	c3660-jsx-mz.123-20.bin	96	32	Until 10M	Full Duplex	QoS, VoIP,ToIP, E1,DLSW + BGP + IPX
3725	IP VOICE	c3725-ipvoice-mz.123-20.bin	128	32	Until 9M	Full Duplex	ATM, QoS, VoIP,ToIP, E1
	IP PLUS	c3725-is-mz.123-20.bin	128	32	Until 9M	Full Duplex	ATM, QoS, VoIP,ToIP, E1
	ENTERPRISE SERVICES	c3725-entservicesk9-mz.123-20.bin	128	32	Until 9M	Full Duplex	Datos + DLSW+ IPX + BGP
3845	IP VOICE	c3845-ipvoicek9-mz.124-8c.bin	256	64	Until 47M	Full Duplex	Datos + DLSW+ Datos
	ENTERPRISE SERVICES	c3845-entservicesk9-mz.124-8c.bin	256	64	Until 47M	Full Duplex	Datos + DLSW+ DatosX + BGP

ANEXO B
SIGLAS Y ABREVIATURAS

B1. SIGLAS Y ABREVIATURAS

- **ACL**: Lista de Acceso
- **AF**: Assured Forwarding
- **AS**: Autonomous Systems
- **ATM**: Asynchronous Transfer Mode
- **BA**: Behavior Aggregate
- **BC**: Commited Burst Size
- **BE**: Exces Burst Size
- **BGP**: Border Gateway Protocol
- **CAR**: Committed Access Rate
- **CBR**: Constraint-Based Routing
- **CBWFQ**:Class-Based Weighted Fair Queuing
- **CIR**: Commited Information Rate
- **CLI**: Command Line Interface
- **CLP**: Cell Loss Priority
- **CoS**: Class of Service
- **CQ**: Custom Queunig
- **CRC**: Cyclic Redundancy Check
- **cRTP**: Compressed Real-Time Transport Protocol
- **CS**: Class Selector
- **DE**: Discard Elegible
- **DLCI**: Data Link Connection Identifier
- **DSCP**:DiffServ Code Point
- **DSL**: Digital Suscriber Line
- **eBGP**: External Border Gateway Protocol
- **EF**: Expedited Forwarding
- **ESP**: Encapsulated Security Payload
- **FEC**: Forwarding Equivalence Class
- **FIFO**: First in – First out
- **GRE**: Generic Routing Encapsulation
- **iBGP**: Internal Border Gateway Protocol
- **IETF**: Internet Engineering Task Force

- **IGP**: Interior Gateway Protocol
- **IP**: Internet Protocol
- **LDP**: Label Distribution Protocol
- **LFI**: Link Fragmentation and Interleaving
- **LLQ**: Low-Latency Queuing
- **LSP**: Label Switched Path
- **LSR**: Label-Swiching Router
- **MPLS**:Multiprotocol Label Switching
- **MQC**: Modular QoS CLI
- **OSPF**: Open Shortest Path First
- **PHB**: Per-Hop Behaviors
- **POP**: Point of Presence
- **PPP**: Point-to-Point Protocol
- **PPTP**: Point-to-Point Tunneling Protocol
- **PQ**: Priority Queuing
- **PVC**: Permanent Virtual Connection
- **RAS**: Remote Access Server
- **RD**: Route Distinguisher
- **RDSI**: Red Digital de Servicios Integrados
- **RSVP**:Resource Reservation Protocol
- **RT**: Route Target
- **TCP**: Transmission Control Protocol
- **ToS**: Type of Service
- **TTL**: Time To Live
- **UDP**: User Datagram Protocol
- **VCI**: Virtual Circuit Identifier
- **VPDN**:Virtual Private Dial up Network
- **VPI**: Virtual Path Identifier
- **VPN**: Virtual Private Network
- **VRF**: VPN Routing and Forwarding Instance
- **WFQ**: Weighted Fair Queuing
- **WRED**:Weighted Random Early Detection

ANEXO C
LISTA DE FIGURAS

C1. LISTA DE FIGURAS

ANEXO D
LISTA DE TABLAS

D1. LISTA DE TABLAS

BIBLIOGRAFIA

1. Lynn Dalton, "Intranet VPN Business Scenario", 1999.
2. Cisco System, Inc, "MPLS Virtual Private Networks", 1999.
3. Cisco System, Inc., "MPLS Class of Service", 2000.
4. Cisco System, Inc., "MPLS Class of Service Enhancements", 2001.
5. NORTEL NETWORKS, "MPLS", 2001
6. William Stallings, "The Internet Protocol Journal", 2001.
7. José Barberá, "MPLS: Una Arquitectura de Backbone para la Internet del Siglo XXI", Telia Iberia – 2001.
8. Cisco IOS Technologies Division, "Service Provider QoS", 2001.
9. Cisco System, Inc., "Implementing Cisco Quality of Service, Versión 2.1", 2004.
10. Raúl Atiénzar Molpeceres, "VOZ sobre banda ancha", 2004.
11. Huawei Technologies, "Considerations and Practice of NGN", 2005.
12. Ing. Marcelo Fernandez - Cisco Chile, "Curso de QoS en equipos Cisco", Cisco System Perú – Diciembre 2006.